## Contents

### Preface

### Chapter 1  Command Reference Overview

### Chapter 2  Commands for Accessing the Switch

<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear account lockout</td>
<td>70</td>
</tr>
<tr>
<td>clear session</td>
<td>71</td>
</tr>
<tr>
<td>configure account</td>
<td>72</td>
</tr>
<tr>
<td>configure account password-policy char-validation</td>
<td>74</td>
</tr>
<tr>
<td>configure account password-policy history</td>
<td>76</td>
</tr>
<tr>
<td>configure account password-policy lockout-on-login-failures</td>
<td>77</td>
</tr>
<tr>
<td>configure account password-policy maxage</td>
<td>78</td>
</tr>
<tr>
<td>configure account password-policy min-pwd-length</td>
<td>79</td>
</tr>
<tr>
<td>configure banner</td>
<td>81</td>
</tr>
<tr>
<td>configure banner netlogin</td>
<td>82</td>
</tr>
<tr>
<td>configure dns-client add</td>
<td>83</td>
</tr>
<tr>
<td>configure dns-client add domain-suffix</td>
<td>84</td>
</tr>
<tr>
<td>configure dns-client add name-server</td>
<td>85</td>
</tr>
<tr>
<td>configure dns-client default-domain</td>
<td>86</td>
</tr>
<tr>
<td>configure dns-client delete</td>
<td>87</td>
</tr>
<tr>
<td>configure dns-client delete domain-suffix</td>
<td>88</td>
</tr>
<tr>
<td>configure dns-client delete name-server</td>
<td>89</td>
</tr>
<tr>
<td>configure idletimeouts</td>
<td>90</td>
</tr>
<tr>
<td>configure time</td>
<td>91</td>
</tr>
<tr>
<td>configure timezone</td>
<td>92</td>
</tr>
</tbody>
</table>
create account 96
delete account 98
disable clipaging 100
disable idletimeouts 101
enable clipaging 102
enable idletimeouts 103
enable license 104
history 106
reboot 107
show accounts password-policy 109
show accounts pppuser 111
show banner 113
show dns-client 114
show esrp-aware 115
show switch 116
traceroute 120

Chapter 3  Commands for Managing the Switch

configure snmp access-profile readonly 123
configure snmp access-profile readwrite 125
configure snmp add community 127
configure snmp add trapreceiver 129
configure snmp community 133
configure snmp delete community 135
configure snmp delete trapreceiver 137
configure snmp sysContact 139
configure snmp sysLocation 140
configure snmp sysName 141
configure snmpv3 add access 142
configure snmpv3 add community 144
configure snmpv3 add filter 146
configure snmpv3 add filter-profile 148
configure snmpv3 add group user 149
configure snmpv3 add mib-view 151
configure snmpv3 add notify 153
configure snmpv3 add target-addr 154
configure snmpv3 add target-params 156
configure snmpv3 add user 158
configure snmpv3 add user clone-from 160
configure snmpv3 delete access 161
configure snmpv3 delete community 163
configure snmpv3 delete filter 164
configure snmpv3 delete filter-profile 165
configure snmpv3 delete group user 166
configure snmpv3 delete mib-view 168
configure snmpv3 delete notify 170
configure snmpv3 delete target-addr 171
configure snmpv3 delete target-params 172
configure snmpv3 delete user 173
configure snmpv3 engine-boots 174
configure snmpv3 engine-id 175
configure snmpv3 extreme-target-addr-ext 176
configure sntp-client server 178
configure sntp-client update-interval 179
configure web login-timeout 180
disable alt-queue-management 181
disable dhcp ports vlan 182
disable eapol-flooding 183
disable snmp access 184
disable snmp dot1dTpFdbTable 185
disable snmp traps 186
disable snmp traps exceed-committed-rate ports 187
disable snmp traps mac-security 188
disable snmp traps port-up-down 189
disable sntp-client 190
disable system-watchdog 191
disable telnet 192
disable web 193
enable alt-queue-management 194
enable dhcp ports vlan 196
enable eapol-flooding 197
enable snmp access 198
enable snmp dot1dTpFdbTable 200
enable snmp traps 201
enable snmp traps exceed-committed-rate ports 202
enable snmp traps mac-security 204
enable snmp traps port-up-down 205
enable sntp-client 206
enable system-watchdog 207
enable telnet 208
enable web 210
exit 211
logout 212
quit 213
show eapol-flooding 214
show management 215
show odometer 218
show session 220
show snmpv3 access 222
show snmpv3 context 225
show snmpv3 counters 226
show snmpv3 engine-info 228
show snmpv3 extreme-target-addr-ext 229
show snmpv3 filter 230
show snmpv3 filter-profile 231
show snmpv3 group 232
show snmpv3 mib-view 234
show snmpv3 notify 236
show snmpv3 target-addr 237
show snmpv3 target-params 238
show snmpv3 user 239
show sntp-client 241
Chapter 4  Commands for Configuring Slots and Ports on a Switch

clear slot 251
configure backplane-ls-policy 252
configure ip-mtu vlan 253
configure jumbo-frame size 255
configure mirroring add 257
configure mirroring delete 259
configure msm-failover link-action 261
configure msm-failover slave-config 263
configure msm-failover timeout 264
configure port aggregate-bandwidth percent 265
configure port interpacket-gap 266
configure ports 267
configure ports auto-polarity 270
configure ports auto off 271
configure ports auto on 273
configure ports display-string 275
configure ports link-detection-level 277
configure ports preferred-medium 278
configure ports redundant 280
configure ports vdsl 282
configure sharing address-based 283
configure slot 285
disable card-scan 288
disable edp ports 289
disable flooding ports 291
disable jumbo-frame ports 292
disable lbdetect port 293
disable learning ports 294
Contents

disable mirroring 295
disable ports 296
disable sharing 298
disable slot 299
disable smartredundancy 300
enable card-scan 301
enable edp ports 302
enable flooding ports 304
enable jumbo-frame ports 305
enable lbdetect port 306
enable learning ports 307
enable mirroring to port 308
enable ports 310
enable sharing grouping 312
enable slot 315
enable smartredundancy 316
restart ports 317
run msm-failover 318
show edp 319
show mirroring 321
show msm-failover 322
show ports vlan stats 324
show ports collisions 325
show ports configuration 327
show ports info 329
show ports packet 333
show ports redundant 335
show ports sharing 336
show ports utilization 338
show ports vlan info 341
show sharing address-based 343
show slot 344
unconfigure msm-failover 353
unconfigure port aggregate-bandwidth 354
Chapter 5  VLAN Commands

configure dot1q ethertype 360
configure gvrp port 361
configure mac-vlan add mac-address 363
configure mac-vlan delete 365
configure ports monitor vlan 366
configure protocol add 367
configure protocol delete 369
configure vlan add member-vlan 370
configure vlan add ports 371
configure vlan add ports loopback-vid 373
configure vlan add secondary-ip 375
configure vlan delete member-vlan 377
configure vlan delete port 378
configure vlan delete secondary-ip 379
configure vlan ipaddress 380
configure vlan name 381
configure vlan protocol 382
configure vlan tag 383
create protocol 384
create vlan 385
delete protocol 387
delete vlan 388
disable gvrp 389
disable mac-vlan port 390
enable gvrp 391
enable mac-vlan mac-group port 392
show gvrp 394
show mac-vlan 395
show protocol 396
Chapter 6  FDB Commands

clear fdb 404
configure fdb agingtime 406
configure fdb-scan failure-action 407
configure fdb-scan period 409
create fdbentry secure-mac 410
create fdbentry vlan blackhole 411
create fdbentry vlan dynamic 413
create fdbentry vlan ports 415
delete fdbentry 417
disable fdb-scan 418
enable fdb-scan 420
run fdb-check 422
show fdb 424
unconfigure fdb-scan failure-action 427
unconfigure fdb-scan period 428

Chapter 7  QoS Commands

clear dlcs 431
configure diffserv examination code-point qosprofile ports 432
configure diffserv replacement priority code-point ports 434
configure dot1p type 436
configure ports qosprofile 438
configure qosprofile 439
configure qostype priority 441
configure red drop-probability 443
configure vlan priority 444
configure vlan qosprofile 445
disable diffserv examination ports 446
disable diffserv replacement ports 447
disable dlcs 448
Chapter 8  NAT Commands

clear nat  472
configure nat add vlan map  473
configure nat delete  477
configure nat finrst-timeout  479
configure nat icmp-timeout  480
configure nat syn-timeout  481
configure nat tcp-timeout  482
configure nat timeout  483
configure nat udp-timeout  484
configure nat vlan  485
disable nat  486
enable nat  487
show nat  488
Chapter 9  SLB Commands—“i” Series Switches Only

- clear slb connections 492
- clear slb persistence vip 493
- configure flow-redirect add next-hop 494
- configure flow-redirect delete next-hop 495
- configure flow-redirect service-check ftp 496
- configure flow-redirect service-check http 497
- configure flow-redirect service-check L4-port 498
- configure flow-redirect service-check nntp 499
- configure flow-redirect service-check ping 500
- configure flow-redirect service-check pop3 501
- configure flow-redirect service-check smtp 502
- configure flow-redirect service-check telnet 503
- configure flow-redirect timer ping-check 504
- configure flow-redirect timer service-check 505
- configure flow-redirect timer tcp-port-check 506
- configure slb esrp vlan 507
- configure slb failover alive-frequency 508
- configure slb failover dead-frequency 509
- configure slb failover failback-now 510
- configure slb failover ping-check 511
- configure slb failover unit 512
- configure slb global connection-block 513
- configure slb global connection-timeout 514
- configure slb global ftp 515
- configure slb global http 516
- configure slb global nntp 518
- configure slb global persistence-level 519
- configure slb global persistence-method 520
- configure slb global ping-check 521
- configure slb global pop3 522
- configure slb global service-check 523
- configure slb global smtp 524
- configure slb global synguard 525
configure slb global tcp-port-check  
configure slb global telnet  
configure slb gogo-mode health-check  
configure slb gogo-mode ping-check  
configure slb gogo-mode service-check ftp  
configure slb gogo-mode service-check http  
configure slb gogo-mode service-check pop3  
configure slb gogo-mode service-check smtp  
configure slb gogo-mode service-check telnet  
configure slb gogo-mode service-check timer  
configure slb gogo-mode tcp-port-check add  
configure slb gogo-mode tcp-port-check delete  
configure slb gogo-mode tcp-port-check timer  
configure slb L4-port  
configure slb node max-connections  
configure slb node ping-check  
configure slb node tcp-port-check  
configure slb pool add  
configure slb pool delete  
configure slb pool lb-method  
configure slb pool member  
configure slb proxy-client-persistence  
configure slb vip  
configure slb vip client-persistence-timeout  
configure slb vip max-connections  
configure slb vip service-check frequency  
configure slb vip service-check ftp  
configure slb vip service-check http  
configure slb vip service-check nntp  
configure slb vip service-check pop3  
configure slb vip service-check smtp  
configure slb vip service-check telnet  
configure vlan slb-type  
create flow-redirect
create slb pool 574
create slb vip 575
delete flow-redirect 576
delete slb pool 577
delete slb vip 578
disable flow-redirect 579
disable slb 580
disable slb 3dns 581
disable slb failover 582
disable slb failover manual-failback 583
disable slb failover ping-check 584
disable slb global synguard 585
disable slb gogo-mode 586
disable slb gogo-mode ping-check 587
disable slb gogo-mode service-check 588
disable slb gogo-mode tcp-port-check 589
disable slb L4-port 591
disable slb node 593
disable slb node ping-check 595
disable slb node tcp-port-check 596
disable slb proxy-client-persistence 598
disable slb vip 599
disable slb vip client-persistence 601
disable slb vip service-check 602
disable slb vip sticky-persistence 603
disable slb vip svcdown-reset 604
enable flow-redirect 605
enable slb 606
enable slb 3dns 607
enable slb failover 608
enable slb failover manual-failback 609
enable slb failover ping-check 610
enable slb global synguard 611
enable slb gogo-mode 612
Contents

enable slb gogo-mode ping-check 613
enable slb gogo-mode service-check 614
enable slb gogo-mode tcp-port-check 615
enable slb L4-port 617
enable slb node 619
enable slb node ping-check 621
enable slb node tcp-port-check 622
enable slb proxy-client-persistence 624
enable slb vip 625
enable slb vip client-persistence 627
enable slb vip service-check 628
enable slb vip sticky-persistence 629
enable slb vip svcdown-reset 630
show flow-redirect 631
show slb 3dns members 633
show slb connections 634
show slb esrp 636
show slb failover 637
show slb global 639
show slb gogo-mode 641
show slb L4-port 642
show slb node 644
show slb persistence 646
show slb pool 647
show slb stats 648
show slb vip 649
unconfigure slb all 651
unconfigure slb gogo-mode health-check 652
unconfigure slb gogo-mode service-check 653
unconfigure slb vip service-check 654
Chapter 10  Commands for Status Monitoring and Statistics

clear counters 657
clear log 658
clear log counters 660
clear log diag error 662
clear log diag remap 663
clear transceiver-test 664
configure flowstats export add port 666
configure flowstats export delete port 668
configure flowstats filter ports 669
configure flowstats source 671
configure flowstats timeout ports 672
configure log display 673
configure log filter events 675
configure log filter events match 678
configure log filter set severity 682
configure log filter set severity match 684
configure log target filter 686
configure log target format 688
configure log target match 692
configure log target severity 694
configure packet-mem-scan-recovery-mode 696
configure sflow agent 698
configure sflow backoff-threshold 699
configure sflow collector 701
configure sflow poll-interval 703
configure sflow sample-rate 704
configure sys-health-check alarm-level 705
configure sys-health-check auto-recovery 708
configure sys-health-check scan recovery 711
configure sys-recovery-level 713
configure syslog add 715
configure syslog delete 717
configure transceiver-test failure-action 718
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure transceiver-test period</td>
<td>720</td>
</tr>
<tr>
<td>configure transceiver-test threshold</td>
<td>721</td>
</tr>
<tr>
<td>configure transceiver-test window</td>
<td>722</td>
</tr>
<tr>
<td>create log filter</td>
<td>723</td>
</tr>
<tr>
<td>delete log filter</td>
<td>725</td>
</tr>
<tr>
<td>disable cli-config-logging</td>
<td>726</td>
</tr>
<tr>
<td>disable flowstats</td>
<td>727</td>
</tr>
<tr>
<td>disable flowstats filter ports</td>
<td>728</td>
</tr>
<tr>
<td>disable flowstats ping-check</td>
<td>730</td>
</tr>
<tr>
<td>disable flowstats ports</td>
<td>731</td>
</tr>
<tr>
<td>disable log debug-mode</td>
<td>732</td>
</tr>
<tr>
<td>disable log display</td>
<td>733</td>
</tr>
<tr>
<td>disable log target</td>
<td>734</td>
</tr>
<tr>
<td>disable rmon</td>
<td>736</td>
</tr>
<tr>
<td>disable sflow</td>
<td>737</td>
</tr>
<tr>
<td>disable sflow backoff-threshold</td>
<td>738</td>
</tr>
<tr>
<td>disable sflow ports</td>
<td>739</td>
</tr>
<tr>
<td>disable sys-health-check</td>
<td>740</td>
</tr>
<tr>
<td>disable syslog</td>
<td>741</td>
</tr>
<tr>
<td>disable temperature-logging</td>
<td>742</td>
</tr>
<tr>
<td>disable transceiver-test</td>
<td>744</td>
</tr>
<tr>
<td>enable cli-config-logging</td>
<td>746</td>
</tr>
<tr>
<td>enable flowstats</td>
<td>747</td>
</tr>
<tr>
<td>enable flowstats filter ports</td>
<td>748</td>
</tr>
<tr>
<td>enable flowstats ping-check</td>
<td>750</td>
</tr>
<tr>
<td>enable flowstats ports</td>
<td>751</td>
</tr>
<tr>
<td>enable log debug-mode</td>
<td>752</td>
</tr>
<tr>
<td>enable log display</td>
<td>753</td>
</tr>
<tr>
<td>enable log target</td>
<td>754</td>
</tr>
<tr>
<td>enable rmon</td>
<td>756</td>
</tr>
<tr>
<td>enable sflow</td>
<td>758</td>
</tr>
<tr>
<td>enable sflow backoff-threshold</td>
<td>759</td>
</tr>
<tr>
<td>enable sflow ports</td>
<td>760</td>
</tr>
<tr>
<td>enable sys-health-check</td>
<td>761</td>
</tr>
</tbody>
</table>
enable syslog 763
enable temperature-logging 764
enable transceiver-test 766
save log 768
show flowstats 770
show flowstats 772
show flowstats export 774
show log 775
show log components 779
show log configuration 781
show log configuration filter 783
show log configuration target 785
show log counters 786
show log events 788
show memory 790
show packet-mem-scan-recovery-mode 792
show packet miscompare 794
show ports rxerrors 795
show ports stats 798
show ports txerrors 801
show sflow configuration 804
show sflow statistics 806
show version 808
unconfigure flowstats filter ports 811
unconfigure flowstats ports 812
unconfigure log filter 813
unconfigure log target format 814
unconfigure packet-mem-scan-recovery-mode 816
unconfigure sflow agent 817
unconfigure sflow backoff-threshold 818
unconfigure sflow collector 819
unconfigure transceiver-test failure-action 820
unconfigure transceiver-test period 821
unconfigure transceiver-test threshold 822
unconfigure transceiver-test window 823
upload log 824

Chapter 11 Security Commands

clear netlogin state 830
clear netlogin state mac-address 831
configure access-profile add 832
configure access-profile delete 835
configure access-profile mode 836
configure auth mgmt-access local 837
configure auth mgmt-access radius 839
configure auth mgmt-access radius-accounting 840
configure auth mgmt-access tacacs 841
configure auth mgmt-access tacacs-accounting 843
configure auth netlogin radius 845
configure auth netlogin radius-accounting 846
configure cpu-dos-protect alert-threshold 847
configure cpu-dos-protect filter-precedence 848
configure cpu-dos-protect filter-type-allowed 849
configure cpu-dos-protect messages 850
configure cpu-dos-protect notice-threshold 851
configure cpu-dos-protect timeouts 852
configure cpu-dos-protect trusted-ports 853
configure cpu-dos-protect (Port-Based) 854
configure cpu-dos-protect trusted-ports 855
configure enhanced-dos-protect ipfdb agingtime 856
configure enhanced-dos-protect ipfdb cache-size 857
configure enhanced-dos-protect ipfdb learn-limit 858
configure enhanced-dos-protect ipfdb learn-window 859
configure enhanced-dos-protect ports 860
configure enhanced-dos-protect rate-limit 861
configure ip-subnet-lookup maskbits 863
configure mac-lockdown-timeout ports aging-time 864
configure netlogin base-url 865
configure netlogin mac-address 866
configure netlogin mac auth-retry-count 867
configure netlogin mac reauth-period 868
configure netlogin redirect-page 869
configure radius server 870
configure radius shared-secret 872
configure radius timeout 873
configure radius-accounting server 875
configure radius-accounting shared-secret 876
configure radius-accounting timeout 877
configure route-map add 878
configure route-map add goto 880
configure route-map add match 881
configure route-map add set 883
configure route-map delete 885
configure route-map delete goto 886
configure route-map delete match 887
configure route-map delete set 889
configure security-profile default-user-vlan 891
configure security-profile dot11-auth network-auth encryption 892
configure security-profile dot1x-wpa-timers group-update-timer 895
configure security-profile dot1x-wpa-timers pairwise-update-timer 896
configure security-profile dot1x-wpa-timers reauth-period 897
configure security-profile ess-name 898
configure security-profile ssid-in-beacon 899
configure security-profile use-dynamic-vlan 900
configure security-profile wep default-key-index 902
configure security-profile wep key add 903
configure security-profile wep key delete 904
configure security-profile wpa-psk 905
configure security-profile wpa2-psk 906
configure security-profile wpa-only 907
configure ssh2 key 908
configure ssl certificate pregenerated 910
configure ssl certificate privkeylen country organization common-name
configure ssl privkey pregenerated
configure tacacs server
configure tacacs server timeout
configure tacacs shared-secret
configure tacacs timeout
configure tacacs-accounting server
configure tacacs-accounting shared-secret
configure tacacs-accounting timeout
configure vlan access-profile
configure vlan dhcp-address-range
configure vlan dhcp-lease-timer
configure vlan dhcp-options
configure vlan netlogin-lease-timer
create access-list
create access-list icmp destination source
create access-list ip destination source ports
create access-list tcp destination source ports
create access-list udp destination source ports
create access-mask
create access-profile type
create rate-limit
create route-map
create security-profile
create trusted-mac-address
delete access-list
delete access-mask
delete access-profile
delete rate-limit
delete route-map
delete security-profile
delete trusted-mac-address
disable access-list
disable arp-learning
disable arp-learning ports 961
disable arp-learning vlan 962
disable arp-learning vlan ports 963
disable cpu-dos-protect 964
disable dhcp ports vlan 965
disable enhanced-dos-protect 966
disable ip-subnet-lookup 967
disable mac-lockdown-timeout ports 968
disable netlogin 969
disable netlogin logout-privilege 971
disable netlogin ports 972
disable netlogin ports mac 973
disable netlogin session-refresh 974
disable radius 975
disable radius-accounting 976
disable source-ip-lockdown ports 977
disable ssh2 978
disable tacacs 979
disable tacacs-accounting 980
disable tacacs-authorization 981
disable trusted-mac-address 982
disable web 983
disable web http 984
disable web https 985
download ssl certificate 986
download ssl privkey 987
enable access-list 989
enable arp-learning 990
enable arp-learning ports 991
enable arp-learning vlan 992
enable arp-learning vlan ports 993
enable cpu-dos-protect 994
enable cpu-dos-protect simulated 995
enable dhcp ports vlan 996
show ip-subnet-lookup fdb 1040
show mac-lockdown-timeout ports 1041
show mac-lockdown-timeout fdb ports 1042
show netlogin 1044
show netlogin mac 1046
show radius 1047
show radius-accounting 1049
show rate-limit 1051
show route-map 1053
show security-profile 1054
show source-ip-lockdown ports 1057
show ssl 1058
show tacacs 1061
show tacacs-accounting 1063
show trusted-mac-address 1065
show vlan security 1066
ssh2 1067
unconfigure auth mgmt-access 1069
unconfigure auth netlogin 1070
unconfigure cpu-dos-protect 1071
unconfigure enhanced-dos-protect ipfdb agingtime 1072
unconfigure enhanced-dos-protect ipfdb cache-size 1073
unconfigure enhanced-dos-protect ipfdb learn-limit 1074
unconfigure enhanced-dos-protect ipfdb learn-window 1075
unconfigure enhanced-dos-protect ports 1076
unconfigure enhanced-dos-protect rate-limit 1077
unconfigure netlogin mac-address 1079
unconfigure netlogin mac auth-retry-count 1080
unconfigure netlogin mac reauth-period 1081
unconfigure radius 1082
unconfigure radius-accounting 1083
unconfigure tacacs 1084
unconfigure tacacs-accounting 1085
unconfigure vlan dhcp-address-range 1086
unconfigure vlan dhcp-options 1088

Chapter 12  Configuration and Image Commands

Chapter 13  Troubleshooting Commands
configure debug-trace dvmrp-neighbor 1136
configure debug-trace dvmrp-route 1138
configure debug-trace dvmrp-timer 1140
configure debug-trace eaps-system 1141
configure debug-trace flow-redirect 1143
configure debug-trace flowstats 1145
configure debug-trace health-check 1146
configure debug-trace iparp 1149
configure debug-trace ipxgns-message 1151
configure debug-trace ipxrip-message 1153
configure debug-trace ipxrip-route 1155
configure debug-trace ipxsap-entry 1156
configure debug-trace ipxsap-message 1157
configure debug-trace isis-cli 1159
configure debug-trace isis-event 1160
configure debug-trace isis-hello 1161
configure debug-trace isis-lsp 1162
configure debug-trace isis-snp 1163
configure debug-trace isis-spf 1164
configure debug-trace mpls 1165
configure debug-trace mpls-signalling 1168
configure debug-trace npcard 1170
configure debug-trace pim-cache 1171
configure debug-trace pim-hello 1173
configure debug-trace pim-message 1175
configure debug-trace pim-neighbor 1177
configure debug-trace pim-rp-mgmt 1179
configure debug-trace rip-message 1181
configure debug-trace rip-route-change 1182
configure debug-trace rip-triggered-update 1183
configure debug-trace slb-3dns 1184
configure debug-trace slb-connection 1185
configure debug-trace slb-failover 1186
configure debug-trace stacking 1187
configure debug-trace transceiver-test 1189
configure debug-trace udp-forwarding 1191
configure debug-trace vrrp 1192
configure debug-trace vrrp-hello 1193
configure debug-trace wireless 1195
configure diagnostics 1197
configure reboot-loop-protection 1199
configure system-dump server 1200
configure system-dump timeout 1201
disable log debug-mode 1202
enable log debug-mode 1203
nslookup 1204
ping 1205
run diagnostics 1207
run diagnostics_noslot 1210
run diagnostics cable ports 1212
run diagnostics packet-memory slot 1214
show debug-trace 1217
show diagnostics 1221
show diagnostics backplane arm mapping 1224
show diagnostics backplane mpls mapping 1225
show diagnostics backplane utilization 1226
show diagnostics cable 1227
show diagnostics packet-memory slot 1229
show diagnostics slot fdb 1231
show ports cable diagnostics 1232
show system-dump 1234
show tech-support 1236
top 1238
unconfigure system-dump 1243
upload system-dump 1244
Chapter 14  Wireless Commands

clear APmgmt port history 1247
clear wireless ports counters 1248
clear wireless ports interface ap-scan results 1249
clear wireless ports interface client-history 1250
clear wireless ports interface client-scan counters 1251
clear wireless ports interface client-scan results 1252
clear wireless ports log 1253
configure antenna-profile 1254
configure rf-profile beacon-interval 1255
configure rf-profile dtim-interval 1256
configure rf-profile frag-length 1257
configure rf-profile long-retry 1258
configure rf-profile preamble 1259
configure rf-profile rts-threshold 1260
configure rf-profile short-retry 1261
configure wireless country-code 1262
configure wireless default-gateway 1264
configure wireless management-vlan 1265
configure wireless port antenna-profile 1266
configure wireless ports antenna-location 1267
configure wireless ports detected-station-timeout 1268
configure wireless ports force-disassociation 1269
configure wireless ports health-check 1270
configure wireless ports interface ap-scan added-trap 1271
configure wireless ports interface ap-scan off-channel 1272
configure wireless ports interface ap-scan off-channel continuous 1273
configure wireless ports interface ap-scan off-channel max-wait 1274
configure wireless ports interface ap-scan off-channel min-wait 1275
configure wireless ports interface ap-scan probe-interval 1276
configure wireless ports interface ap-scan removed-trap 1277
configure wireless ports interface ap-scan results size 1278
configure wireless ports interface ap-scan results timeout 1279
configure wireless ports interface ap-scan send-probe 1280
configure wireless ports interface ap-scan updated-trap 1281
configure wireless ports interface channel 1282
configure wireless ports interface client-history size 1284
configure wireless ports interface client-history timeout 1285
configure wireless ports interface client-scan added-trap 1286
configure wireless ports interface client-scan removed-trap 1287
configure wireless ports interface client-scan results size 1288
configure wireless ports interface client-scan results timeout 1289
configure wireless ports interface max-clients 1290
configure wireless ports interface rf-profile 1291
configure wireless ports interface security-profile 1292
configure wireless ports interface transmit-power 1293
configure wireless ports interface transmit-rate 1294
configure wireless ports interface wireless-bridging 1295
configure wireless ports ipaddress 1296
configure wireless ports location 1297
create antenna-profile 1298
create rf-profile copy 1299
create rf-profile mode 1300
delete antenna-profile 1301
delete rf-profile 1302
disable wireless ports 1303
disable wireless ports cancel-scheduler 1304
disable wireless ports every 1305
disable wireless ports interface 1306
disable wireless ports interface ap-scan 1307
disable wireless ports interface ap-scan off-channel 1308
disable wireless ports interface client-history 1309
disable wireless ports interface client-scan 1310
disable wireless ports interface iapp 1311
disable wireless ports interfacesvp 1312
disable wireless ports time 1313
enable wireless ports 1314
enable wireless ports cancel-scheduler 1315
enable wireless ports every 1316
enable wireless ports interface 1317
enable wireless ports interface ap-scan 1318
enable wireless ports interface ap-scan off-channel 1319
enable wireless ports interface client-history 1320
enable wireless ports interface client-scan 1321
enable wireless ports interface iapp 1322

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.

enable wireless ports interface svp 1323
enable wireless ports time 1324
reset wireless ports 1325
reset wireless ports interface 1326
show antenna-profile 1327
show APmgmt port 1328
show rf-profile 1330
show wireless ap-scan results 1335
show wireless ap-scan results mac_address 1337
show wireless client-scan results 1338
show wireless configuration 1340
show wireless ports 1341
show wireless ports configuration 1343
show wireless ports debug-trace 1345
show wireless ports interface ap-scan configuration 1347

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.

show wireless ports interface ap-scan results 1349
show wireless ports interface ap-scan results mac-address 1352

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.

show wireless ports interface client mac-statistics 1354
show wireless ports interface client-history configuration 1356
show wireless ports interface client-history diagnostics 1357
show wireless ports interface client-history mac-layer 1359
show wireless ports interface client-history status 1361
show wireless ports interface client-scan configuration 1363
show wireless ports interface client-scan results 1365
Contents

show wireless ports interface client-scan results mac-address 1367
show wireless ports interface client-scan status 1368
show wireless ports interface clients 1370
show wireless ports interface configuration 1372
show wireless ports interface pae-diagnostics 1375
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface pae-statistics 1376
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface rf-status 1377
show wireless ports interface security-status 1379
show wireless ports interface stats 1381
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface status 1382
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports log 1383
unconfigure wireless ports ipaddress 1385

Chapter 15  Stacking Commands

configure stacking fallback-ip-address 1389
configure stacking priority 1391
configure stacking requested-slot 1392
configure stacking slot-binding 1393
disable stacking 1394
enable stacking 1396
show stacking 1397
show stacking port 1400
unconfigure stacking fallback-ip-address 1401
unconfigure stacking requested-slot 1402

Chapter 16  EAPS Commands

configure eaps add control vlan 1404
configure eaps add protect vlan 1405
configure eaps delete control vlan 1406
configure eaps delete protect vlan 1407
configure eaps failtime 1408
configure eaps failtime expiry-action 1409
configure eaps fast-convergence 1411
configure eaps hellotime 1412
configure eaps mode 1413
configure eaps name 1414
configure eaps port 1415
configure eaps shared-port link-id 1416
configure eaps shared-port mode 1417
create eaps 1418
create eaps shared-port 1419
delete eaps 1420
delete eaps shared-port 1421
disable eaps 1422
enable eaps 1423
show eaps 1424
show eaps shared-port 1429
show eaps summary 1431
unconfigure eaps port 1433
unconfigure eaps shared-port link-id 1434
unconfigure eaps shared-port mode 1435

Chapter 17  STP Commands

configure stpd add vlan 1439
configure stpd delete vlan 1441
configure stpd forwarddelay 1442
configure stpd hellotime 1443
configure stpd maxage 1444
configure stpd mode 1445
configure stpd ports cost 1446
configure stpd ports link-type 1448
configure stpd ports link-type edge edge-safeguard disable 1450
configure stpd ports link-type edge edge-safeguard enable 1451
configure stpd ports mode 1452
configure stpd ports priority 1453
configure stpd priority 1455
Chapter 18 ESRP Commands

clear elrp stats

clear elsm auto-restart ports

clear elsm counters ports

configure debug elsm-port

configure debug elsm-system

configure elrp-client one-shot

configure elrp-client periodic

configure elsm hellotime

configure elsm hold-threshold

configure esrp port-mode ports

configure msm-failover esrp-failover-mode

configure vlan add domain-member vlan

configure vlan add elrp-poll ports

configure vlan add ports no-restart
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure vlan add ports restart</td>
<td>1509</td>
</tr>
<tr>
<td>configure vlan add track-bgp</td>
<td>1510</td>
</tr>
<tr>
<td>configure vlan add track-diagnostic</td>
<td>1511</td>
</tr>
<tr>
<td>configure vlan add track-environment</td>
<td>1512</td>
</tr>
<tr>
<td>configure vlan add track-iproute</td>
<td>1513</td>
</tr>
<tr>
<td>configure vlan add track-ospf</td>
<td>1514</td>
</tr>
<tr>
<td>configure vlan add track-ping</td>
<td>1515</td>
</tr>
<tr>
<td>configure vlan add track-rip</td>
<td>1516</td>
</tr>
<tr>
<td>configure vlan add track-vlan</td>
<td>1517</td>
</tr>
<tr>
<td>configure vlan delete domain-member vlan</td>
<td>1518</td>
</tr>
<tr>
<td>configure vlan delete elrp-poll ports</td>
<td>1519</td>
</tr>
<tr>
<td>configure vlan delete track-bgp</td>
<td>1520</td>
</tr>
<tr>
<td>configure vlan delete track-diagnostic</td>
<td>1521</td>
</tr>
<tr>
<td>configure vlan delete track-environment</td>
<td>1522</td>
</tr>
<tr>
<td>configure vlan delete track-iproute</td>
<td>1523</td>
</tr>
<tr>
<td>configure vlan delete track-ospf</td>
<td>1524</td>
</tr>
<tr>
<td>configure vlan delete track-ping</td>
<td>1525</td>
</tr>
<tr>
<td>configure vlan delete track-rip</td>
<td>1526</td>
</tr>
<tr>
<td>configure vlan delete track-vlan</td>
<td>1527</td>
</tr>
<tr>
<td>configure vlan esrp elrp-master-poll disable</td>
<td>1528</td>
</tr>
<tr>
<td>configure vlan esrp elrp-master-poll enable</td>
<td>1529</td>
</tr>
<tr>
<td>configure vlan esrp elrp-premaster-poll disable</td>
<td>1531</td>
</tr>
<tr>
<td>configure vlan esrp elrp-premaster-poll enable</td>
<td>1532</td>
</tr>
<tr>
<td>configure vlan esrp esrp-election</td>
<td>1534</td>
</tr>
<tr>
<td>configure vlan esrp esrp-premaster-timeout</td>
<td>1536</td>
</tr>
<tr>
<td>configure vlan esrp group</td>
<td>1537</td>
</tr>
<tr>
<td>configure vlan esrp group add esrp-aware-ports</td>
<td>1538</td>
</tr>
<tr>
<td>configure vlan esrp group delete esrp-aware-ports</td>
<td>1540</td>
</tr>
<tr>
<td>configure vlan esrp priority</td>
<td>1541</td>
</tr>
<tr>
<td>configure vlan esrp timer</td>
<td>1542</td>
</tr>
<tr>
<td>disable elrp-client</td>
<td>1544</td>
</tr>
<tr>
<td>disable elsm auto-restart ports</td>
<td>1545</td>
</tr>
<tr>
<td>disable elsm ports</td>
<td>1546</td>
</tr>
<tr>
<td>disable esrp vlan</td>
<td>1548</td>
</tr>
</tbody>
</table>
enable elrp-client 1549
enable elsm auto-restart ports 1550
enable elsm ports 1551
enable esrp vlan 1553
show elrp 1554
show elsm 1557
show elsm ports 1558
show esrp 1560
show esrp vlan 1563
show esrp-aware vlan 1565
show esrp-aware-ports 1566
unconfigure elrp-client 1567

Chapter 19  VRRP Commands
configure vrrp add vlan 1571
configure vrrp delete 1572
configure vrrp vlan add 1573
configure vrrp vlan authentication 1574
configure vrrp vlan delete vrid 1575
configure vrrp vlan vrid 1576
disable vrrp 1578
enable vrrp 1579
show vrrp 1580
show vrrp vlan stats 1582

Chapter 20  IP Unicast Commands
clear iparp 1586
clear ipfdb 1587
configure bootprelay add 1588
configure bootprelay delete 1589
configure bootprelay dhcp-agent information check 1590
configure bootprelay dhcp-agent information option 1592
configure bootprelay dhcp-agent information policy 1594
configure ip-down-vlan-action 1596
configure iparp add 1597
configure iparp add proxy 1598
configure iparp delete 1600
configure iparp delete proxy 1601
configure iparp max-entries 1602
configure iparp max-pending-entries 1603
configure iparp timeout 1604
configure ipfdb route-add 1605
configure iproute add 1606
configure iproute add blackhole 1607
configure iproute add blackhole default 1608
configure iproute add default 1609
configure iproute delete 1610
configure iproute delete blackhole 1611
configure iproute delete blackhole default 1612
configure iproute delete default 1613
configure iproute priority 1614
configure iproute route-map 1616
configure irdp 1618
configure udp-profile add 1620
configure udp-profile delete 1621
configure vlan secondary-ip 1622
configure vlan subvlan 1624
configure vlan subvlan-address-range 1625
configure vlan upd-profile 1626
create udp-profile 1627
delete udp-profile 1628
disable bootp vlan 1629
disable bootprelay 1630
disable icmp access-list 1631
disable icmp address-mask 1632
disable icmp parameter-problem 1633
disable icmp port-unreachables 1634
disable icmp redirects 1635
disable icmp time-exceeded
disable icmp timestamp
disable icmp unreachable
disable icmp userredirects
disable ip-option loose-source-route
disable ip-option record-route
disable ip-option record-timestamp
disable ip-option strict-source-route
disable ip-option use-router-alert
disable iparp checking
disable iparp refresh
disable ipforwarding
disable ipforwarding lpm-routing
disable iproute sharing
disable irdp
disable loopback-mode vlan
disable multinetting
disable subvlan-proxy-arp vlan
disable udp-echo-server
enable bootp vlan
enable bootprelay
enable icmp access-list
enable icmp address-mask
enable icmp parameter-problem
enable icmp port-unreachable
enable icmp redirects
enable icmp time-exceeded
enable icmp timestamp
enable icmp unreachable
enable icmp userredirects
enable ip-option loose-source-route
enable ip-option record-route
enable ip-option record-timestamp
enable ip-option strict-source-route
Contents

enable ip-option use-router-alert 1671
enable iparp checking 1672
enable iparp refresh 1673
enable ipforwarding 1674
enable ipforwarding lpm-routing 1676
enable iproute sharing 1677
enable irdp 1678
enable loopback-mode vlan 1679
enable multinetting 1680
enable subvlan-proxy-arp vlan 1681
enable udp-echo-server 1682
rtlookup 1683
run ipfdb-check 1684
show iparp 1685
show iparp proxy 1686
show ipconfig 1687
show ipfdb 1689
show iproute 1691
show ipstats 1694
show udp-profile 1697
unconfigure bootprelay dhcp-agent information check 1698
unconfigure bootprelay dhcp-agent information option 1699
unconfigure bootprelay dhcp-agent information policy 1700
unconfigure icmp 1701
unconfigure iparp 1702
unconfigure irdp 1703
unconfigure udp-profile 1704

Chapter 21 IGP Commands

clear isis adjacency 1707
clear isis lsdb 1708
configure isis add area address 1709
configure isis add vlan 1710
configure isis area add domain-summary 1711
configure isis area delete domain-summary 1712
configure isis area domain-filter 1713
configure isis authentication 1714
configure isis delete area-address 1715
configure isis delete vlan 1716
configure isis external-filter 1717
configure isis lsp holddown interval 1718
configure isis lsp lifetime 1719
configure isis lsp refresh interval 1720
configure isis metric-size 1721
configure isis spf hold time 1722
configure isis system-identifier 1723
configure isis vlan 1724
configure isis vlan authentication 1725
configure isis vlan cost 1726
configure isis vlan hello-multiplier 1727
configure isis vlan priority 1728
configure isis vlan timer 1729
configure ospf add virtual-link 1731
configure ospf add vlan area 1732
configure ospf add vlan area link-type 1734
configure ospf area add range 1735
configure ospf area delete range 1736
configure ospf area external-filter 1737
configure ospf area interarea-filter 1738
configure ospf area normal 1739
configure ospf area nssa stub-default-cost 1740
configure ospf area stub stub-default-cost 1741
configure ospf asbr-filter 1742
configure ospf ase-limit 1743
configure ospf ase-summary add 1744
configure ospf ase-summary delete 1745
configure ospf cost 1746
configure ospf delete virtual-link 1747
configure ospf delete vlan 1748
configure ospf direct-filter 1749
configure ospf lsa-batch-interval 1750
configure ospf metric-table 1751
configure ospf priority 1752
configure ospf routerid 1753
configure ospf spf-hold-time 1755
configure ospf timer 1756
configure ospf virtual-link authentication password 1758
configure ospf vlan area 1759
configure ospf vlan neighbor add 1760
configure ospf vlan neighbor delete 1761
configure ospf vlan timer 1762
configure rip add vlan 1764
configure rip delete vlan 1765
configure rip garbagetime 1766
configure rip routetimeout 1767
configure rip rmode 1768
configure rip txmode 1769
configure rip updatetime 1770
configure rip vlan cost 1771
configure rip vlan export-filter 1772
configure rip vlan import-filter 1773
configure rip vlan trusted-gateway 1774
create isis area 1775
create ospf area 1776
delete isis area 1777
delete ospf area 1778
disable isis 1779
disable isis export 1780
disable isis ignore-attached-bit 1782
disable isis originate-default 1783
disable isis overload 1784
disable ospf 1785
disable ospf capability opaque-lsa 1786
disable ospf export 1787
disable ospf originate-router-id 1789
disable rip 1790
disable rip aggregation 1791
disable rip export 1792
disable rip exportstatic 1794
disable rip originate-default 1795
disable rip poisonreverse 1796
disable rip splithorizon 1797
disable rip triggerupdate 1798
enable isis 1799
enable isis export 1800
enable isis ignore-attached-bit 1802
enable isis originate-default 1803
enable isis overload 1804
enable ospf 1805
enable ospf capability opaque-lsa 1806
enable ospf export 1807
enable ospf export direct 1809
enable ospf export rip 1811
enable ospf export static 1813
enable ospf export vip 1815
enable ospf originate-default 1817
enable ospf originate-router-id 1818
enable rip 1819
enable rip aggregation 1820
enable rip export cost 1821
enable rip export static cost 1823
enable rip exportstatic 1824
enable rip originate-default cost 1825
enable rip poisonreverse 1826
enable rip splithorizon 1827
enable rip triggerupdate 1828
show ospf
show ospf area
show ospf area detail
show ospf ase-summary
show ospf interfaces
show ospf interfaces detail
show ospf lsdb area lstype
show ospf virtual-link
show rip
show rip stats
show rip stats vlan
show rip vlan
unconfigure ospf
unconfigure rip

Chapter 22  BGP Commands—“i” Series Switches Only

clear bgp neighbor counters
clear bgp neighbor flap-statistics
configure bgp add aggregate-address
configure bgp add confederation-peer sub-AS-number
configure bgp add network
configure bgp AS-number
configure bgp cluster-id
configure bgp confederation-id
configure bgp delete aggregate-address
configure bgp delete confederation-peer sub-AS-number
configure bgp delete network
configure bgp local-preference
configure bgp med
configure bgp neighbor as-path-filter
configure bgp neighbor dampening
configure bgp neighbor maximum-prefix
configure bgp neighbor next-hop-self
configure bgp neighbor nlrifilter
configure bgp neighbor no-dampening 1868
configure bgp neighbor password 1869
configure bgp neighbor peer-group 1871
configure bgp neighbor route-map-filter 1872
configure bgp neighbor route-reflector-client 1873
configure bgp neighbor send-community 1874
configure bgp neighbor soft-reset 1875
configure bgp neighbor source-interface 1876
configure bgp neighbor timer 1877
configure bgp neighbor weight 1878
configure bgp peer-group as-path-filter 1879
configure bgp peer-group dampening 1880
configure bgp peer-group maximum-prefix 1882
configure bgp peer-group next-hop-self 1884
configure bgp peer-group nlri-filter 1885
configure bgp peer-group no-dampening 1886
configure bgp peer-group route-reflector-client 1887
configure bgp peer-group send-community 1888
configure bgp peer-group password 1889
configure bgp peer-group remote-AS-number 1890
configure bgp peer-group route-map-filter 1891
configure bgp peer-group soft-reset 1892
configure bgp peer-group source-interface 1893
configure bgp peer-group timer 1894
configure bgp peer-group weight 1895
configure bgp routerid 1896
configure bgp soft-reconfiguration 1897
create bgp neighbor peer-group 1898
create bgp neighbor remote-AS-number 1899
create bgp peer-group 1900
delete bgp neighbor 1901
delete bgp peer-group 1902
disable bgp 1903
disable bgp aggregation 1904
disable bgp always-compare-med 1905
disable bgp community format 1906
disable bgp export 1907
disable bgp neighbor 1909
disable bgp neighbor remove-private-AS-numbers 1910
disable bgp neighbor soft-in-reset 1911
disable bgp peer-group 1912
disable bgp synchronization 1913
enable bgp 1914
enable bgp aggregation 1915
enable bgp always-compare-med 1916
enable bgp community format 1917
enable bgp export 1918
enable bgp neighbor 1920
enable bgp neighbor remove-private-AS-numbers 1921
enable bgp neighbor soft-in-reset 1922
enable bgp peer-group 1923
enable bgp synchronization 1924
show bgp 1925
show bgp neighbor 1926
show bgp peer-group 1928
show bgp routes 1929

Chapter 23  IP Multicast Commands

clear igmp group 1934
clear igmp snooping 1935
clear ipmc cache 1936
clear ipmc fdb 1937
configure dvmrp add vlan 1938
configure dvmrp delete vlan 1939
configure dvmrp timer 1940
configure dvmrp vlan cost 1941
configure dvmrp vlan export-filter 1942
configure dvmrp vlan import-filter 1943
configure dvmrp vlan timer 1944
configure dvmrp vlan trusted-gateway 1945
configure ext-mcast loopback-port 1946
configure igmp 1947
configure igmp snooping add static group 1948
configure igmp snooping add static router 1950
configure igmp snooping delete static group 1951
configure igmp snooping delete static router 1952
configure igmp snooping filter 1953
configure igmp snooping flood-list 1954
configure igmp snooping leave-timeout 1956
configure igmp snooping timer 1957
configure mcast-queue-mgmt 1959
configure mroute add 1960
configure mroute delete 1961
configure pim add vlan 1962
configure pim cbsr 1964
configure pim crp static 1965
configure pim crp timer 1966
configure pim crp vlan access profile 1967
configure pim delete vlan 1968
configure pim register-checksum-to 1969
configure pim register-rate-limit-interval 1970
configure pim register-suppress-interval register-probe-interval 1971
configure pim spt-threshold 1972
configure pim timer vlan 1973
configure pim vlan trusted-gateway 1974
disable dvmrp 1975
disable dvmrp rxmode vlan 1976
disable dvmrp txmode vlan 1977
disable ext-mcast 1978
disable igmp 1979
disable igmp snooping 1980
disable igmp snooping with-proxy 1982
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>disable ipmcforwarding</td>
<td>1983</td>
</tr>
<tr>
<td>disable mcast-queue-mgmt</td>
<td>1984</td>
</tr>
<tr>
<td>disable pim</td>
<td>1985</td>
</tr>
<tr>
<td>disable pim snooping</td>
<td>1986</td>
</tr>
<tr>
<td>enable dvmrp</td>
<td>1987</td>
</tr>
<tr>
<td>enable dvmrp rxmode vlan</td>
<td>1988</td>
</tr>
<tr>
<td>enable dvmrp txmode vlan</td>
<td>1989</td>
</tr>
<tr>
<td>enable ext-mcast</td>
<td>1990</td>
</tr>
<tr>
<td>enable igmp</td>
<td>1991</td>
</tr>
<tr>
<td>enable igmp snooping</td>
<td>1992</td>
</tr>
<tr>
<td>enable igmp snooping with-proxy</td>
<td>1994</td>
</tr>
<tr>
<td>enable ipmcforwarding</td>
<td>1995</td>
</tr>
<tr>
<td>enable mcast-queue-mgmt</td>
<td>1996</td>
</tr>
<tr>
<td>enable pim</td>
<td>1997</td>
</tr>
<tr>
<td>enable pim snooping</td>
<td>1998</td>
</tr>
<tr>
<td>mrcinfo</td>
<td>1999</td>
</tr>
<tr>
<td>mtrace</td>
<td>2001</td>
</tr>
<tr>
<td>run ipmcfdb-check</td>
<td>2003</td>
</tr>
<tr>
<td>show dvmrp</td>
<td>2004</td>
</tr>
<tr>
<td>show igmp group</td>
<td>2005</td>
</tr>
<tr>
<td>show igmp snooping</td>
<td>2006</td>
</tr>
<tr>
<td>show igmp snooping filter</td>
<td>2007</td>
</tr>
<tr>
<td>show igmp snooping static group</td>
<td>2008</td>
</tr>
<tr>
<td>show ipmc cache</td>
<td>2009</td>
</tr>
<tr>
<td>show ipmc fdb</td>
<td>2010</td>
</tr>
<tr>
<td>show l2stats</td>
<td>2011</td>
</tr>
<tr>
<td>show mcast-queue-mgmt</td>
<td>2012</td>
</tr>
<tr>
<td>show mroute</td>
<td>2013</td>
</tr>
<tr>
<td>show pim</td>
<td>2015</td>
</tr>
<tr>
<td>show pim snooping</td>
<td>2016</td>
</tr>
<tr>
<td>unconfigure dvmrp</td>
<td>2017</td>
</tr>
<tr>
<td>unconfigure ext-mcast</td>
<td>2018</td>
</tr>
<tr>
<td>unconfigure igmp</td>
<td>2019</td>
</tr>
<tr>
<td>unconfigure mcast-queue-mgmt</td>
<td>2020</td>
</tr>
</tbody>
</table>
unconfigure pim

Chapter 24  IPX Commands—“f” Series Platforms Only

configure ipxmaxhops
configure ipxrip add vlan
configure ipxrip delete vlan
configure ipxrip vlan delay
configure ipxrip vlan export-filter
configure ipxrip vlan import-filter
configure ipxrip vlan max-packet-size
configure ipxrip vlan trusted-gateway
configure ipxrip vlan update-interval
configure ipxroute add
configure ipxroute delete
configure ipxsap add vlan
configure ipxsap delete vlan
configure ipxsap vlan delay
configure ipxsap vlan export-filter
configure ipxsap vlan import-filter
configure ipxsap vlan max-packet-size
configure ipxsap vlan trusted-gateway
configure ipxsap vlan update-interval
configure ipxsap vlan gns-delay
configure ipxservice add
configure ipxservice delete
configure vlan xnetid
disable ipxrip
disable ipxsap
disable ipxsap gns-reply
disable type20 forwarding
enable ipxrip
enable ipxsap
enable ipxsap gns-reply
enable type20 forwarding
Contents

show ipxconfig 2055
show ipxfdb 2056
show ipxrip 2057
show ipxroute 2058
show ipxsap 2059
show ipxservice 2060
show ipxstats 2061
unconfigure ipxrip 2062
unconfigure ipxsap 2063
unconfigure vlan xnetid 2064
xping 2065

Chapter 25  ARM Commands—BlackDiamond Switch Only

clear accounting counters 2069
configure route-map set accounting-index 1 value 2070
configure route-map set iphost-routing 2072
configure route-map set lpm-routing 2073
disable accounting 2074
disable ipforwarding lpm-routing 2075
disable lpm 2076
enable accounting 2077
enable ipforwarding lpm-routing 2078
enable lpm 2079
show accounting 2080
show lpm 2081

Chapter 26  Remote Connect Commands

clear APmgmt redirect-db history 2084
clear APmgmt unknown-ap history 2085
configure wireless bind 2086
configure wireless device-db 2087
configure wireless ports bind 2088
configure wireless redirect-db 2089
show APmgmt redirect-db history 2090
show APmgmt unknown-ap history 2091
show wireless device-db
show wireless redirect-db

Chapter 27  ATM Commands—BlackDiamond 6800 Series Platforms Only
configure atm add pvc
configure atm delete pvc
configure atm scrambling
show atm
show atm pvc

Chapter 28  PoS Commands—BlackDiamond Switch Only
configure aps
configure aps add
configure aps authenticate
configure aps delete
configure aps force
configure aps lockout
configure aps manual
configure aps timers
configure diffserv dscp-mapping ports
configure dot1q tagmapping ports
configure dot1q tagnesting ports
configure flowstats export add
configure flowstats export delete
configure flowstats filter ports
configure flowstats source ipaddress
configure ports tunnel hdlc
configure ppp ports
configure ppp authentication ports
configure ppp delayed-down-time ports
configure ppp echo ports
configure ppp pos checksum ports
configure ppp pos scrambling ports
configure ppp quality ports
configure ppp user ports
configure qosprofile 2140  
configure red 2142  
configure red min-threshold ports 2144  
configure sonet clocking ports 2145  
configure sonet framing ports 2146  
configure sonet loop 2147  
configure sonet signal label ports 2148  
configure sonet threshold signal degrade ports 2149  
configure sonet threshold signal fail ports 2150  
configure sonet trace path ports 2151  
configure sonet trace section ports 2152  
create account pppuser 2153  
create aps 2154  
delete account pppuser 2155  
delete aps 2156  
disable aps 2157  
disable red ports queue 2158  
enable aps 2159  
enable red ports queue 2160  
show accounts pppuser 2161  
show aps 2162  
show flowstats 2164  
show ppp 2166  
show sonet 2168  
unconfigure aps 2169  
unconfigure diffserv dscp-mapping ports 2170  
unconfigure ppp ports 2172  
unconfigure sonet ports 2173  

Chapter 29  T1, E1, and T3 WAN Commands—Alpine 3800 Series Platforms  
configure multilink add 2176  
configure multilink delete 2177  
configure ports clock source 2178  
configure ports e1 framing 2179
configure ports e1 receivergain
configure ports e1 timeslots
configure ports snmp alert
configure ports t1 cablelength
configure ports t1 fd1
configure ports t1 framing
configure ports t1 lbdetect
configure ports t1 linecoding
configure ports t1 yellow
configure ports t3 cablelength
configure ports t3 framing
configure ppp
configure ppp authentication
configure ppp user
configure qosprofile min-bps
configure qosprofile wanqos maxbuf
configure vlan add multilink
configure vlan delete multilink
configure wanqos egress map dot1p_priority
create account pppuser
create multilink
delete account pppuser
delete multilink
disable multilink
disable ports loopback
disable wanqos
enable multilink
enable ports loopback
enable ports loopback remote
enable ports t1 loopback network payload
enable vman termination
enable wanqos
restart multilink
show accounts pppuser
show multilink 2216
show multilink alarms 2217
show multilink e1 errors 2218
show multilink stats 2219
show multilink t1 errors 2220
show ports alarms 2221
show ports configuration 2222
show ports errors 2223
show ports e1 errors 2224
show ports info 2225
show ports stats 2226
show ppp 2227
show ppp info 2228
unconfigure ppp 2229

Chapter 30  High-Density Gigabit Ethernet Commands—Alpine 3800 and BlackDiamond 6800 Series Only
abort diagnostics cable 2232
configure application examination ports 2233
configure diagnostics cable 2234
configure diffserv ingress replacement ports 2236
configure ports egress-rate-limit 2238
configure qosprofile ingress 2239
configure qostype ingress priority 2241
configure vlan qosprofile ingress 2243
create application examination 2244
delete application examination 2246
disable application examination ports 2247
disable diagnostics cable 2248
disable diffserv ingress replacement ports 2249
disable flow-control ports 2250
enable application examination ports 2251
enable diagnostics cable 2252
enable diffserv ingress replacement ports 2253
enable flow-control ports 2255
Chapter 31  Power Over Ethernet Commands—Summit 300 and 400-24p Switches and Alpine PoE Module

clear inline-power connection-history slot 2275
clear inline-power fault ports 2276
clear inline-power stats
  clear inline-power stats ports 2277
configure inline-power backup-source 2279
configure inline-power budget 2280
configure inline-power detection 2281
configure inline-power disconnect-precedence 2282
configure inline-power display-string
  configure inline-power label ports 2283
configure inline-power operator-limit ports 2285
configure inline-power power-supply 2287
configure inline-power priority 2288
configure inline-power reserved budget 2289
configure inline-power type 2290
configure inline-power usage-threshold 2292
configure inline-power violation-precedence ports 2293
disable inline-power 2295
disable inline-power legacy 2296
disable inline-power ports 2298
disable inline-power slots 2300
download firmware slot 2302
enable inline-power 2303
enable inline-power legacy 2304
enable inline-power ports
enable inline-power slots
reset inline-power ports
reset inline-power slot
show inline-power
show inline-power configuration port
show inline-power configuration slot
show inline-power info
show inline-power info port
show inline-power slot
show inline-power stats ports
show inline-power stats slot
unconfigure inline-power backup-source slot
unconfigure inline-power detection ports
unconfigure inline-power disconnect-precedence
unconfigure inline-power operator-limit ports
unconfigure inline-power power-supply
unconfigure inline-power priority ports
unconfigure inline-power reserved-budget ports
unconfigure inline-power usage-threshold
unconfigure inline-power violation-precedence ports

Chapter 32  LLDP Commands
configure lldp ports management-address
configure lldp ports port-description
configure lldp ports system-capabilities
configure lldp ports system-description
configure lldp ports system-name
configure lldp ports vendor-specific dot1 port-protocol-vlan-ID
configure lldp ports vendor-specific dot1 port-vlan-ID
configure lldp ports vendor-specific dot1 protocol-identity
configure lldp ports vendor-specific dot1 vlan-name
configure lldp ports vendor-specific dot3 link-aggregation
configure lldp ports vendor-specific dot3 mac-phy
configure lldp ports vendor-specific dot3 max-framesize
Chapter 33  H-VPLS Commands—BlackDiamond Switch Only

configure lldp ports vendor-specific dot3 power-via-mdi 2350
configure lldp reinitialize-delay 2351
configure lldp snmp-notification-interval 2352
configure lldp transmit-delay 2353
configure lldp transmit-hold 2354
configure lldp transmit-interval 2355
disable lldp ports 2356
disable snmp traps lldp port 2357
enable lldp ports 2358
enable snmp traps lldp port 2359
show lldp 2360
show lldp neighbor 2362
show lldp port statistics 2364
show lldp ports 2366
show lldp ports neighbor 2368
unconfigure lldp 2370
unconfigure lldp port 2371

clear mpls vpls counters 2374
configure mpls add vpls 2375
configure mpls delete 2377
configure mpls edge-service-mode 2378
configure mpls ldp acl 2379
configure mpls ldp acl add peer 2380
configure mpls ldp acl delete peer 2381
configure mpls vpls add 2382
configure mpls vpls add peer 2384
configure mpls delete vpls 2387
configure mpls health-check add mplsing 2388
configure mpls health-check delete mplsing 2390
configure mpls health-check add vplsing 2391
configure mpls health-check delete vplsing 2393
configure mpls health-check delete vplsing 2394
configure mpls rsvp-te add profile
configure mpls rsvp-te profile
configure mpls tls-tunnel lsp
configure mpls vpls
configure mpls vpls add
configure mpls vpls add peer
configure mpls vpls delete
configure mpls vpls delete peer
configure mpls vpls peer
mplsping
mplstrace
show fdb vpls
show mpls health-check mplsping
show mpls health-check vplsping
show mpls ldp acl
show mpls vpls
show mpls vpls nodes
vplsping
vplstrace

**Chapter 34  MPLS Commands—BlackDiamond Switch Only**

clear mpls vpls counters
configure mpls
configure mpls add vpls
configure mpls add tls-tunnel
configure mpls add vlan
configure mpls delete
configure mpls delete tls-tunnel
configure mpls delete vlan
configure mpls delete vpls
configure mpls edge-service-mode
configure mpls health-check add mplsping
configure mpls health-check delete mplsping
configure mpls health-check add vplsping
configure mpls health-check delete vplsping
configure mpls health-check delete vplsping
configure mpls ldp acl
configure mpls ldp acl add peer
configure mpls ldp acl delete peer
configure mpls ldp advertise
configure mpls ldp advertise vlan
configure mpls php
configure mpls propagate-ip-ttl
configure mpls qos-mapping
configure mpls rsvp-te add lsp
configure mpls rsvp-te add path
configure mpls rsvp-te add profile
configure mpls rsvp-te delete lsp
configure mpls rsvp-te delete path
configure mpls rsvp-te delete profile
configure mpls rsvp-te lsp add path
configure mpls rsvp-te delete path
configure mpls rsvp-te add ero
configure mpls rsvp-te delete ero
configure mpls rsvp-te profile
configure mpls rsvp-te vlan
configure mpls tls-tunnel lsp
configure mpls vlan ip-mtu
configure mpls vlan ldp propagate
configure vlan add track-lsp
configure vlan delete track-lsp
configure mpls vpls
configure mpls vpls add
configure mpls vpls add peer
configure mpls vpls delete
configure mpls vpls delete peer
configure mpls vpls peer
disable mpls
Preface

This preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

Introduction

This guide provides the complete syntax for all the commands available in the currently-supported versions of the ExtremeWare® software running on either modular or stand-alone switches from Extreme Networks®. This also includes commands that support specific modules such as the ARM, MPLS or PoS modules.

This guide is intended for use as a reference by network administrators who are responsible for installing and setting up network equipment. It assumes knowledge of Extreme Networks switch configuration. For conceptual information and guidance on configuring Extreme Networks switches, see the ExtremeWare Software User Guide for your version of the ExtremeWare software.

Terminology

When features, functionality, or operation is specific to a modular or stand-alone switch family, the family name is used. Explanations about features and operations that are the same across all product families simply refer to the product as the “switch.”

Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

Table 1: Notice Icons

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Alerts you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image" alt="Note Icon" /></td>
<td>Note</td>
<td>Important features or instructions.</td>
</tr>
<tr>
<td><img src="image" alt="Caution Icon" /></td>
<td>Caution</td>
<td>Risk of personal injury, system damage, or loss of data.</td>
</tr>
</tbody>
</table>
Table 1: Notice Icons (Continued)

<table>
<thead>
<tr>
<th>Icon</th>
<th>Notice Type</th>
<th>Alerts you to...</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Warning Icon]</td>
<td>Warning</td>
<td>Risk of severe personal injury.</td>
</tr>
</tbody>
</table>

Table 2: Text Conventions

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen displays</td>
<td>This typeface indicates command syntax, or represents information as it appears on the screen.</td>
</tr>
<tr>
<td>The words &quot;enter&quot; and &quot;type&quot;</td>
<td>When you see the word &quot;enter&quot; in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says &quot;type.&quot;</td>
</tr>
<tr>
<td>[Key] names</td>
<td>Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].</td>
</tr>
<tr>
<td>Words in italicized type</td>
<td>Italics emphasize a point or denote new terms at the place where they are defined in the text.</td>
</tr>
</tbody>
</table>

Command Titles

For clarity and brevity, the command titles omit variables, values, and optional arguments. The complete command syntax is displayed directly below the command titles.

Related Publications

The publications related to this one are:

- ExtremeWare release notes
- ExtremeWare User Guide
- Consolidated Hardware Installation Guide

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

http://www.extremenetworks.com/
Using ExtremeWare Publications Online

You can access ExtremeWare publications by downloading them from the Extreme Networks World Wide Web location or from your ExtremeWare product CD. Publications are provided in Adobe® Portable Document Format (PDF). Displaying or printing PDF files requires that your computer be equipped with Adobe® Reader® software, which is available free of charge from Adobe Systems Incorporated.

**NOTE**

If you are using Adobe Reader or Adobe Acrobat® Version 6.0 or later to view PDF files, see “Using Adobe Reader Version 6.0” in this section for important information on making a configuration adjustment to ensure proper viewing and linking of PDF files.

The following two ExtremeWare publications are available as PDF files that are designed to be used online together:

- ExtremeWare 7.4 User Guide
- ExtremeWare 7.4 Command Reference Guide

The user guide PDF file provides links that connect you directly to relevant command information in the command reference guide PDF file. This quick-referencing capability enables you to easily find detailed information in the command reference guide for any command mentioned in the user guide.

To ensure that the quick-referencing feature functions properly, follow these steps:

1. Download both the user guide PDF file and the command reference guide PDF file to the same destination directory on your computer.

2. You may open one or both PDF files to enable cross-referenced linking between the user guide and command reference guide; however, it is recommended that for ease of use, you keep both files open concurrently on your computer desktop. To keep both PDF files open when you activate a cross-reference link, open both PDF files before using the link.

Handling PDF Display Problems

To avoid PDF display problems that can complicate effective cross-referenced linking between the ExtremeWare Software User Guide and the ExtremeWare Software Command Reference Guide, follow the PDF guidelines in this section.

**Opening Both PDF Files Before Using the Links.** If you activate a cross-referencing link from the ExtremeWare Software User Guide PDF file to the ExtremeWare Software Command Reference PDF file when the command reference PDF file is closed (that is, not currently open on your computer desktop), the system will first close the user guide PDF file and then open the command reference PDF file. To keep both PDF files open when you activate a cross-reference link, open both PDF files before using the link.
**Using Adobe Reader Version 6.0.** If you are using Adobe Reader version 6.0 or later, or if you are using Reader embedded in Adobe Acrobat version 6.0 or later, follow these steps to ensure proper concurrent viewing and linking of both the user guide and command reference guide PDF files:

1. Double-click a PDF icon to open the Adobe Reader or Adobe Acrobat window.
   
   You can also open the Adobe Reader or Acrobat window by double-clicking the Reader or Acrobat icon on your desktop or by using the Windows *Start* menu and navigating to the appropriate Adobe program.

2. In the *Edit* pull-down menu, select *Preferences*. The Preferences window will be displayed.

3. In the Preferences window, select the *General* option displayed in the left-hand column in the list of preference options. The General options will be displayed in the Preferences window.

4. In the Miscellaneous area of the Preferences window (shown in the lower section of the Preferences window), deselect the following option:
   
   Open cross-document links in same window
   
   To deselect this option, make sure that the check box next to it is *unchecked*.

5. Click *OK*. 
Introduction
This guide provides details of the command syntax for all ExtremeWare commands as of ExtremeWare version 7.4.0.

**NOTE**
ExtremeWare 7.4.0 supports the “i” series platforms, including the BlackDiamond, Alpine, and Summit “i” series switches. In addition, ExtremeWare supports the “e” series platforms, including the Summit 200, Summit 300, and Summit 400 series switches. Certain commands are available only on selected platforms; these restrictions are noted in the command description.

This guide does not provide feature descriptions, explanations of the technologies, or configuration examples. For information about the various features and technologies supported by Extreme Networks switches, see the installation and user guides for your product. This guide does not replace the installation and user guides; this guide supplements the installation and user guides.

Audience
This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of the following:
- Local area networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- Internet Protocol (IP) concepts
- Routing Information Protocol (RIP) and Open Shortest Path First (OSPF) concepts
- Border Gateway Protocol (BGP-4) concepts (BGP is supported only on the “i” series platforms.)
- IP Multicast concepts
- Distance Vector Multicast Routing Protocol (DVMRP) concepts
• Protocol Independent Multicast (PIM) concepts (PIM dense mode commands are supported only on the “i” series platforms.)
• Internet Packet Exchange (IPX) concepts (IPX-related commands are supported only on the “i” series platforms.)
• Server Load Balancing (SLB) concepts (SLB-related commands are supported only on the “i” series platforms.)
• Simple Network Management Protocol (SNMP)

This guide also assumes that you have read the Installation and User Guide for your product.

Structure of this Guide

This guide documents each ExtremeWare command. Related commands are grouped together and organized into chapters based on their most common usage. The chapters reflect the organization of the ExtremeWare Software User Guide. If a specific command is relevant to a wide variety of functions and could be included in a number of different chapters, we have attempted to place the command in the most logical chapter. Within each chapter, commands appear in alphabetical order. You can use the Index of Commands to locate specific commands if they do not appear where you expect to find them.

NOTE

The ExtremeWare command line interface (CLI) supports only the US character set.

For each command, the following information is provided:

• Command Syntax—The actual syntax of the command. The syntax conventions (the use of braces or curly brackets, for example) are defined in the section “Understanding the Command Syntax” on page 65.
• Description—A brief (one sentence) summary of what the command does.
• Syntax Description—The definition of any keywords and options used in the command.
• Default—The defaults, if any, for this command. The default can be the default action of the command if optional arguments are not provided, or it can be the default state of the switch (such as for an enable/disable command).
• Usage Guidelines—Information to help you use the command. This may include prerequisites, prohibitions, and related commands, as well as other information.
• Example—Examples of the command usage, including output, if relevant.
• History—The version of ExtremeWare in which the command was introduced, and version(s) where it was modified, if appropriate.
• Platform Availability—The platforms on which the command is supported.

NOTE

Commands designated as “available on all platforms” are supported on Summit chipset-based, “i” series, “e” series, and “3” series platforms.
Understanding the Command Syntax

When entering a command at the prompt, be sure that you have the appropriate privilege level. Most configuration commands require you to have the administrator privilege level.

A variety of symbols are shown in this guide as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. Table 3 summarizes command syntax symbols.

Table 3: Command Syntax Symbols

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>angle brackets <code>&lt; &gt;</code></td>
<td>Enclose a variable or value. You must specify the variable or value. For example, in the syntax <code>configure vlan &lt;vlan name&gt; ipaddress &lt;ip_address&gt;</code> you must supply a VLAN name for <code>&lt;vlan name&gt;</code> and an address for <code>&lt;ip_address&gt;</code> when entering the command. Do not type the angle brackets.</td>
</tr>
<tr>
<td>square brackets <code>[ ]</code></td>
<td>Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax `use image [primary</td>
</tr>
<tr>
<td>vertical bar `</td>
<td>`</td>
</tr>
<tr>
<td>braces <code>{ }</code></td>
<td>Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax `reboot {&lt;date&gt; &lt;time&gt;</td>
</tr>
</tbody>
</table>

Command Completion with Syntax Helper

The CLI has a built-in syntax helper. If you are unsure of the complete syntax for a particular command, enter as much of the command as possible and press [Tab]. The syntax helper provides a list of options for the remainder of the command, and places the cursor at the end of the command you have entered so far, ready for the next option.

If the command is one where the next option is a named component, such as a VLAN, access profile, or route map, the syntax helper will also list any currently configured names that might be used as the next option. In situations where this list might be very long, the syntax helper will list only one line of names, followed by an ellipses to indicate that there are more names than can be displayed.

The syntax helper also provides assistance if you have entered an incorrect command.
Abbreviated Syntax

Abbreviated syntax is the shortest unambiguous allowable abbreviation of a command or parameter. Typically, this is the first three letters of the command. If you do not enter enough letters to allow the switch to determine which command you mean, the syntax helper will provide a list of the options based on the portion of the command you have entered.

NOTE

When using abbreviated syntax, you must enter enough characters to make the command unambiguous and distinguishable to the switch.

Names

All named components of the switch configuration must have a unique name. Names must begin with an alphabetical character and are delimited by whitespace, unless enclosed in quotation marks.

Command Shortcuts

All named components of the switch configuration must have a unique name. Components are named using the create command. When you enter a command to configure a named component, you do not need to use the keyword of the component. For example, to create a VLAN, you must enter a unique VLAN name:

create vlan engineering

After you have created the VLAN with a unique name, you can eliminate the keyword vlan from all subsequent commands that require the name to be entered. For example, instead of entering the modular switch command

configure vlan engineering delete port 1:3,4:6

you could enter the following shortcut:

configure engineering delete port 1:3,4:6

Similarly, on a stand-alone switch, instead of entering the command

configure vlan engineering delete port 1-3,6

you could enter the following shortcut:

configure engineering delete port 1-3,6

Modular Switch Numerical Ranges

Commands that require you to enter one or more port numbers on a modular switch use the parameter <portlist> in the syntax. A <portlist> can be one port on a particular slot. For example,

port 3:1

A <portlist> can be a range of numbers. For example,

port 3:1-3:3

You can add additional slot and port numbers to the list, separated by a comma:

port 3:1,4:8,6:10
You can specify all ports on a particular slot. For example,
port 3:*

indicates all ports on slot 3.

You can specify a range of slots and ports. For example,
port 2:3-4:5

indicates slot 2, port 3 through slot 4, port 5.

**Stand-alone Switch Numerical Ranges**

Commands that require you to enter one or more port numbers on a stand-alone switch use the parameter `<portlist>` in the syntax. A portlist can be a range of numbers, for example:

port 1-3

You can add additional port numbers to the list, separated by a comma:

port 1-3,6,8

**Line-Editing Keys**

Table 4 describes the line-editing keys available when you use the CLI.

**Table 4: Line-Editing Keys**

<table>
<thead>
<tr>
<th>Key(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backspace</td>
<td>Deletes character to left of cursor and shifts remainder of line to left.</td>
</tr>
<tr>
<td>Delete or [Ctrl] + D</td>
<td>Deletes character under cursor and shifts remainder of line to left.</td>
</tr>
<tr>
<td>[Ctrl] + K</td>
<td>Deletes characters from under cursor to end of line.</td>
</tr>
<tr>
<td>Insert</td>
<td>Toggles on and off. When toggled on, inserts text and shifts previous text to right.</td>
</tr>
<tr>
<td>Left Arrow</td>
<td>Moves cursor to left.</td>
</tr>
<tr>
<td>Right Arrow</td>
<td>Moves cursor to right.</td>
</tr>
<tr>
<td>Home or [Ctrl] + A</td>
<td>Moves cursor to first character in line.</td>
</tr>
<tr>
<td>End or [Ctrl] + E</td>
<td>Moves cursor to last character in line.</td>
</tr>
<tr>
<td>[Ctrl] + L</td>
<td>Clears screen and moves cursor to beginning of line.</td>
</tr>
<tr>
<td>[Ctrl] + P or Up Arrow</td>
<td>Displays previous command in command history buffer and places cursor at end of command.</td>
</tr>
<tr>
<td>[Ctrl] + N or Down Arrow</td>
<td>Displays next command in command history buffer and places cursor at end of command.</td>
</tr>
<tr>
<td>[Ctrl] + U</td>
<td>Clears all characters typed from cursor to beginning of line.</td>
</tr>
<tr>
<td>[Ctrl] + W</td>
<td>Deletes previous word.</td>
</tr>
</tbody>
</table>
Command History

ExtremeWare “remembers” the last 49 commands you entered. You can display a list of these commands by using the following command:

```
history
```
This chapter describes:

- Commands used for accessing and configuring the switch including how to set up user accounts, passwords, date and time settings, and software licenses
- Commands used for configuring the Domain Name Service (DNS) client
- Commands used for checking basic switch connectivity

ExtremeWare supports the following two levels of management:

- User
- Administrator

A user-level account has viewing access to all manageable parameters, with the exception of:

- User account database
- SNMP community strings

A user-level account can use the `ping` command to test device reachability and change the password assigned to the account name.

An administrator-level account can view and change all switch parameters. It can also add and delete users and change the password associated with any account name. The administrator can disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged on by way of the Telnet connection is notified that the session has been terminated.

The DNS client in ExtremeWare augments certain ExtremeWare commands to accept either IP addresses or host names. For example, DNS can be used during a Telnet session when you are accessing a device or when using the `ping` command to check the connectivity of a device.

The switch offers the following commands for checking basic connectivity:

- `ping`
- `traceroute`

The `ping` command enables you to send Internet Control Message Protocol (ICMP) echo messages to a remote IP device. The `traceroute` command enables you to trace the routed path between the switch and a destination endstation.
clear account lockout

    clear account [all | <name>] lockout

Description
Re-enables an account that has been locked out (disabled) for exceeding the permitted number failed login attempts, which was configured by using the `configure account password-policy lockout-on-login-failures` command.

Syntax Description

<table>
<thead>
<tr>
<th>all</th>
<th>Specifies all users.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies an account name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command applies to sessions at the console port of the switch as well as all other sessions. You can re-enable both user and administrative accounts, once they have been disabled for exceeding the three failed login attempts.

**NOTE**
The default admin account and failsafe accounts are never locked out.

This command only clears the locked-out (or disabled) condition of the account. The action of locking out accounts following the failed login attempts remains until you turn it off by issuing the `configure account [all | <name>] password-policy lockout-on-login-failures off` command.

Example
The following command re-enables the account finance, which had been locked out (disabled) for exceeding three failed login attempts:

    clear account finance lockout

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
clear session

clear session <number>

**Description**
Terminates a Telnet, SSH, NetLogin, or Console session from the switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Specifies a session number from <code>show session</code> output to terminate.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
An administrator-level account can disconnect a management session that has been established by way of a Telnet connection. You can determine the session number of the session you want to terminate by using the `show switch` command. The `show switch` output displays information about current Telnet sessions including:

- The session number
- The login date and time
- The user name
- The type of Telnet session

Depending on the software version running on your switch, additional session information may be displayed. The session number is the first number displayed in the `show session` output.

**Example**
The following command terminates session 4 from the system:

clear session 4

**History**
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure account

configure account <user account> {encrypted} {<password>}

Description
Configures a user account password.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user account</td>
<td>Specifies a user account name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>This option is for use only by the switch when generating an ASCII configuration file. Specifies that the password should be encrypted when the configuration is uploaded to a file. Should not be used through the CLI.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a user password. Supported in ExtremeWare 4.x and ExtremeWare 6.0.x only. In ExtremeWare 6.1 and later, the switch prompts for entry of the password interactively.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You must create a user account before you can configure a user account. Use the create account command to create a user account.

You must have administrator privileges to change passwords for accounts other than your own. User names and passwords are case-sensitive.

The encrypted option is used by the switch when generating an ASCII configuration file (using the upload configuration command), and parsing a switch-generated configuration file (using the download configuration command). Do not select the encrypted option in the CLI.

For ExtremeWare 6.1 and higher:
- The password cannot be specified on the command line. Instead, the switch will interactively prompt you to enter the password, and will then prompt you to reenter the password to verify that you have entered it correctly.

For ExtremeWare 6.0 and higher:
- Passwords must have a minimum of 1 character and can have a maximum of 30 characters.

For ExtremeWare 4.x:
- Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.
**Example**
The following command defines a new password for the account *admin*:

```bash
configure account admin
```

The switch responds with a password prompt:

```
password:
```

Your keystrokes will not be echoed as you enter the new password. After you enter the password, the switch will then prompt you to reenter it.

```
Reenter password:
```

Assuming you enter it successfully a second time, the password is now changed.

In ExtremeWare 4.1.19, the following command defines a new password, *Extreme1*, for the account *admin*:

```bash
configure account admin Extreme1
```

**History**
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure account password-policy char-validation

configure account [all | <name>] password-policy char-validation [none | all-char-groups]

Description
Requires that the user include an upper-case letter, a lower-case letter, a digit, and a symbol in the password.

Syntax Description

<table>
<thead>
<tr>
<th>all</th>
<th>Specifies all users (and future users).</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies an account name.</td>
</tr>
<tr>
<td>none</td>
<td>Resets password to accept all formats.</td>
</tr>
<tr>
<td>all-char-groups</td>
<td>Specifies that the password must contain at least two characters from each of the four groups.</td>
</tr>
</tbody>
</table>

**NOTE:** The password minimum length will be 8 characters if you specify this option.

Default
N/A

Usage Guidelines
This feature is disabled by default.

Once you issue this command, each password must include at least two characters of each of the following four types:

- Upper-case A-Z
- Lower-case a-z
- 0-9
- !, @, #, $, %, ^, *, (, )

The minimum number of characters for these specifically formatted passwords is 8 characters and the maximum is 32 characters.

Use the `none` option to reset the password to accept all formats.

Example
The following command requires all users to use this specified format for all passwords:

```
configure account all password-policy char-validation all-char-groups
```

History
This command was first available in ExtremeWare 7.4.
Platform Availability

This command is available on all platforms.
configure account password-policy history

configure account [all | <name>] password-policy history [<num_passwords> | none]

**Description**

Configures the switch to verify the specified number of previous passwords for the account. The user is prevented from changing the password on a user or administrative account to any of these previously saved passwords.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all accounts (and future users).</td>
</tr>
<tr>
<td>name</td>
<td>Specifies an account name.</td>
</tr>
<tr>
<td>num_passwords</td>
<td>Specifies the number of previous passwords the system verifies for each account. The range is 1 to 10 passwords.</td>
</tr>
<tr>
<td>none</td>
<td>Resets the system to not remember any previous passwords.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Use this command to instruct the system to verify new passwords against a list of all previously used passwords, once an account successfully changes a password. The limit is the number of previous passwords that the system checks against in the record to verify the new password.

If this parameter is configured, the system returns an error message if a user attempts to change the password to one that is saved by the system (up to the configured limit) for that account; this applies to both user and administrative accounts. This also applies to a configured password on the default admin account on the switch.

The limit of previous passwords that the system checks for previous use is configurable from 1 to 10. Using the `none` option disables previous password tracking and returns the system to the default state of no record of previous passwords.

**Example**

The following command instructs the system to verify that the new password has not been used as a password in the previous 5 passwords for the account engineering:

```
configure account engineering password-policy history 5
```

**History**

This command was first available in ExtremeWare 7.4.

**Platform Availability**

This command is available on all platforms.
configure account password-policy lockout-on-login-failures

configure account [all | <name>] password-policy lockout-on-login-failures [on | off]

Description
Disables an account after the user has 3 consecutive failed login attempts.

Syntax Description

| all     | Specifies all users (and future users). |
| name    | Specifies an account name.              |
| on      | Specifies an account name.              |
| off     | Resets the password to never lockout the user. |

Default
N/A

Usage Guidelines
This command applies to sessions at the console port of the switch as well as all other sessions and to user-level and administrator-level accounts. This command locks out the user after three consecutive failed login attempts; the user’s account must be specifically re-enabled by an administrator.

Using the off option resets the account to allow innumerable consecutive failed login attempts, which is the system default. The system default is that three failed consecutive login attempts terminate the particular session, but the user may launch another session; there is no lockout feature by default.

NOTE
The default admin account and failsafe accounts are never locked out, no matter how many consecutive failed login attempts.

Example
The following command enables the account finance for lockout. After three consecutive failed login attempts, the account is subsequently locked out:

configure account finance password-policy lockout-on-login-failures on

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
configure account password-policy maxage

configure account [all | <name>] password-policy maxage [<num_days> | none]

Description
Configures a time limit for the passwords for specified accounts. The passwords for the default admin account and the failsafe account do not age out.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all accounts (and future users).</td>
</tr>
<tr>
<td>name</td>
<td>Specifies an account name.</td>
</tr>
<tr>
<td>num_days</td>
<td>Specifies the length of time that a password can be used. The range is 1 to 365 days.</td>
</tr>
<tr>
<td>none</td>
<td>Resets the password to never expire.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The passwords for the default admin account and the failsafe account never expire.

The time limit is specified in days, from 1 to 365 days. Existing sessions are not closed when the time limit expires; it will not open the next time the user attempts to log in.

When a user logs into an account with an expired password, the system first verifies that the entered password had been valid prior to expiring and then prompts the user to change the password.

NOTE
This is the sole time that a user with a user-level (opposed to an administrator-level) account can make any changes to the user-level account.

Using the none option prevents the password for the specified account from ever expiring (it resets the password to the system default of no time limit).

Example
The following command sets a 3-month time limit for the password for the account marketing:

```
configure account marketing password-policy max-age 90
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
configure account password-policy min-pwd-length

configure account [all | <name>] password-policy min-pwd-length
[<num_characters> | none]

Description
Requires a minimum number of characters for passwords.

Syntax Description

<table>
<thead>
<tr>
<th>all</th>
<th>Specifies all accounts (and future users).</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies an account name.</td>
</tr>
<tr>
<td>num_characters</td>
<td>Specifies the minimum number of characters required for the password. The range is 1 to 32 characters.</td>
</tr>
<tr>
<td>none</td>
<td>Resets password to accept a minimum of 0 characters.</td>
</tr>
</tbody>
</table>

**NOTE:** If you configure the `configure account password-policy char-validation` parameter, the minimum length is 8 characters.

Usage Guidelines

Use this command to configure a minimum length restriction for all passwords for specified accounts. This command affects the minimum allowed length for the next password; the current password is unaffected.

The minimum password length is configurable from 1 to 32 characters. Using the `none` option disables the requirement of minimum password length and returns the system to the default state (password minimum is 0 by default).

**NOTE**

*If the account is configured to require a specific password format, the minimum is 8 characters. See `configure account password-policy char-validation` for more information.*

Example

The following command requires a minimum of 8 letters for the password for the account management:

```
configure account management password-policy min-length 8
```

History

This command was first available in ExtremeWare 7.4.
Platform Availability

This command is available on all platforms.
configure banner

configure banner

Description
Configures the banner string that is displayed at the beginning of each login prompt of each session.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Press [Return] at the beginning of a line to terminate the command and apply the banner. To clear the banner, press [Return] at the beginning of the first line.

For ExtremeWare 6.0 and higher including the “e” series releases:
• You can enter up to 24 rows of 79-column text that is displayed before the login prompt of each session.

For ExtremeWare 2.0 and ExtremeWare 4.x:
• You can enter up to 24 rows of 80-column text that is displayed before the login prompt of each session.

Example
The following command adds a banner, Welcome to the switch, before the login prompt:

    configure banner [Return]
    Welcome to the switch

History
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure banner netlogin

configure banner netlogin

Description
Configures the network login banner that is displayed at the beginning of each login prompt of each session.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
The network login banner and the switch banner cannot be used at the same time. If you configure a Network Login banner, users do not see the normal banner. If no banner is configured, the Extreme logo is displayed. The network login banner displays in HTML. No links or images are supported.

Press [Enter] to enter text on a new line. Press [Enter] twice to finish entering the network login banner. You can enter up to 1024 characters in the banner.

Example
The following command adds the banner “Welcome to your switch” in 8 point purple Arial before the login prompt:
configure banner netlogin [Enter]
<font face="Arial" size=8 color=534579>Welcome to your switch</font>
[Enter]
[Enter]

History
This command was introduced in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure dns-client add

    configure dns-client add <ipaddress>

Description
Add a DNS name server to the available server list for the DNS client.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Up to three DNS name servers can be configured in ExtremeWare versions prior to 6.2.1. In ExtremeWare 6.2.1 and later, eight DNS name servers can be configured.

Example
The following command specifies that the switch use the DNS server 10.1.2.1:

    configure dns-client add 10.1.2.1

History
This command was first available in ExtremeWare 4.0.
This command was modified in ExtremeWare 6.2.1 to support up to eight DNS name servers.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure dns-client add domain-suffix

configure dns-client add domain-suffix <domain_name>

Description
Adds a domain name to the domain suffix list.

Syntax Description

| domain_name       | Specifies a domain name. |

Default
N/A

Usage Guidelines
The domain suffix list can include up to six items. If the use of all previous names fails to resolve a name, the most recently added entry on the domain suffix list will be the last name used during name resolution. This command will not overwrite any exiting entries. If a null string is used as the last suffix in the list, and all other lookups fail, the name resolver will attempt to look up the name with no suffix.

Example
The following command configures a domain name and adds it to the domain suffix list:

```bash
configure dns-client add domain-suffix xyz_inc.com
```

History
This command was first available in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure dns-client add name-server

configure dns-client add name-server <ipaddress>

Description
Adds a DNS name server to the available server list for the DNS client.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Up to three DNS name servers can be configured in ExtremeWare versions prior to 6.2.1. In ExtremeWare 6.2.1 and later, eight DNS name servers can be configured.

Example
The following command specifies that the switch use the DNS server 10.1.2.1:

```bash
configure dns-client add name-server 10.1.2.1
```

History
This command was first available in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure dns-client default-domain

configure dns-client default-domain <domain_name>

Description
Configures the domain that the DNS client uses if a fully qualified domain name is not entered.

Syntax Description

| domain_name | Specifies a default domain name. |

Default
N/A

Usage Guidelines
Sets the DNS client default domain name to domain_name. The default domain name will be used to create a fully qualified host name when a domain name is not specified. For example, if the default default domain name is set to “food.com” then when a command like “ping dog” is entered, the ping will actually be executed as “ping dog.food.com”.

Example
The following command configures the default domain name for the server:

configure dns-client default-domain xyz_inc.com

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure dns-client delete

   configure dns-client delete <ipaddress>

Description
Removes a DNS name server from the available server list for the DNS client.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes a DNS server from the list:
configure dns-client delete 10.1.2.1

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
**configure dns-client delete domain-suffix**

    configure dns-client delete domain-suffix <domain_name>

**Description**
Deletes a domain name from the domain suffix list.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>domain_name</td>
<td>Specifies a domain name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command randomly removes an entry from the domain suffix list. If the deleted item was not the last entry in the list, all items that had been added later are moved up in the list. If no entries in the list match the domain name specified, an error message will be displayed.

**Example**
The following command deletes a domain name from the domain suffix list:

    configure dns-client delete domain-suffix xyz_inc.com

**History**
This command was first available in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure dns-client delete name-server

configure dns-client delete name-server <ipaddress>

Description
Removes a DNS name server from the available server list for the DNS client.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None.

Example
The following command removes a DNS server from the list:
configure dns-client delete name-server 10.1.2.1

History
This command was first available in ExtremeWare 6.2.2.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure idletimeouts

    configure idletimeouts <minutes>

Description
Configures the time-out for idle HTTP, console, and Telnet sessions.

Syntax Description

| minutes | Specifies the time-out interval, in minutes. Range is 1 to 240 (1 minute to 4 hours). |

Default
Default time-out is 20 minutes.

Usage Guidelines
This command configures the length of time the switch will wait before disconnecting idle HTTP, console, or Telnet sessions. The idletimeouts feature must be enabled for this command to have an effect (the idletimeouts feature is disabled by default).

In ExtremeWare v 6.2.0, the time-out interval was specified in seconds, not minutes.

Example
The following command sets the time-out for idle HTTP, login and console sessions to 10 minutes:

    configure idletimeouts 10

History
This command was first available in ExtremeWare 6.2.

This command was modified in ExtremeWare 6.2.1 to change the time-out value specification to minutes.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure time

    configure time <date> <time>

Description
Configures the system date and time.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>Specifies the date in mm/dd/yyyy format.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time in hh:mm:ss format.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The format for the system date and time is as follows:

```
mm/dd/yyyy hh:mm:ss
```

The time uses a 24-hour clock format. The AM hours range from 1 through 11, and the PM hours range from 12 through 23.

For ExtremeWare 7.1e and higher on the “e” series of switches:

- You cannot set the year past 2036.

For ExtremeWare 6.0 and higher on the “i” series of switches:

- You cannot set the year past 2035.

For ExtremeWare 2.0 and 4.x:

- You cannot set the year past 2023.

Example
The following command configures a system date of February 15, 2005 and a system time of 8:42 AM and 55 seconds:

```
configure time 02/15/2005 08:42:55
```

History
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure timezone

configure timezone {name <std_timezone_ID>} <GMT_offset>  
{autodst {name <dst_timezone_ID>} {<dst_offset>}}  
{begins [every <floatingday> | on <absoluteday>] {at <time_of_day>}}  
{ends [every <floatingday> | on <absoluteday>] {at <time_of_day>}}  
| noautodst}

Description

Configures the Greenwich Mean Time (GMT) offset and Daylight Saving Time (DST) preference.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMT_offset</td>
<td>Specifies a Greenwich Mean Time (GMT) offset, in + or - minutes.</td>
</tr>
<tr>
<td>std-timezone-ID</td>
<td>Specifies an optional name for this timezone specification. May be up to six characters in length. The default is an empty string.</td>
</tr>
<tr>
<td>autodst</td>
<td>Enables automatic Daylight Saving Time.</td>
</tr>
<tr>
<td>dst-timezone-ID</td>
<td>Specifies an optional name for this DST specification. May be up to six characters in length. The default is an empty string.</td>
</tr>
<tr>
<td>dst_offset</td>
<td>Specifies an offset from standard time, in minutes. Value is in the range of 1 to 60. Default is 60 minutes.</td>
</tr>
</tbody>
</table>
| floating_day    | Specifies the day, week, and month of the year to begin or end DST each year. Format is:  
                  | <week><day><month> where:  
                  | • <week> is specified as [first | second | third | fourth | last] or 1-5  
                  | • <day> is specified as [sunday | monday | tuesday | wednesday | thursday | friday | saturday] or 1-7 (where 1 is Sunday)  
                  | • <month> is specified as [january | february | march | april | may | june | july | august | september | october | november | december] or 1-12  
                  | Default for beginning is first sunday april; default for ending is last sunday october. |
| absolute_day    | Specifies a specific day of a specific year on which to begin or end DST. Format is:  
                  | <month>/<day>/<year> where:  
                  | • <month> is specified as 1-12  
                  | • <day> is specified as 1-31  
                  | • <year> is specified as 1970 - 2035  
                  | The year must be the same for the begin and end dates. |
| time_of_day     | Specifies the time of day to begin or end Daylight Saving Time. May be specified as an hour (0-23) or as hour:minutes. Default is 2:00. |
| noautodst       | Disables automatic Daylight Saving Time.                                     |

Default

Autodst, beginning every first Sunday in April, and ending every last Sunday in October.
Usage Guidelines

Network Time Protocol (NTP) server updates are distributed using GMT time. To properly display the local time in logs and other timestamp information, the switch should be configured with the appropriate offset to GMT based on geographic location.

The `gmt_offset` is specified in +/- minutes from the GMT time.

Automatic DST changes can be enabled or disabled. The default configuration, where DST begins on the first Sunday in April at 2:00 AM and ends the last Sunday in October at 2:00 AM, applies to most of North America, and can be configured with the following syntax: `configure timezone <gmt_offst> autodst`.

As of ExtremeWare 6.2.1, the starting and ending date and time for DST may be specified, as these vary in time zones around the world.

- Use the `every` keyword to specify a year-after-year repeating set of dates (e.g. the last Sunday in March every year)
- Use the `on` keyword to specify a non-repeating, specific date for the specified year. If you use this option, you will need to specify the command again every year.
- The `begins` specification defaults to every first sunday april.
- The `ends` specification defaults to every last sunday october.
- The `ends` date may occur earlier in the year than the `begins` date. This will be the case for countries in the Southern Hemisphere.
- If you specify only the starting or ending time (not both) the one you leave unspecified will be reset to its default.
- The `time_of_day` specification defaults to 2:00
- The timezone IDs are optional. They are used only in the display of timezone configuration information in the `show switch` command.

To disable automatic DST changes, re-specify the GMT offset using the `noautodst` option: `configure timezone <gmt_offst> noautodst`.

NTP updates are distributed using GMT time. To properly display the local time in logs and other timestamp information, the switch should be configured with the appropriate offset to GMT based on geographical location. Table 5 describes the GMT offsets.

Table 5: Greenwich Mean Time Offsets

<table>
<thead>
<tr>
<th>GMT Offset in Hours</th>
<th>GMT Offset in Minutes</th>
<th>Common Time Zone References</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>+0:00</td>
<td>+0</td>
<td>GMT - Greenwich Mean</td>
<td>London, England; Dublin, Ireland; Edinburgh, Scotland; Lisbon, Portugal; Reykjavik, Iceland; Casablanca, Morocco</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UT or UTC - Universal (Coordinated)</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>WET - Western European</td>
<td></td>
</tr>
<tr>
<td>-1:00</td>
<td>-60</td>
<td>WAT - West Africa</td>
<td>Azores, Cape Verde Islands</td>
</tr>
<tr>
<td>-2:00</td>
<td>-120</td>
<td>AT - Azores</td>
<td>Brasilia, Brazil; Buenos Aires, Argentina; Georgetown, Guyana;</td>
</tr>
<tr>
<td>-3:00</td>
<td>-180</td>
<td></td>
<td></td>
</tr>
<tr>
<td>-4:00</td>
<td>-240</td>
<td>AST - Atlantic Standard</td>
<td>Caracas; La Paz</td>
</tr>
</tbody>
</table>
Table 5: Greenwich Mean Time Offsets (Continued)

<table>
<thead>
<tr>
<th>GMT Offset in Hours</th>
<th>GMT Offset in Minutes</th>
<th>Common Time Zone References</th>
<th>Cities</th>
</tr>
</thead>
<tbody>
<tr>
<td>-5:00</td>
<td>-300</td>
<td>EST - Eastern Standard</td>
<td>Bogota, Columbia; Lima, Peru; New York, NY, Trevor City, MI USA</td>
</tr>
<tr>
<td>-6:00</td>
<td>-360</td>
<td>CST - Central Standard</td>
<td>Mexico City, Mexico</td>
</tr>
<tr>
<td>-7:00</td>
<td>-420</td>
<td>MST - Mountain Standard</td>
<td>Saskatchewan, Canada</td>
</tr>
<tr>
<td>-8:00</td>
<td>-480</td>
<td>PST - Pacific Standard</td>
<td>Los Angeles, CA, Cupertino, CA, Seattle, WA USA</td>
</tr>
<tr>
<td>-9:00</td>
<td>-540</td>
<td>YST - Yukon Standard</td>
<td></td>
</tr>
<tr>
<td>-10:00</td>
<td>-600</td>
<td>AHST - Alaska-Hawaii Standard</td>
<td></td>
</tr>
<tr>
<td>-11:00</td>
<td>-660</td>
<td>NT - Nome</td>
<td></td>
</tr>
<tr>
<td>-12:00</td>
<td>-720</td>
<td>IDLW - International Date Line West</td>
<td></td>
</tr>
<tr>
<td>+1:00</td>
<td>+60</td>
<td>CET - Central European</td>
<td>Paris, France; Berlin, Germany; Amsterdam, The Netherlands; Brussels, Belgium; Vienna, Austria; Madrid, Spain; Rome, Italy; Bern, Switzerland; Stockholm, Sweden; Oslo, Norway</td>
</tr>
<tr>
<td></td>
<td></td>
<td>FWT - French Winter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MET - Middle European</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>MEWT - Middle European Winter</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>SWT - Swedish Winter</td>
<td></td>
</tr>
<tr>
<td>+2:00</td>
<td>+120</td>
<td>EET - Eastern European, Russia Zone 1</td>
<td>Athens, Greece; Helsinki, Finland; Istanbul, Turkey; Jerusalem, Israel; Harare, Zimbabwe</td>
</tr>
<tr>
<td>+3:00</td>
<td>+180</td>
<td>BT - Baghdad, Russia Zone 2</td>
<td>Kuwait; Nairobi, Kenya; Riyadh, Saudi Arabia; Moscow, Russia; Tehran, Iran</td>
</tr>
<tr>
<td>+4:00</td>
<td>+240</td>
<td>ZP4 - Russia Zone 3</td>
<td>Abu Dhabi, UAE; Muscat; Tblisi; Volgograd; Kabul</td>
</tr>
<tr>
<td>+5:00</td>
<td>+300</td>
<td>ZP5 - Russia Zone 4</td>
<td></td>
</tr>
<tr>
<td>+5:30</td>
<td>+330</td>
<td>IST – India Standard Time</td>
<td>New Delhi, Pune, Allahabad, India</td>
</tr>
<tr>
<td>+6:00</td>
<td>+360</td>
<td>ZP6 - Russia Zone 5</td>
<td></td>
</tr>
<tr>
<td>+7:00</td>
<td>+420</td>
<td>WAST - West Australian Standard</td>
<td></td>
</tr>
<tr>
<td>+8:00</td>
<td>+480</td>
<td>CCT - China Coast, Russia Zone 7</td>
<td></td>
</tr>
<tr>
<td>+9:00</td>
<td>+540</td>
<td>JST - Japan Standard, Russia Zone 8</td>
<td></td>
</tr>
<tr>
<td>+10:00</td>
<td>+600</td>
<td>EAST - East Australian Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>GST - Guam Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Russia Zone 9</td>
<td></td>
</tr>
<tr>
<td>+11:00</td>
<td>+660</td>
<td>IDLE - International Date Line East</td>
<td>Wellington, New Zealand; Fiji, Marshall Islands</td>
</tr>
<tr>
<td>+12:00</td>
<td>+720</td>
<td>NZST - New Zealand Standard</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NZT - New Zealand</td>
<td></td>
</tr>
</tbody>
</table>
**Example**

The following command configures GMT offset for Mexico City, Mexico and disables automatic DST:

```bash
configure timezone -360 noautodst
```

The following four commands are equivalent, and configure the GMT offset and automatic DST adjustment for the US Eastern timezone, with an optional timezone ID of EST:

```bash
configure timezone name EST -300 autodst name EDT 60 begins every first sunday april at 2:00 ends every last sunday october at 2:00
configure timezone name EST -300 autodst name EDT 60 begins every 1 1 4 at 2:00 ends every 5 1 10 at 2:00
configure timezone name EST -300 autodst name EDT
configure timezone -300 autodst
```

The following command configures the GMT offset and automatic DST adjustment for the Middle European timezone, with the optional timezone ID of MET:

```bash
configure timezone name MET 60 autodst name MDT begins every last sunday march at 1 ends every last sunday october at 1
```

The following command configures the GMT offset and automatic DST adjustment for New Zealand. The ending date must be configured each year because it occurs on the first Sunday on or after March 5:

```bash
configure timezone name NZST 720 autodst name NZDT 60 begins every first sunday october at 2 ends on 3/16/2002 at 2
```

**History**

This command was first available in ExtremeWare 4.0.

Modified in ExtremeWare 6.2.1 to allow configuration of a beginning and ending time for the automatic DST.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to allow configuration of a beginning and ending time for the automatic DST.

**Platform Availability**

This command is available on all platforms.
create account

create account [admin | user] <username> {encrypted} {<password>}

Description
Creates a new user account.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>Specifies an access level for account type admin.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies an access level for account type user.</td>
</tr>
<tr>
<td>username</td>
<td>Specifies a new user account name. See “Usage Guidelines” for more information.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Specifies an encrypted option.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a user password. See “Usage Guidelines” for more information.</td>
</tr>
</tbody>
</table>

Default

By default, the switch is configured with two accounts with the access levels shown in Table 6:

Table 6: User Account Levels

<table>
<thead>
<tr>
<th>Account Name</th>
<th>Access Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>This user can access and change all manageable parameters. The admin account cannot be deleted.</td>
</tr>
<tr>
<td>user</td>
<td>This user can view (but not change) all manageable parameters, with the following exceptions:</td>
</tr>
<tr>
<td></td>
<td>• This user cannot view the user account database.</td>
</tr>
<tr>
<td></td>
<td>• This user cannot view the SNMP community strings.</td>
</tr>
<tr>
<td></td>
<td>This user has access to the ping command.</td>
</tr>
</tbody>
</table>

You can use the default names (admin and user), or you can create new names and passwords for the accounts. Default accounts do not have passwords assigned to them.

Usage Guidelines

The switch can have a total of 16 user accounts. There must be one administrator account on the system.

You must have administrator privileges to change passwords for accounts other than your own. User names and passwords are case-sensitive.

For ExtremeWare 6.0 and higher:

• User account names must have a minimum of 1 character and can have a maximum of 32 characters.
• Passwords must have a minimum of 0 characters and can have a maximum of 16 characters.

For ExtremeWare 4.x and higher:

• Admin-level users and users with RADIUS command authorization can use the create account command.
For ExtremeWare 4.x:

- User account name specifications are not available.
- Passwords must have a minimum of 4 characters and can have a maximum of 12 characters.
- The encrypted option should only be used by the switch to generate an ASCII configuration (using the `upload configuration` command), and parsing a switch-generated configuration (using the `download configuration` command).

For version 2.0:

- User account name specifications are not available.
- Password specifications are not available.

**Example**

The following command creates a new account named John2 with administrator privileges:

```
create account admin john2
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support the encrypted option. In addition, admin-level users with RADIUS command authorization were allowed to use the `create account` command.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
delete account

    delete account <username>

Description
Deletes a specified user account.

Syntax Description

| username | Specifies a user account name. |

Default
N/A

Usage Guidelines

Use the show accounts command to determine which account you want to delete from the system. The show accounts output displays the following information in a tabular format:

- The user name
- Access information associated with each user
- User login information
- Session information

Depending on the software version running on your switch and the type of switch you have, additional account information may be displayed.

You must have administrator privileges to delete a user account. There must be one administrator account on the system; the command will fail if an attempt is made to delete the last administrator account on the system.

Do not delete the default administrator account. If you do, it is automatically restored, with no password, the next time you download a configuration. To ensure security, change the password on the default account, but do not delete it. The changed password will remain intact through configuration uploads and downloads.

If you must delete the default account, first create another administrator-level account. Remember to manually delete the default account again every time you download a configuration.

Example
The following command deletes account John2:

delete account john2

History
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
disable clipaging

disable clipaging

Description
Disables pausing at the end of each show screen.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
The command line interface (CLI) is designed for use in a VT100 environment. Most show command output will pause when the display reaches the end of a page. This command disables the pause mechanism and allows the display to print continuously to the screen.

NOTE
Press [q] and then press [Return] to force a pause when CLI paging is disabled.

To view the status of CLI paging on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for CLI paging.

Example
The following command disables clipping and allows you to print continuously to the screen:

disable clipaging

History
This command was first available in ExtremeWare 6.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable idletimeouts

disable idletimeouts

Description
Disables the timer that disconnects idle sessions from the switch.

Syntax Description
This command has no arguments or variables.

Default
Enabled. Timeout 20 minutes.

Usage Guidelines
When idle time-outs are disabled, console sessions remain open until the switch is rebooted or you logoff. Telnet sessions remain open until you close the Telnet client.

To view the status of idle time-outs on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for idle time-outs.

Example
The following command disables the timer that disconnects all sessions to the switch:

disable idletimeouts

History
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable clipaging

enable clipaging

Description
Enables the pause mechanism and does not allow the display to print continuously to the screen.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
The command line interface (CLI) is designed for use in a VT100 environment. Most show command output will pause when the display reaches the end of a page.

To view the status of CLI paging on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for CLI paging.

If CLI paging is enabled and you use the show tech-support command to diagnose system technical problems, the CLI paging feature is disabled.

Example
The following command enables clipaging and does not allow the display to print continuously to the screen:

enable clipaging

History
This command was first available in ExtremeWare 6.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable idletimeouts

Description
Enables a timer that disconnects Telnet and console sessions after 20 minutes of inactivity.

Syntax Description
This command has no arguments or variables.

Default
Enabled. Timeout 20 minutes.

Usage Guidelines
You can use this command to ensure that a Telnet, HTTP, or console session is disconnected if it has been idle for the required length of time. This ensures that there are no hanging connections.

To view the status of idle time-outs on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for idle time-outs.

In ExtremeWare 6.2 or later, you can configure the length of the time-out interval.

Example
The following command enables a timer that disconnects any Telnet, HTTP, and console sessions after 20 minutes of inactivity:

```
enable idletimeouts
```

History
This command was first available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable license

For the “i” series switches:

    enable license [basic_L3 | advanced_L3 | full_L3 ] <license_key>

For the “e” series switches:

    enable license [advanced-edge] <license_key>

Description
Enables a particular software feature license.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>basic_L3</td>
<td>Specifies a basic L3 license.</td>
</tr>
<tr>
<td>advanced_L3</td>
<td>Specifies an advanced L3 license.</td>
</tr>
<tr>
<td>full_L3</td>
<td>Specifies a full L3 license.</td>
</tr>
<tr>
<td>license_key</td>
<td>Specifies your software license key.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Specify license_key as an integer.

The unconfigure switch all command does not clear licensing information. This feature cannot be disabled after the license has been enabled on the switch.

Depending on the software version running on your switch, and the type of switch you have, only the license parameters applicable to your software or switch can be used.

To view the type of license you are currently running on the switch, use the show switch command. The license key number is not displayed, but the type of license is displayed in the show switch output. The type of license is displayed after the system name, system location, system contact, and system MAC address.

Example
The following command enables a full L3 license on the switch:

    enable license fullL3

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
history

Description
Displays a list of the previous 49 commands entered on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
ExtremeWare “remembers” the last 49 commands you entered on the switch. Use the history command to display a list of these commands.

Example
The following command displays the previous 49 commands entered on the switch:
history

History
This command was first available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
reboot

For the “i” series switches:

```
reboot {time <date> <time> | cancel} {slot <slot number> | msm-a | msm-b}
```

For the “e” series switches:

```
reboot {time <date> <time> | cancel}{slot <slot number>}
```

**Description**
Reboots the switch or the module in the specified slot at a specified date and time.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>date</td>
<td>Specifies a reboot date in <code>mm/dd/yyyy</code> format.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies a reboot time in <code>hh:mm:ss</code> format.</td>
</tr>
<tr>
<td>cancel</td>
<td>Cancels a previously scheduled reboot.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot where the module is installed on the “i” series of switches.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies a BlackDiamond MSM module installed in slot A.</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies a BlackDiamond MSM module installed in slot B.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
If you do not specify a reboot time, the switch will reboot immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the `cancel` option.

**On the “i” Series of Switches.** The `slot <slot number>` option is added to the command to make it possible to reboot a module in a specific slot. When you specify this option, the command applies to the module in the specified slot, rather than to the switch. In general, the modules that can be rebooted have separate images from the ExtremeWare image for the switch.

The modules that can be rebooted are: E1, T1, T3, ARM, ATM, MPLS, PoS, and slave or switch fabric MSM modules.

**NOTE**
When you configure a timed reboot of an MSM, there is no show output in the CLI to view the configuration.
The E1, T1, and T3 `reboot slot` command does not support the `time` or `cancel` keywords, so this command can only be executed immediately.

Example
The following command reboots the switch at 8:00 AM on April 15, 2002:
`reboot 04/15/2002 08:00:00`

On the “i” series of switches, the following command reboots the MPLS module in slot number 5. It would also reboot the fifth switch in a stack of switches on the “e” series of switches:
`reboot time 10/04/2001 10,46,00 slot 5`

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 7.0.0 to include the `slot` option.

This command was modified in ExtremeWare 7.1.0 to include the `msm-a` and `msm-b` options.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.4 to support the slot option on the “e” series of switches.

Platform Availability
This command is available on all platforms.
show accounts password-policy

Description
Displays password policy information for all users on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
To view the password management information, you must have administrator privileges.

The `show accounts password-policy` command displays the following information in a tabular format:

- Global password management parameters applied to new accounts upon creation:
  - Maximum age—The maximum number of days for the passwords to remain valid.
  - History limit—The number of previous password that the switch scans prior to validating a new password.
  - Minimum length—The minimum number of characters in passwords.
  - Character validation—The passwords must be in the specific format required by the `configure account password-policy char-validation` command.
  - Lockout on login failures—If enabled, the system locks out users after 3 failed login attempts.
  - Accounts locked out—Number of accounts locked out.
- **User Name**—The name of the user. This list displays all of the users who have access to the switch.
- **Password Expiry Date**—Date the password for this account expires; may be blank.
- **Password Max. age**—The number of days originally allowed to passwords on this account; may show None.
- **Password Min. length**—The minimum number of characters required for passwords on this account; may show None.
- **Password History Limit**—The number of previous passwords the system scans to disallow duplication on this account; may show None.

Example
The following command displays the password management parameters configured for each account on the switch:

`show accounts password-policy`
Output from this command looks similar to the following:

```
Accounts global configuration(applied to new accounts on creation)

<table>
<thead>
<tr>
<th>Password Max. age</th>
<th>: None</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password History limit</td>
<td>: None</td>
</tr>
<tr>
<td>Password Min. length</td>
<td>: None</td>
</tr>
<tr>
<td>Password Character Validation</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Accts. lockout on login failures</td>
<td>: Disabled</td>
</tr>
<tr>
<td>Accounts locked out</td>
<td>: No</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>User Name</th>
<th>Password Expiry</th>
<th>Max. age</th>
<th>Min. len</th>
<th>History Limit</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>user</td>
<td>None</td>
<td>None</td>
<td>None</td>
<td>None</td>
</tr>
<tr>
<td>test</td>
<td>Apr-17-2005</td>
<td>12</td>
<td>32</td>
<td>9</td>
</tr>
</tbody>
</table>

Flags: (C) Password character validation enabled, (L) Account locked out
(l) Account lockout on login failures enabled
```

**History**

This command was first available in ExtremeWare 7.4.

**Platform Availability**

This command is available on all platforms.
show accounts pppuser

Description
Displays user account information for all users on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
You need to create a user account using the create account command before you can display user account information.

To view the accounts that have been created, you must have administrator privileges.

The show accounts command displays the following information in a tabular format:

- **User Name**—The name of the user. This list displays all of the users who have access to the switch.
- **Access**—The SNMP community strings. This may be listed as R/W for read/write or RO for read only.
- **Login OK**—The number of logins that are okay.
- **Failed**—The number of failed logins.

Depending on the software version running on your switch, additional or different account information may be displayed.

Example
The following command displays user account information on the switch:

```
show accounts pppuser
```

Output from this command looks similar to the following:

<table>
<thead>
<tr>
<th>User Name</th>
<th>Access</th>
<th>LoginOK</th>
<th>Failed</th>
<th>PPPUser</th>
</tr>
</thead>
<tbody>
<tr>
<td>admin</td>
<td>R/W</td>
<td>3</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>user</td>
<td>RO</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>dbackman</td>
<td>R/W</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ron</td>
<td>RO</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>nocteam</td>
<td>RO</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 2.0.
Platform Availability

This command is only available on the “i” series of switches.
show banner

Usage Guidelines
Use this command to view the banner that is displayed before the login prompt.

Example
The following command displays the switch banner:
show banner

Output from this command looks similar to the following:
Extreme Networks Summit48i Layer 3 Switch
#########################################################
Unauthorized Access is strictly prohibited.
Violators will be prosecuted.
#########################################################

History
This command was first available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show dns-client

show dns-client

**Description**
Displays the DNS configuration.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A

**Usage Guidelines**
None.

**Example**
The following command displays the DNS configuration:
show dns-client

Output from this command looks similar to the following:

Number of domain suffixes: 2
Domain Suffix 1: njudah.local
Domain Suffix 2: dbackman.com
Number of name servers: 2
Name Server 1: 172.17.1.104
Name Server 2: 172.17.1.123

**History**
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show esrp-aware

    show esrp-aware [vlan <vlan name>]

Description
Displays ESRP awareness information.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Without the vlan option, the show command displays all VLAN interfaces receiving ESRP packets.

Usage Guidelines
The VLANs associated with the ports connecting an ESRP-aware switch to an ESRP-enabled switch must be configured using an 802.1Q tag on the connecting port, or, if only a single VLAN is involved, as untagged.

Example
The following command displays ESRP awareness information for a VLAN named esrpEn.

* Summit400-48t:8 # show esrp-aware vlan "esrpEn"

The output of the command is similar to the following:

VLAN Interface: [esrpEn]. DisableLearnTimeout=0 secs, Total-Fdb-Flushes=0
    Esrp-Group:0  Esrp-Master-Mac=00:04:96:14:46:90,  Age=1 secs

History
This command was first available in ExtremeWare 7.2e.

Platform Availability
This command is only available on the “e” series platform of switches.
show switch

show switch

Description
Displays the current switch information.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

The show switch command displays:
- sysName, sysLocation, sysContact
- MAC address
- License type
- System mode
- Recovery mode
- Transceiver diagnostics
- Watchdog state
- Reboot loop information
- Current date, time, system boot time, and time zone configuration
- Configuration modified information
- Any scheduled reboot information
- Scheduled upload/download information
- Operating environment (temperature, fans, and power supply status)
- Software image information (primary/secondary image, date/time, version)
- NVRAM configuration information (primary/secondary configuration, date/time, size, version)
- PACE configuration information
- Software licensing information

On the “i” series of switches, the command also displays:
- Diagnostics mode (BlackDiamond switch only)
- RED configuration
show switch

- DLCS state
- Backplane load sharing (BlackDiamond switch only)
- System health check
- FDB-scan diagnostics
- MSM failover information (BlackDiamond switch only)
- MSM information (BlackDiamond switch only)
- Mode of switch operation (Alpine 3802 only)
- Default configuration mode (standard or enhanced)

This information may be useful for your technical support representative if you have a problem.

Depending on the software version running on your switch, additional or different switch information may be displayed.

**Example**

The following command displays current switch information:

```
show switch
```

Output from this command looks similar to the following:

```
SysName:          Alpine3804
SysLocation:      Extreme Networks HQ
SysContact:       Carlos_Beronio
System MAC:       00:01:30:23:C1:00
License:          Full L3
System Mode:      802.1Q EtherType is 8100 (Hex).   CPU Tx-Priority = High
RED Probability:  0
DLCS:             Enabled
SysHealth Check:  Enabled.   Alarm Level = Log
Recovery Mode:    All - System-dump/Reboot
Transceiver Diag: Enabled.    Failure action:  log only
Fdb-Scan Diag:    Enabled.    Failure action:  log only
System Watchdog:  Enabled
Reboot Loop Prot: Disabled
Timezone:         [Auto DST Enabled] GMT Offset: 0 minutes, name is GMT.
                  DST of 60 minutes is currently not in effect, name is not set.
                  DST begins every first Sunday April at 2:00
                  DST ends every last Sunday October at 2:00
Config Modified:  Mon Jun 9 15:09:44 2003
Next Reboot:      None scheduled
Timed Upload:     None scheduled
Timed Download:   None scheduled
Temperature:      Normal.    All fans are operational.
Power supply:     Upper (PSU-A) not present,   Lower (PSU-B) OK
Image Selected:   Primary
```
Image Booted: Primary

Primary EW Ver: 7.0.0b61 [unknown-ssh]
Secondary EW Ver: 7.1.0b34 [non-ssh]

<table>
<thead>
<tr>
<th>Module</th>
<th>Image Selected</th>
<th>Image Booted</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMM</td>
<td>Secondary</td>
<td>Secondary</td>
</tr>
<tr>
<td>Slot 2 (WM4T1)</td>
<td>Secondary</td>
<td>Secondary</td>
</tr>
</tbody>
</table>

Config Selected: Primary
Config Booted: Primary
Primary Config: Created by EW Version:
7.1.0 Build 34 [38]
7928 bytes saved on Wed Jun 4 11:54:03 2003
Secondary Config: Created by EW Version:
6.2.2 Build 56 [38]
2900 bytes saved on Thu Jan 30 04:21:10 2003

The same example run on an “e” series switch would have the following output:

* Summit400-48t:2 # show switch

SysName: Summit400-48t
SysLocation: 
SysContact: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:04:96:18:40:AF
License: Advanced Edge
System Mode: 802.1Q EtherType is 8100 (Hex).
Recovery Mode: None
System Watchdog: Enabled
Reboot Loop Prot: Disabled
Current Time: Mon Jun 14 16:26:10 2055
Timezone: [Auto DST Enabled] GMT Offset: 0 minutes, name is GMT. DST of 60 minutes is currently in effect, name is not set. DST begins every first Sunday April at 2:00 DST ends every last Sunday October at 2:00
Boot Time: Mon Jun 14 16:19:20 2055
Config Modified: Thu Jan 1 00:00:00 1970
Next Reboot: None scheduled
Timed Upload: None scheduled
Timed Download: None scheduled
Temperature: Normal. All fans are operational.
Power supply: Internal power supply OK, External power supply not present.

Primary EW Ver: 7.2e.0b28 beta.s400-r28 [non-ssh]
Secondary EW Ver: 7.2e.0b27 beta.s400-r27 [non-ssh]
Image Selected: Primary
Image Booted: Primary
Config Selected: Secondary
Config Booted: Secondary
Primary Config: Created by EW Version:
show switch

7.2e.0 Build 26 [46]
5990 bytes saved on Wed Jan 12 15:54:31 2056
Secondary Config: Empty

* Summit400-48t:3 #

History
This command was first available in ExtremeWare 2.0.
This command was modified in ExtremeWare 6.1.8 to display the mode of switch operation—extended, standard, or auto—for the Alpine 3802.
This command was modified in ExtremeWare 7.0.0.
This command was added to the “e” series of switches in ExtremWare 7.1e.
This command was modified in ExtremeWare 7.3.0 to add an indicator for default configuration mode (standard or enhanced).

Platform Availability
This command is available on all platforms.
tracert

Usage:
```
tracert <host name | ip_address> {from <source IP address>} {ttl <number>} {port <port number>}
```

**Description**
Enables you to trace the routed path between the switch and a destination endstation.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host name</td>
<td>Specifies the hostname of the destination endstation.</td>
</tr>
<tr>
<td>ip_address</td>
<td>Specifies the IP address of the destination endstation.</td>
</tr>
<tr>
<td>from &lt;source IP address&gt;</td>
<td>Uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used. (6.1 and higher)</td>
</tr>
<tr>
<td>ttl &lt;number&gt;</td>
<td>Configures the switch to trace up to the time-to-live number of the switch. (6.1 and higher)</td>
</tr>
<tr>
<td>port &lt;port number&gt;</td>
<td>Specifies the UDP port number. (6.1 and higher)</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
To use the **host name** parameter, you must first configure DNS.

Each router along the path is displayed.

**Example**
The following command enables the tracert function to a destination of 123.45.67.8:
```
tracert 123.45.67.8
```

**History**
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support the **hostname** parameter.

This command was modified in ExtremeWare 6.1 to support the **from**, ttl, and port parameters.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
This chapter describes:

- Commands for configuring Simple Network Management Protocol (SNMP) parameters on the switch
- Commands for managing the switch using Telnet and web access
- Commands for configuring Simple Network Time Protocol (SNTP) parameters on the switch

SNMP

Any network manager running the Simple Network Management Protocol (SNMP) can manage the switch, if the Management Information Base (MIB) is installed correctly on the management station. Each network manager provides its own user interface to the management facilities.

The following SNMP parameters can be configured on the switch:

- **Authorized trap receivers**—An authorized trap receiver can be one or more network management stations on your network. The switch sends SNMP traps to all trap receivers. Entries in this list can be created, modified, and deleted using the RMON2 trapDestTable MIB variable, as described in RFC 2021.
- **Authorized managers**—An authorized manager can be either a single network management station, or a range of addresses (for example, a complete subnet) specified by a prefix and a mask. The switch can have a maximum of eight authorized managers.
- **Community strings**—The community strings allow a simple method of authentication between the switch and the remote Network Manager. The default read-only community string is `public`. The default read-write community string is `private`. The community strings for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps.
- **System contact (optional)**—The system contact is a text field that enables you to enter the name of the person(s) responsible for managing the switch.
- **System name**—The system name is the name that you have assigned to this switch. The default name is the model name of the switch (for example, Summit1).
- **System location (optional)**—Using the system location field, you can enter an optional location for this switch.
The following can also be configured on the switch for version 6.0 and higher:

- **SNMP read access**—The ability to read SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.
- **SNMP read/write access**—The ability to read and write SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.

**Telnet**

Telnet allows you to access the switch remotely using TCP/IP through one of the switch ports or a workstation with a Telnet facility. If you access the switch via Telnet, you will use the command line interface (CLI) to manage the switch and modify switch configurations.

**Simple Network Time Protocol**

ExtremeWare supports the client portion of the Simple Network Time Protocol (SNTP) Version 3 based on RFC1769. SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. When enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean time (GMT) offset and the use of Daylight Saving Time. These features have been tested for year 2000 compliance.

**ExtremeWare Vista**

ExtremeWare Vista is a device management software running in the switch that allows you to access the switch over a TCP/IP network using a standard web browser. ExtremeWare Vista provides a subset of the CLI commands available for configuring and monitoring the switch. If a particular command is not available using ExtremeWare Vista, you must use the CLI to access the desired functionality.
configure snmp access-profile readonly

configure snmp access-profile readonly [<access-profile> | none]

Description
Assigns an access profile that limits which stations have read-only access to the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-profile</td>
<td>Specifies a user defined access profile.</td>
</tr>
<tr>
<td>none</td>
<td>Cancels a previously configured access profile.</td>
</tr>
</tbody>
</table>

Default
All users have access until an access profile is created and specified.

Usage Guidelines
The ability to read SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.

You must create and configure an access profile before you can use this command. You create an access profile using the `create access-profile type` command. You configure an access profile using the `configure access-profile` command.

Use the `none` option to remove a previously configured access profile.

Read community strings provide read-only access to the switch. The default read-only community string is public. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 32 characters.

To view the SNMP read-only access communities configured on the switch, use the `show management` command. The `show management` command displays information about the switch including the encrypted names and the number of read-only communities configured on the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp access-profile readonly` command, use the `unconfigure management` command.

Example
The following command allows the user defined access profile `admin` read-only access to the switch:
`configure snmp access-profile readonly admin`

History
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in 7.2e.
Platform Availability

This command is available on all platforms.
configure snmp access-profile readwrite

configure snmp access-profile readwrite [access-profile | none]

**Description**
Assigns an access profile that limits which stations have read/write access to the switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access-profile</td>
<td>Specifies a user defined access profile.</td>
</tr>
<tr>
<td>none</td>
<td>Cancels a previously configured access profile.</td>
</tr>
</tbody>
</table>

**Default**
All users have access until an access profile is specified.

**Usage Guidelines**
The ability to read SNMP information can be restricted through the use of an access profile. An access profile permits or denies a named list of IP addresses and subnet masks.

You must create and configure an access profile before you can use this command. You create an access profile using the `create access-profile type` command. You configure an access profile using the `configure access-profile` command.

Use the `none` option to remove a previously configured access profile.

Read/write community strings provide read and write access to the switch. The default read/write community string is `private`. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 32 characters.

To view the SNMP read/write access communities configured on the switch, use the `show management` command. The `show management` command displays information about the switch including the names and the number of read/write communities configured on the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp access-profile readwrite` command, use the `unconfigure management` command.

**Example**
The following command allows the user defined access profile `management` read/write access to the switch:

```
configure snmp access-profile readwrite management
```

**History**
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in 7.2e.

**Platform Availability**

This command is available on all platforms.
configure snmp add community

configure snmp add community [readonly | readwrite] {encrypted}
<alphanumeric string>

Description
Adds an SNMP read or read/write community string.

Syntax Description

<table>
<thead>
<tr>
<th>readonly</th>
<th>Specifies read-only access to the system.</th>
</tr>
</thead>
<tbody>
<tr>
<td>readwrite</td>
<td>Specifies read and write access to the system.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Specifies encryption, for use only by the switch when uploading or downloading a configuration. Should not be used through the CLI.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies an SNMP community string name. See “Usage Guidelines” for more information.</td>
</tr>
</tbody>
</table>

Default
The default read-only community string is public. The default read/write community string is private.

Usage Guidelines
Community strings provide a simple method of authentication between a switch and a remote network manager. Read community strings provide read-only access to the switch. The default read-only community string is public. Read-write community strings provide read and write access to the switch. The default read/write community string is private.

An authorized trap receiver must be configured to use the correct community strings on the switch for the trap receiver to receive switch-generated traps. In some cases, it may be useful to allow multiple community strings so that all switches and trap receivers are not forced to use identical community strings. The configure snmp add community command allows you to add multiple community strings in addition to the default community string.

An SNMP community string can contain up to 32 characters.

To change the value of the default read/write and read-only community strings, use the configure snmp community command.

The encrypted option is intended for use by the switch when generating an ASCII configuration file (using the upload configuration command), or parsing a switch-generated configuration (using the download configuration command). Do not select the encrypted option in the CLI.

For version 6.0 and 6.1:
• A total of eight community strings can be configured on the switch.

For version 4.x:
• SNMP community strings can contain up to 126 characters.

For version 2.0:
• The `add` parameter is included in the command syntax. It is available only in version 2.0.
• SNMP community strings can contain up to 127 characters.

**Example**
The following command adds a read/write community string with the value `extreme`:
```
configure snmp add community readwrite extreme
```

**History**
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in 7.1e.
This command was modified in ExtremeWare 7.2e to add support for encryption.

**Platform Availability**
This command is available on all platforms.
configure snmp add trapreceiver

On the “i” series of switches:

```bash
configure snmp add trapreceiver <ip address> {port <number>} community {<hex value>} <community string> {from <source ip address>} {mode [enhanced | standard]} trap-group {auth-traps{},} {bgp-traps{},} {extreme-traps{},}
{link-up-down-traps{},} {ospf-traps{},} {ping-traceroute-traps{},}
{rmon-traps{},} {security-traps{},} {smart-traps{},} {stp-traps{},}
{system-traps{},} {vrrp-traps{,}}
```

On the “e” series of switches:

```bash
configure snmp add trapreceiver <ip address> {port <number>} community {hex <hex value>} <community string> {from <source ip address>} {mode [enhanced | standard]} trap-group {auth-traps{},} {extreme-traps{},}
{link-up-down-traps{},} {ospf-traps{},} {ping-traceroute-traps{},}
{rmon-traps{},} {security-traps{},} {smart-traps{},} {stp-traps{},}
{system-traps{},} {vrrp-traps{,}}
```

**Description**

Adds the IP address of a trap receiver to the trap receiver list and specifies which SNMPv1/v2c traps are to be sent.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an SNMP trap receiver IP address.</td>
</tr>
<tr>
<td>port &lt;number&gt;</td>
<td>Specifies a UDP port to which the trap should be sent. Default is 162.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>community string</td>
<td>Specifies the community string of the trap receiver.</td>
</tr>
<tr>
<td>source ip address</td>
<td>Specifies the IP address of a VLAN to be used as the source address for the trap</td>
</tr>
<tr>
<td>enhanced</td>
<td>Specifies enhanced traps, which contain extra varbinds at the end.</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies standard traps, which do not constrain the extra varbinds.</td>
</tr>
<tr>
<td>auth-traps</td>
<td>Specifies that authentication traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>bgp-traps</td>
<td>Specifies that BGP traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>extreme-traps</td>
<td>Specifies that Extreme Networks specific traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>link-up-down-traps</td>
<td>Specifies that link state traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>ospf-traps</td>
<td>Specifies that OSPF traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>ping-traceroute-traps</td>
<td>Specifies that ping and traceroute traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>rmon-traps</td>
<td>Specifies that RMON traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>security-traps</td>
<td>Specifies that security traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>smart-traps</td>
<td>Specifies that Extreme Networks smart traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>stp-traps</td>
<td>Specifies that STP traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>system-traps</td>
<td>Specifies that system traps will be sent to the trap receiver.</td>
</tr>
<tr>
<td>vrrp-traps</td>
<td>Specifies that VRRP traps will be sent to the trap receiver.</td>
</tr>
</tbody>
</table>
Default

Trap receivers are in enhanced mode by default, and the version is SNMPv2c by default.

Usage Guidelines

The IP address can be unicast, multicast, or broadcast.

An authorized trap receiver can be one or more network management stations on your network. Authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. The switch sends SNMP traps to all trap receivers configured to receive the specific trap group. If no trap groups are specified, all traps will be sent to the receiver. Entries in this list can be created, modified, and deleted using the RMON2 trapDestTable MIB variable, as described in RFC 2021.

Table 7 lists the currently defined SNMP trap groups. From time to time, new trap groups may be added to this command.

Table 7: SNMP Trap Groups

<table>
<thead>
<tr>
<th>Trap Group</th>
<th>Notifications</th>
<th>MIB Subtree</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp-traps</td>
<td>newRoot</td>
<td>dot1dBridge, 1.3.6.1.2.1.17</td>
</tr>
<tr>
<td></td>
<td>topologyChange</td>
<td></td>
</tr>
<tr>
<td>bgp-traps</td>
<td>bgpEstablished</td>
<td>bgpTraps, 1.3.6.1.2.1.15.7</td>
</tr>
<tr>
<td></td>
<td>bgpBackwardTransition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extremeBgpPrefixReachedThreshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extremeBgpPrefixMaxExceeded</td>
<td></td>
</tr>
<tr>
<td>ospf-traps</td>
<td>ospfIfStateChange</td>
<td>ospfTraps, 1.3.6.1.2.1.14.16.2</td>
</tr>
<tr>
<td></td>
<td>ospfIfStateChange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfNbrStateChange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfNbrStateChange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfConfigError</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfConfigError</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfAuthFailure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfAuthFailure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfRxBadPacket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfRxBadPacket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfTxRetransmit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfTxRetransmit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfOriginLsa</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfMaxAgeLsa</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfLsdbOverflow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfLsdbApproachingOverflow</td>
<td></td>
</tr>
<tr>
<td>ping-traceroute-traps</td>
<td>pingTestFailed</td>
<td>pingNotifications, 1.3.6.1.2.1.80.0</td>
</tr>
<tr>
<td></td>
<td>pingTestCompleted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tracerouteTestFailed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tracerouteTestCompleted</td>
<td></td>
</tr>
<tr>
<td>vrrp-traps</td>
<td>vrrpTrapNewMaster</td>
<td>vrrpNotifications, 1.3.6.1.2.1.68.0</td>
</tr>
<tr>
<td></td>
<td>vrrpTrapAuthFailure</td>
<td></td>
</tr>
</tbody>
</table>

Table 7: SNMP Trap Groups

<table>
<thead>
<tr>
<th>Trap Group</th>
<th>Notifications</th>
<th>MIB Subtree</th>
</tr>
</thead>
<tbody>
<tr>
<td>stp-traps</td>
<td>newRoot</td>
<td>dot1dBridge, 1.3.6.1.2.1.17</td>
</tr>
<tr>
<td></td>
<td>topologyChange</td>
<td></td>
</tr>
<tr>
<td>bgp-traps</td>
<td>bgpEstablished</td>
<td>bgpTraps, 1.3.6.1.2.1.15.7</td>
</tr>
<tr>
<td></td>
<td>bgpBackwardTransition</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extremeBgpPrefixReachedThreshold</td>
<td></td>
</tr>
<tr>
<td></td>
<td>extremeBgpPrefixMaxExceeded</td>
<td></td>
</tr>
<tr>
<td>ospf-traps</td>
<td>ospfIfStateChange</td>
<td>ospfTraps, 1.3.6.1.2.1.14.16.2</td>
</tr>
<tr>
<td></td>
<td>ospfIfStateChange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfNbrStateChange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfNbrStateChange</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfConfigError</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfConfigError</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfAuthFailure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfAuthFailure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfRxBadPacket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfIfRxBadPacket</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfTxRetransmit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfTxRetransmit</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfOriginLsa</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfMaxAgeLsa</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfLsdbOverflow</td>
<td></td>
</tr>
<tr>
<td></td>
<td>ospfLsdbApproachingOverflow</td>
<td></td>
</tr>
<tr>
<td>ping-traceroute-traps</td>
<td>pingTestFailed</td>
<td>pingNotifications, 1.3.6.1.2.1.80.0</td>
</tr>
<tr>
<td></td>
<td>pingTestCompleted</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tracerouteTestFailed</td>
<td></td>
</tr>
<tr>
<td></td>
<td>tracerouteTestCompleted</td>
<td></td>
</tr>
<tr>
<td>vrrp-traps</td>
<td>vrrpTrapNewMaster</td>
<td>vrrpNotifications, 1.3.6.1.2.1.68.0</td>
</tr>
<tr>
<td></td>
<td>vrrpTrapAuthFailure</td>
<td></td>
</tr>
</tbody>
</table>
configure snmp add trapreceiver

Table 7: SNMP Trap Groups (Continued)

<table>
<thead>
<tr>
<th>Trap Group</th>
<th>Notifications</th>
<th>MIB Subtree</th>
</tr>
</thead>
<tbody>
<tr>
<td>system-traps</td>
<td>extremeOverheat</td>
<td>1.3.6.1.4.1.1916.0.6</td>
</tr>
<tr>
<td></td>
<td>extremeFanFailed</td>
<td>1.3.6.1.4.1.1916.0.7</td>
</tr>
<tr>
<td></td>
<td>extremeFanOK</td>
<td>1.3.6.1.4.1.1916.0.8</td>
</tr>
<tr>
<td></td>
<td>extremePowerSupplyFail</td>
<td>1.3.6.1.4.1.1916.0.10</td>
</tr>
<tr>
<td></td>
<td>extremePowerSupplyGood</td>
<td>1.3.6.1.4.1.1916.0.11</td>
</tr>
<tr>
<td></td>
<td>extremeModuleStateChange</td>
<td>1.3.6.1.4.1.1916.0.15</td>
</tr>
<tr>
<td></td>
<td>extremeHealthCheckFailed</td>
<td>1.3.6.1.4.1.1916.1.0.1</td>
</tr>
<tr>
<td></td>
<td>extremeCpuUtilizationRisingTrap</td>
<td>1.3.6.1.4.1.1916.1.0.2</td>
</tr>
<tr>
<td></td>
<td>extremeCpuUtilizationFalling</td>
<td>1.3.6.1.4.1.1916.1.0.3</td>
</tr>
<tr>
<td></td>
<td>coldStart</td>
<td>1.3.6.1.6.3.1.1.5.1</td>
</tr>
<tr>
<td></td>
<td>warmStart</td>
<td>1.3.6.1.6.3.1.1.5.2</td>
</tr>
<tr>
<td>extreme-traps</td>
<td>extremeEsrpStateChange</td>
<td>1.3.6.1.4.1.1916.0.17</td>
</tr>
<tr>
<td></td>
<td>extremeEdpNeighborAdded</td>
<td>1.3.6.1.4.1.1916.0.20</td>
</tr>
<tr>
<td></td>
<td>extremeEdpNeighborRemoved</td>
<td>1.3.6.1.4.1.1916.0.21</td>
</tr>
<tr>
<td></td>
<td>extremeSblUnitAdded</td>
<td>1.3.6.1.4.1.1916.0.18</td>
</tr>
<tr>
<td></td>
<td>extremeSblUnitRemoved</td>
<td>1.3.6.1.4.1.1916.0.19</td>
</tr>
<tr>
<td>smart-traps</td>
<td>extremeSmartTrap</td>
<td>1.3.6.1.4.1.1916.0.14</td>
</tr>
<tr>
<td>auth-traps</td>
<td>AuthenticationFailure</td>
<td>1.3.6.1.6.3.1.1.5.5</td>
</tr>
<tr>
<td></td>
<td>extremeInvalidLoginAttempt</td>
<td>1.3.6.1.4.1.1916.0.9</td>
</tr>
<tr>
<td>link-up-down-traps</td>
<td>linkDown</td>
<td>1.3.6.1.6.3.1.1.5.3</td>
</tr>
<tr>
<td></td>
<td>linkUp</td>
<td>1.3.6.1.6.3.1.1.5.4</td>
</tr>
<tr>
<td>rmon-traps</td>
<td>risingAlarm</td>
<td>rmon-traps, 1.3.6.1.2.1.16.0</td>
</tr>
<tr>
<td></td>
<td>fallingAlarm</td>
<td></td>
</tr>
<tr>
<td>security-traps</td>
<td>extremeMacLimitExceeded</td>
<td>1.3.6.1.4.1.1916.4.3.0.1</td>
</tr>
<tr>
<td></td>
<td>extremeUnauthorizedPortForMacDetected</td>
<td>1.3.6.1.4.1.1916.4.3.0.2</td>
</tr>
<tr>
<td></td>
<td>extremeMacDetectedOnLockedPort</td>
<td>1.3.6.1.4.1.1916.4.3.0.3</td>
</tr>
<tr>
<td></td>
<td>extremeNetloginUserLogin</td>
<td>1.3.6.1.4.1.1916.4.3.0.4</td>
</tr>
<tr>
<td></td>
<td>extremeNetloginUserLogout</td>
<td>1.3.6.1.4.1.1916.4.3.0.5</td>
</tr>
<tr>
<td></td>
<td>extremeNetloginAuthFailure</td>
<td>1.3.6.1.4.1.1916.4.3.0.6</td>
</tr>
</tbody>
</table>

1This SNMP trap group is only available on the “i” series of switches.

To view the SNMP trap receivers configured on the switch, use the show management command. The show management command displays information about the switch including the destination and community of the SNMP trap receivers configured on the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the configure snmp add trapreceiver command, use the unconfigure management command.

For version 7.1 and higher:
- Only the trap groups specified will be sent to the receiver.

  ExtremeWare 7.1 introduced support for SNMPv3, and the concept of trap groups was added to allow SNMPv1/v2c users to access a simplified version of the capabilities of SNMPv3. ExtremeWare 7.2e added the same function for the Summit “e” series of switches. The trap groups are pre-defined and cannot be modified. See chapter 3, “Managing the Switch”, in the ExtremeWare User Guide for more detail about trap groups.

For version 6.0 and higher:
- A maximum of sixteen trap receivers can be configured for each switch.

For version 4.x:
- A maximum of six trap receivers can be configured for each switch.
Example

The following command adds the IP address 10.101.0.100 as a trap receiver with community string purple:

```
configure snmp add trapreceiver 10.101.0.100 community purple
```

The following command adds the IP address 10.101.0.105 as a trap receiver with community string green, using port 3003:

```
configure snmp add trapreceiver 10.101.0.105 port 3003 community green
```

The following command adds the IP address 10.101.0.105 as a trap receiver with community string blue, and IP address 10.101.0.25 as the source:

```
configure snmp add trapreceiver 10.101.0.105 community blue from 10.101.0.25
```

The following command adds port 9990 at the IP address 10.203.0.22 as a trap receiver with the community string public, and the receiver should be sent standard traps for the trap groups for BGP and Extreme Networks:

```
configure snmp add trapreceiver ipaddress 10.203.0.22 port 9990 community public mode standard trap-group extreme-traps, bgp-traps
```

History

This command was first available in ExtremeWare 1.0.

This command was modified in ExtremeWare 6.2.1 to support the port, community, and source (from) options.

This command was modified in ExtremeWare 6.2.2 to add the mode options.

This command was modified in ExtremeWare 7.1.0 to add trap groups and the version option.

This command was added to the “e” series of switches in 7.1e.

This command was modified in ExtremeWare 7.2e to add support for SNMP Version 2 and for the trap groups.

Platform Availability

This command is available on all platforms.
configure snmp community

configure snmp community [readonly | readwrite] {encrypted} <alphanumeric string>

Description
Configures the value of the default SNMP read or read/write community string.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>readonly</td>
<td>Specifies read-only access to the system.</td>
</tr>
<tr>
<td>readwrite</td>
<td>Specifies read and write access to the system.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Specifies encryption, for use only by the switch when uploading or downloading a configuration. Should not be used through the CLI.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies an SNMP community string name. See “Usage Guidelines” for more information.</td>
</tr>
</tbody>
</table>

Default
The default read-only community string is public. The default read/write community string is private.

Usage Guidelines
This command has been superseded by the configure snmp add community command and can be used only to modify the first read-only or read-write community string which, are normally the default public and private community strings.

The community strings allow a simple method of authentication between the switch and the remote network manager. There are two types of community strings on the switch. Read community strings provide read-only access to the switch. The default read-only community string is public. Read-write community strings provide read and write access to the switch. The default read/write community string is private.

It is recommended that you change the values of the default read/write and read-only community strings. You use the configure snmp community command to change the value of the default community strings. An SNMP community string can contain up to 32 characters.

The encrypted option is intended for use by the switch when generating an ASCII configuration file (using the upload configuration command), or parsing a switch-generated configuration (using the download configuration command). Do not select the encrypted option in the CLI.

For version 6.2:
- A total of sixteen community strings can be configured on the switch. You can add additional community strings (in addition to the default community strings) using the configure snmp add community command.

Example
The following command sets the read/write community string to extreme:
configure snmp community readwrite extreme
History
This command was first available in ExtremeWare 1.0.
This command was added to the Summit “e” series of switches in 7.1e.
This command was modified in ExtremeWare 7.2e to add support for encryption.

Platform Availability
This command is available on all platforms.
configure snmp delete community

configure snmp delete community [readonly | readwrite] {encrypted} [all | <alphanumeric string>]

Description
Deletes an SNMP read or read/write community string.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>readonly</td>
<td>Specifies read-only access to the system.</td>
</tr>
<tr>
<td>readwrite</td>
<td>Specifies read and write access to the system.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Specifies an encrypted option.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all of the SNMP community strings.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies an SNMP community string name. See “Usage Guidelines” for more information.</td>
</tr>
</tbody>
</table>

Default
The default read-only community string is public. The default read/write community string is private.

Usage Guidelines
The community strings allow a simple method of authentication between the switch and the remote network manager. There are two types of community strings on the switch. Read community strings provide read-only access to the switch. The default read-only community string is public. read/write community strings provide read and write access to the switch. The default read/write community string is private. Sixteen read-only and sixteen read-write community strings can be configured on the switch, including the defaults. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 32 characters.

It is recommended that you change the defaults of the read/write and read-only community strings.

Use the configure snmp add command to configure an authorized SNMP management station.

The encrypted option should only be used by the switch to generate an ASCII configuration (using the upload configuration command), and parsing a switch-generated configuration (using the download configuration command). Do not select the encrypted option in the CLI.

For version 6.0 and later, including the Summit “e” series of switches:

- A total of eight community strings can be configured on the switch.

For version 4.x:

- SNMP community strings can contain up to 126 characters.

For version 2.0:

- The add parameter is included in the command syntax. It is available only in version 2.0.
- SNMP community strings can contain up to 127 characters.
Example
The following command deletes a read/write community string named \textit{extreme}:
\texttt{configure snmp delete community readwrite extreme}

History
This command was first available in ExtremeWare 2.0.
Support for the \texttt{add} parameter was discontinued in ExtremeWare 4.0.
This command was added to the Summit \textit{“e”} series of switches in 7.2e.

Platform Availability
This command is available on all platforms.
configure snmp delete trapreceiver

configure snmp delete trapreceiver [ip address> | {all}]

Description
Deletes a specified trap receiver or all authorized trap receivers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an SNMP trap receiver IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all SNMP trap receiver IP addresses.</td>
</tr>
</tbody>
</table>

Default
The default port number is 162.

Usage Guidelines
Use this command to delete a trap receiver of the specified IP address, or all authorized trap receivers.

Beginning in ExtremeWare 7.1.0, this command deletes only the first SNMPv1/v2c trap receiver whose IP address and port number match the specified value.

If a trap receiver has been added multiple times with different community strings, the community option specifies that only the trap receiver entry with the specified community string should be removed.

Example
The following command deletes the trap receiver 10.101.0.100 from the trap receiver list:
configure snmp delete trapreceiver 10.101.0.100

The following command deletes entries in the trap receiver list for 10.101.0.100, port 9990:
configure snmp delete trapreceiver 10.101.0.100 port 9990

Any entries for this IP address with a different community string will not be affected.

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.1 to support the community option.

This command was modified in ExtremeWare 7.1.0 for SNMPv3 compatibility.

This command was added to the Summit “e” series of switches in 7.1e.

This command was modified in ExtremeWare 7.2e. for SNMPv3 compatibility.
Platform Availability

This command is available on all platforms.
configure snmp sysContact

  configure snmp syscontact <alphanumeric string>

Description
Configures the name of the system contact.

Syntax Description

| alphanumerics string | Specifies a system contact name. |

Default
N/A.

Usage Guidelines
The system contact is a text field that enables you to enter the name of the person(s) responsible for managing the switch. A maximum of 255 characters is allowed.

To view the name of the system contact listed on the switch, use the show switch command. The show switch command displays switch statistics including the name of the system contact.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the configure snmp syscontact <alphanumeric string> command, use the unconfigure management command.

Example
The following command defines FredJ as the system contact:

  configure snmp syscontact fredj

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in 7.1e.

Platform Availability
This command is available on all platforms.
configure snmp sysLocation

configure snmp syslocation <alphanumeric string>

**Description**
Configures the location of the switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alphanumeric string</td>
<td>Specifies the switch location.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Use this command to indicate the location of the switch. A maximum of 255 characters is allowed.

To view the location of the switch on the switch, use the `show switch` command. The `show switch` command displays switch statistics including the location of the switch.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the `configure snmp syslocation <alphanumeric string>` command, use the `unconfigure management` command.

**Example**
The following command configures a switch location name on the system:
```
communize snmp syslocation englab
```

**History**
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in 7.1e.

**Platform Availability**
This command is available on all platforms.
configure snmp sysName

configure snmp sysname <alphanumeric string>

Description
Configures the name of the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;alphanumeric string&gt;</td>
<td>Specifies a device name.</td>
</tr>
</tbody>
</table>

Default
The default sysname is the model name of the device (for example, Summit1).

Usage Guidelines
You can use this command to change the name of the switch. A maximum of 32 characters is allowed. The sysname appears in the switch prompt.

To view the name of the system listed on the switch, use the show switch command. The show switch command displays switch statistics including the name of the system.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the configure snmp sysname <alphanumeric string> command, use the unconfigure management command.

Example
The following command names the switch:
configure snmp sysname engineeringlab

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in 7.1e.

Platform Availability
This command is available on all platforms.
configure snmpv3 add access

configure snmpv3 add access [hex <hex value> | <group name>] {sec-model [snmpv1 | snmpv2 | usm]} {sec-level [noauth | authnopriv | authpriv]} {read-view [hex <hex value> | <view name>] {write-view [hex <hex value> | <view name>] {notify-view [hex <hex value> | <view name>]} {volatile}

Description
Create (and modify) a group and its access rights.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>group name</td>
<td>Specifies the group name to add or modify.</td>
</tr>
<tr>
<td>sec-model</td>
<td>Specifies the security model to use.</td>
</tr>
<tr>
<td>snmpv1</td>
<td>Specifies the SNMPv1 security model.</td>
</tr>
<tr>
<td>snmpv2</td>
<td>Specifies the SNMPv2c security model.</td>
</tr>
<tr>
<td>usm</td>
<td>Specifies the SNMPv3 User-based Security Model (USM).</td>
</tr>
<tr>
<td>sec-level</td>
<td>Specifies the security level for the group.</td>
</tr>
<tr>
<td>noauth</td>
<td>Specifies no authentication (and implies no privacy) for the security level.</td>
</tr>
<tr>
<td>authnopriv</td>
<td>Specifies authentication and no privacy for the security level.</td>
</tr>
<tr>
<td>authpriv</td>
<td>Specifies authentication and privacy for the security level.</td>
</tr>
<tr>
<td>read-view</td>
<td>Specifies the read view name.</td>
</tr>
<tr>
<td>write-view</td>
<td>Specifies the write view name.</td>
</tr>
<tr>
<td>notify-view</td>
<td>Specifies the notify view name.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default values are:
- sec-model—USM
- sec-level—noauth
- read view name—defaultUserView
- write view name—“’”
- notify view name—defaultUserView
- non-volatile storage

Usage Guidelines
Use this command to configure access rights for a group. All access groups are created with a unique default context, “’”, as that is the only supported context.

There are a number of default (permanent) groups already defined. These groups are: admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv, v1v2c_ro, v1v2c_rw.
The default groups defined (permanent) are \texttt{v1v2c\_ro} for security names \texttt{snmpv1} and \texttt{snmpv2c}, \texttt{v1v2c\_rw} for security names \texttt{snmpv1} and \texttt{snmpv2c}, \texttt{admin} for security name \texttt{admin}, and \texttt{initial} for security names \texttt{initial}, \texttt{initialmd5}, \texttt{initialsha}, \texttt{initialmd5Priv} and \texttt{initialshaPriv}.

The default access defined (permanent) are \texttt{admin}, \texttt{initial}, \texttt{v1v2c\_ro}, \texttt{v1v2c\_rw}, and \texttt{v1v2cNotifyGroup}.

**Example**

In the following command, access for the group \texttt{defaultROGroup} is created with all the default values: security model \texttt{usm}, security level \texttt{noauth}, read view \texttt{defaultUserView}, no write view, notify view \texttt{defaultUserView}, and storage nonvolatile.

```bash
configure snmpv3 add access defaultROGroup
```

In the following command, access for the group \texttt{defaultROGroup} is created with the values: security model \texttt{USM}, security level \texttt{authnopriv}, read view \texttt{defaultAdminView}, write view \texttt{defaultAdminView}, notify view \texttt{defaultAdminView}, and storage nonvolatile.

```bash
configure snmpv3 add access defaultROGroup sec-model usm sec-level authnopriv read-view defaultAdminView write-view defaultAdminView notify-view defaultAdminView
```

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in 7.1e.

**Platform Availability**

This command is available on all platforms.
configure snmpv3 add community

configure snmpv3 add community (hex <hex value>) <community index> name (hex <hex value>) <community name> user (hex <hex value>) <user name> {tag (hex <hex value>) <transport tag>} {volatile}

Description
Add an SNMPv3 community entry.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>community index</td>
<td>Specifies the row index in the snmpCommunityTable</td>
</tr>
<tr>
<td>community name</td>
<td>Specifies the community name.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the USM user name.</td>
</tr>
<tr>
<td>transport tag</td>
<td>Specifies the tag used to locate transport endpoints in SnmpTargetAddrTable. When this community entry is used to authenticate v1/v2c messages, this tag is used to verify the authenticity of the remote entity.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to create or modify an SNMPv3 community in the community MIB.

Example
Use the following command to create an entry with the community index comm_index, community name comm_public, and user (security) name v1v2c_user:

configure snmpv3 add community comm_index name comm_public user v1v2c_user

Use the following command to create an entry with the community index (hex) of 4:E, community name (hex) of EA:12:CD:CF:AB:11:3C, user (security) name v1v2c_user, using transport tag 34872 and volatile storage:

configure snmpv3 add community hex 4:E name hex EA:12:CD:CF:AB:11:3C user v1v2c_user tag 34872 volatile

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability
This command is available on all platforms.
configure snmpv3 add filter

configure snmpv3 add filter {hex <hex value>} <profile name> subtree <object identifier> {/<subtree mask>} type [included | excluded] {volatile}

Description
Add a filter to a filter profile.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>profile name</td>
<td>Specifies the filter profile that the current filter is added to.</td>
</tr>
<tr>
<td>object identifier</td>
<td>Specifies a MIB subtree.</td>
</tr>
<tr>
<td>subtree mask</td>
<td>Specifies a hex octet string used to mask the subtree. For example, f7a indicates 1.1.1.1.0.1.1.1.1.0.1.0.</td>
</tr>
<tr>
<td>included</td>
<td>Specifies that the MIB subtree defined by &lt;object identifier&gt;/&lt;mask&gt; is to be included.</td>
</tr>
<tr>
<td>excluded</td>
<td>Specifies that the MIB subtree defined by &lt;object identifier&gt;/&lt;mask&gt; is to be excluded.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default mask value is an empty string (all 1s). The other default value is non-volatile.

Usage Guidelines
Use this command to create a filter entry in the snmpNotifyFilterTable. Each filter includes or excludes a portion of the MIB. Multiple filter entries comprise a filter profile that can eventually be associated with a target address. Other commands are used to associate a filter profile with a parameter name, and the parameter name with a target address.

This command can be used multiple times to configure the exact filter profile desired.

Example
Use the following command to add a filter to the filter profile prof1 that includes the MIB subtree 1.3.6.1.4.1/f0:

configure snmpv3 add filter prof1 subtree 1.3.6.1.4.1/f0 type included

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability
This command is available on all platforms.
configure snmpv3 add filter-profile

configure snmpv3 add filter-profile {hex <hex value>} <profile name> param {hex <hex value>} <param name> {volatile}

Description
Associate a filter profile with a parameter name.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>profile name</td>
<td>Specifies the filter profile name.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies a parameter name to associate with the filter profile.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default storage type is non-volatile.

Usage Guidelines
Use this command to add an entry to the snmpNotifyFilterProfileTable. This table associates a filter profile with a parameter name. The parameter name is associated with target addresses, and the filter profile is associated with a series of filters, so, in effect, you are associating a series of filters with a target address.

Example
Use the following command to associate the filter profile prof1 with the parameter name P1:

configure snmpv3 add filter-profile prof1 param P1

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 add group user

configure snmpv3 add group [hex <hex value> | <group name>] user [hex <hex value> | <user name>] {sec-model [snmpv1 | snmpv2 | usm]} {volatile}

Description
Add a user name (security name) to a group.

Syntax Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>group name</td>
<td>Specifies the group name to add or modify.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name to add or modify.</td>
</tr>
<tr>
<td>sec-model</td>
<td>Specifies the security model to use.</td>
</tr>
<tr>
<td>snmpv1</td>
<td>Specifies the SNMPv1 security model.</td>
</tr>
<tr>
<td>snmpv2</td>
<td>Specifies the SNMPv2c security model.</td>
</tr>
<tr>
<td>usm</td>
<td>Specifies the SNMPv3 User-based Security Model (USM).</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default values are:

- sec-model—USM
- non-volatile storage

Usage Guidelines
Use this command to associate a user name with a group.

As per the SNMPv3 RFC, a security name is model independent while a username is model dependent. For simplicity, both are assumed to be same here. User names and security names are handled the same. In other words, if a user is created with the user name *username*, the security name value is the same, *username*.

Every group is uniquely identified by a security name and security model. So the same security name can be associated to a group name but with different security models.

Example
Use the following command to associate the user *userV1* to the group *defaultRoGroup* with SNMPv1 security:

```
configure snmpv3 add group defaultRoGroup user userV1 sec-model snmpv1
```

Use the following command to associate the user *userV3* with security model *USM* and storage type *volatile* to the access group *defaultRoGroup*:

```
configure snmpv3 add group defaultRoGroup user userV3 volatile
```
**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 add mib-view

configure snmpv3 add mib-view {{hex <hex value>} | <view name> subtree <object identifier> {{/<subtree mask>}} {type [included | excluded]} {volatile}

Description
Add (and modify) a MIB view.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>view name</td>
<td>Specifies the MIB view name to add or modify.</td>
</tr>
<tr>
<td>subtree</td>
<td>Specifies a MIB subtree.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a hex octet string used to mask the subtree. For example, f7a indicates 1.1.1.1.1.0.0.1.0.1.0.</td>
</tr>
<tr>
<td>included</td>
<td>Specifies that the MIB subtree defined by &lt;subtree&gt;/&lt;mask&gt; is to be included.</td>
</tr>
<tr>
<td>excluded</td>
<td>Specifies that the MIB subtree defined by &lt;subtree&gt;/&lt;mask&gt; is to be excluded.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default mask value is an empty string (all 1s). The other default values are included and non-volatile.

Usage Guidelines
Use this command to create a MIB view into a subtree of the MIB. If the view already exists, this command modifies the view to additionally include or exclude the specified subtree.

In addition to the created MIB views, there are three default views. They are of storage type permanent and cannot be deleted, but they can be modified. The default views are: defaultUserView, defaultAdminView, and defaultNotifyView.

Example
Use the following command to create the MIB view allMIB with the subtree 1.3 included as non-volatile:

configure snmpv3 add mib-view allMIB subtree 1.3

Use the following command to create the view extremeMib with the subtree 1.3.6.1.4.1.1916 included as non-volatile:

configure snmpv3 add mib-view extremeMib subtree 1.3.6.1.4.1.1916

Use the following command to create a view vrrpTrapNewMaster which excludes VRRP notification.1 and the entry is volatile.

configure snmpv3 add mib-view vrrpTrapNewMaster subtree 1.3.6.1.4.1.1916
configure snmpv3 add mib-view vrrpTrapNewMaster 1.3.6.1.2.1.68.0.1/ff8 type excluded volatile

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 add notify

    configure snmpv3 add notify {hex <hex value>} <notify name> tag {hex <hex value>} <tag> {volatile}

**Description**
Add an entry to the snmpNotifyTable.

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>notify name</td>
<td>Specifies the notify name to add.</td>
</tr>
<tr>
<td>tag</td>
<td>Specifies a string identifier for the notifications to be sent to the target.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

**Default**
The default storage type is non-volatile.

**Usage Guidelines**
Use this command to add an entry to the snmpNotifyTable. When a notification is to be sent, this table is examined. For the target addresses that have been associated with the tags present in the table, notifications will be sent, based on the filters also associated with the target addresses.

**Example**
Use the following command to send notification to addresses associated with the tag *type1*:

    configure snmpv3 add notify N1 tag type1

**History**
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 add target-addr

configure snmpv3 add target-addr [{hex <hex value}> | <addr name>] param [{hex <hex value}> | <param name>] ipaddress <ip address> {/<target-addr mask>} {transport-port <port>} {from <source IP address>} {tag-list {hex <hex value>} <tag>, {hex <hex value>} <tag>, ...} {volatile}

**Description**

Add and configure an SNMPv3 target address and associate filtering, security, and notifications with that address.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>addr name</td>
<td>Specifies a string identifier for the target address.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies the parameter name associated with the target.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an SNMPv3 target IP address.</td>
</tr>
<tr>
<td>target-addr mask</td>
<td>Specifies a hex octet string used to mask the target address. For example, f7a indicates 1.1.1.1.0.1.1.1.1.0.1.0.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a UDP port. Default is 162.</td>
</tr>
<tr>
<td>source ip address</td>
<td>Specifies the IP address of a VLAN to be used as the source address for the trap</td>
</tr>
<tr>
<td>tag</td>
<td>Specifies a string identifier for the notifications to be sent to the target.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

**Default**

The default values are:

- transport-port—port 162
- tag-list—the single tag defaultNotify, a pre-defined value in the snmpNotifyTable
- non-volatile storage

**Usage Guidelines**

Use this command to create an entry in the SNMPv3 snmpTargetAddressTable. The param parameter associates the target address with an entry in the snmpTargetParamsTable, which specifies security and storage parameters for messages to the target address, and an entry in the snmpNotifyFilterProfileTable, which specifies filters to use for notifications to the target address.

**Example**

The following command specifies a target address of 10.203.0.22, port 9990, with the name A1, and associates it with the security parameters and filter profile P1, and the notification tags type1 and type2:

```
configure snmpv3 add target-addr A1 param P1 ipaddress 10.203.0.22 transport-port 9990 tag-list type1, type2
```
History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 add target-params

configure snmpv3 add target-params [hex <hex value> | <param name>] user [hex <hex value> | <user name>] mp-model [snmpv1 | snmpv2c | snmpv3] sec-model [snmpv1 | snmpv2c | usm] {sec-level [noauth | authnopriv | priv]} (volatile)

Description
Add and configure SNMPv3 target parameters.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies the parameter name associated with the target.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies a user.</td>
</tr>
<tr>
<td>mp-model</td>
<td>Specifies a message processing model; choose from SNMPv1, SNMPv2, or SNMPv3.</td>
</tr>
<tr>
<td>sec-model</td>
<td>Specifies the security model to use.</td>
</tr>
<tr>
<td>snmpv1</td>
<td>Specifies the SNMPv1 security model.</td>
</tr>
<tr>
<td>snmpv2</td>
<td>Specifies the SNMPv2c security model.</td>
</tr>
<tr>
<td>usm</td>
<td>Specifies the SNMPv3 User-based Security Model (USM).</td>
</tr>
<tr>
<td>sec-level</td>
<td>Specifies the security level for the group.</td>
</tr>
<tr>
<td>noauth</td>
<td>Specifies no authentication (and implies no privacy) for the security level.</td>
</tr>
<tr>
<td>authnopriv</td>
<td>Specifies authentication and no privacy for the security level.</td>
</tr>
<tr>
<td>authpriv</td>
<td>Specifies authentication and privacy for the security level.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default values are:
- sec-level—noauth
- non-volatile storage

Usage Guidelines
Use this command to create an entry in the SNMPv3 snmpTargetParamsTable. This table specifies the message processing model, security level, security model, and the storage parameters for messages to any target addresses associated with a particular parameter name.

To associate a target address with a parameter name, see the command “configure snmpv3 add target-addr” on page 154.

Example
The following command specifies a target parameters entry named P1, a user name of guest, message processing and security model of SNMPv2c, and a security level of no authentication:
configure snmpv3 add target-params P1 user guest mp-model snmpv2c sec-model snmpv2c sec-level noauth

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 add user

configure snmpv3 add user {hex} <user name> {authentication [md5 | sha] [hex <hex octet> | <password>]} {privacy [hex <hex octet> | <password>]} {volatile}

Description
Add (and modify) an SNMPv3 user.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name to add or modify.</td>
</tr>
<tr>
<td>MD5</td>
<td>Specifies MD5 authentication.</td>
</tr>
<tr>
<td>SHA</td>
<td>Specifies SHA authentication.</td>
</tr>
<tr>
<td>authentication</td>
<td>Specifies the authentication password or hex string to use for generating the authentication key for this user.</td>
</tr>
<tr>
<td>privacy</td>
<td>Specifies the privacy password or hex string to use for generating the privacy key for this user.</td>
</tr>
<tr>
<td>volatile</td>
<td>Specifies volatile storage.</td>
</tr>
</tbody>
</table>

Default
The default values are:
- authentication—no authentication
- privacy—no privacy
- non-volatile storage

Usage Guidelines
Use this command to create or modify an SNMPv3 user configuration.

If hex is specified, supply a 16 octet hex string for MD5, or a 20 octet hex string for SHA.

You must specify authentication if you want to specify privacy. There is no support for privacy without authentication.

The default user names are: admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv. The initial password for admin is password. For the other default users, the initial password is the user name.

Example
Use the following command to configure the user guest on the local SNMP Engine with security level noauth (no authentication and no privacy):

configure snmpv3 add user guest
Use the following command to configure the user authMD5 to use MD5 authentication with the password palertyu:

```
configure snmpv3 add user authMD5 authentication md5 palertyu
```

Use the following command to configure the user authSHApriv to use SHA authentication with the hex key shown below, the privacy password palertyu, and volatile storage:

```
```

**History**

This command was first available in ExtremeWare 7.1.0. This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure snmpv3 add user clone-from

configure snmpv3 add user {hex <hex value>} <user name> clone-from {hex <hex value>} <user name>

Description
Create a new user by cloning from an existing SNMPv3 user.

Syntax Description

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
</tr>
<tr>
<td>user name</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to create a new user by cloning an existing one. Once you have successfully cloned the new user, you can modify its parameters using the following command:

```
configure snmpv3 add user {hex <hex value>} <user name> {authentication [md5 | sha] [hex <hex octet> | <password>]} {privacy [hex <hex octet> | <password>]} {volatile}
```

Users cloned from the default users will have the storage type of non-volatile. The default names are: admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv.

Example
Use the following command to create a user cloneMD5 with same properties as the default user initialmd5. All authorization and privacy keys will initially be the same as with the default user initialmd5.

```
configure snmpv3 add user cloneMD5 clone-from initialmd5
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 delete access

configure snmpv3 delete access [all-non-defaults | {hex <hex value>} | 
<group name> {sec-model [snmpv1 | snmpv2c | usm] sec-level [noauth | 
authnopriv | priv]}]

Description
Delete access rights for a group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-non-defaults</td>
<td>Specifies that all non-default (non-permanent) security groups are to be deleted.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>group name</td>
<td>Specifies the group name to add or modify.</td>
</tr>
<tr>
<td>sec-model</td>
<td>Specifies the security model to use.</td>
</tr>
<tr>
<td>snmpv1</td>
<td>Specifies the SNMPv1 security model.</td>
</tr>
<tr>
<td>snmpv2c</td>
<td>Specifies the SNMPv2c security model.</td>
</tr>
<tr>
<td>usm</td>
<td>Specifies the SNMPv3 User-based Security Model (USM).</td>
</tr>
<tr>
<td>sec-level</td>
<td>Specifies the security level for the group.</td>
</tr>
<tr>
<td>noauth</td>
<td>Specifies no authentication (and implies no privacy) for the security level.</td>
</tr>
<tr>
<td>authnopriv</td>
<td>Specifies authentication and no privacy for the security level.</td>
</tr>
<tr>
<td>authpriv</td>
<td>Specifies authentication and privacy for the security level.</td>
</tr>
</tbody>
</table>

Default
The default values are:
- sec-model—USM
- sec-level—noauth

Usage Guidelines
Use this command to remove access rights for a group. Use the all-non-defaults keyword to delete all the security groups, except for the default groups. The default groups are: admin, initial, v1v2c_ro, v1v2c_rw.

Deleting an access will not implicitly remove the related group to user association from the VACMSecurityToGroupTable. To remove the association, use the following command:

```configure snmpv3 delete group {{hex} <group name>} user {all-non-defaults | {{hex} <user name> sec-model {sec-model [snmpv1|snmpv2c|usm]}}}
```

Example
The following command deletes all entries with the group name userGroup:

```configure snmpv3 delete access userGroup```
The following command deletes the group *userGroup* with the security model *snmpv1* and security level of authentication and no privacy (*authnopriv*):

```
configure snmpv3 delete access userGroup sec-model snmpv1 sec-level authnopriv
```

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure snmpv3 delete community

configure snmpv3 delete community [all-non-defaults | {{hex <hex value>} <community index>} | {name {hex <hex value>} <community name> }]

**Description**
Delete an SNMPv3 community entry.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>community index</td>
<td>Specifies the row index in the snmpCommunityTable</td>
</tr>
<tr>
<td>community name</td>
<td>Specifies the community name.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the USM user name.</td>
</tr>
<tr>
<td>all-non-defaults</td>
<td>Specifies that all non-default community entries are to be removed.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Use this command to delete an SNMPv3 community in the community MIB. The default entries are *public* and *private*.

**Example**
Use the following command to delete an entry with the community index *comm_index*:

```
configure snmpv3 delete community comm_index
```

Use the following command to create an entry with the community name (hex) of *EA:12:CD:CF:AB:11:3C*:

```
configure snmpv3 delete community name hex EA:12:CD:CF:AB:11:3C
```

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 delete filter

configure snmpv3 delete filter [all | [{hex <hex value>} <profile name> (subtree <object identifier>)}]

**Description**
Delete a filter from a filter profile.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all filters.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>profile name</td>
<td>Specifies the filter profile of the filter to delete.</td>
</tr>
<tr>
<td>object identifier</td>
<td>Specifies the MIB subtree of the filter to delete.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Use this command to delete a filter entry from the snmpNotifyFilterTable. Specify `all` to remove all entries. Specify a profile name to delete all entries for that profile name. Specify a profile name and a subtree to delete just those entries for that filter profile and subtree.

**Example**

Use the following command to delete the filters from the filter profile `prof1` that reference the MIB subtree `1.3.6.1.4.1`:

```
configure snmpv3 delete filter prof1 subtree 1.3.6.1.4.1
```

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 delete filter-profile

configure snmpv3 delete filter-profile [all | [{hex <hex value>}<profile name> {param {hex <hex value>}<param name>}]]

**Description**
Remove the association of a filter profile with a parameter name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all filter profiles.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>profile name</td>
<td>Specifies the filter profile name to delete.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies to delete the filter profile with the specified profile name and parameter name.</td>
</tr>
</tbody>
</table>

**Default**
The default storage type is non-volatile.

**Usage Guidelines**
Use this command to delete entries from the snmpNotifyFilterProfileTable. This table associates a filter profile with a parameter name. Specify all to remove all entries. Specify a profile name to delete all entries for that profile name. Specify a profile name and a parameter name to delete just those entries for that filter profile and parameter name.

**Example**
Use the following command to delete the filter profile prof1 with the parameter name P1:

```
configure snmpv3 delete filter-profile prof1 param P1
```

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 delete group user

configure snmpv3 delete group {{hex <hex value>} | <group name>} user [all-non-defaults | {{hex <hex value>} | <user name>} {sec-model [snmpv1|snmpv2c|usm]}}

Description
Delete a user name (security name) from a group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>group name</td>
<td>Specifies the group name to add or modify.</td>
</tr>
<tr>
<td>all-non-defaults</td>
<td>Specifies that all non-default (non-permanent) users are to be deleted from the group.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name to add or modify.</td>
</tr>
<tr>
<td>sec-model</td>
<td>Specifies the security model to use.</td>
</tr>
<tr>
<td>snmpv1</td>
<td>Specifies the SNMPv1 security model.</td>
</tr>
<tr>
<td>snmpv2</td>
<td>Specifies the SNMPv2c security model.</td>
</tr>
<tr>
<td>usm</td>
<td>Specifies the SNMPv3 User-based Security Model (USM).</td>
</tr>
</tbody>
</table>

Default
The default values are:
- sec-model—USM

Usage Guidelines
Use this command to remove the associate of a user name with a group.

As per the SNMPv3 RFC, a security name is model independent while a username is model dependent. For simplicity, both are assumed to be same here. User names and security names are handled the same. In other words, if a user is created with the user name `username`, the security name value is the same, `username`.

Every group is uniquely identified by a security name and security model. So the same security name can be associated to a group name but with different security models.

The default groups are: `admin, initial, v1v2c_ro, v1v2c_rw`.

The default users are: `admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv`.

Example
Use the following command to delete the user `guest` from the group `UserGroup` for the security model `snmpv2c`:

`configure snmpv3 delete group UserGroup user guest sec-model snmpv2c`
Use the following command to delete the user `guest` from the group `userGroup` with the security model USM:

```
configure snmpv3 delete group userGroup user guest
```

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure snmpv3 delete mib-view

configure snmpv3 delete mib-view [all-non-defaults | {{hex <hex value>} | <view name> {subtree <object identifier>}}]

Description
Delete a MIB view.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-non-defaults</td>
<td>Specifies that all non-default (non-permanent) MIB views are to be deleted.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>view name</td>
<td>Specifies the MIB view name to add or modify.</td>
</tr>
<tr>
<td>subtree</td>
<td>Specifies a MIB subtree.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to delete a MIB view. Views which are being used by security groups cannot be deleted. Use the all-non-defaults keyword to delete all the MIB views (not being used by security groups) except for the default views. The default views are: defaultUserView, defaultAdminView, and defaultNotifyView.

Use the configure snmpv3 add mib-view command to remove a MIB view from its security group, by specifying a different view.

Example
The following command deletes all views (only the permanent views will not be deleted):
configure snmpv3 delete mib-view all-non-defaults

The following command deletes all subtrees with the view name AdminView:
configure snmpv3 delete mib-view AdminView

The following command deletes the view AdminView with subtree 1.3.6.1.2.1.2
configure snmpv3 delete mib-view AdminView subtree 1.3.6.1.2.1.2

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability

This command is available on all platforms.
configure snmpv3 delete notify

    configure snmpv3 delete notify [{hex <hex value>} <notify name>] | all-non-defaults]

Description
Delete an entry from the snmpNotifyTable.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>notify name</td>
<td>Specifies the notify name to add.</td>
</tr>
<tr>
<td>all-non-defaults</td>
<td>Specifies that all non-default (non-permanent) notifications are to be deleted.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to delete an entry from the snmpNotifyTable. When a notification is to be sent, this table is examined. For the target addresses that have been associated with the tags present in the table, notifications will be sent, based on the filters also associated with the target addresses.

There is one default notification that cannot be deleted, defaultNotify.

Example
Use the following command to remove the N1 entry from the table:

    configure snmpv3 delete notify N1

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 delete target-addr

configure snmpv3 delete target-addr [{hex <hex value>} | <addr name> | all}]

**Description**
Delete SNMPv3 target addresses.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>addr name</td>
<td>Specifies a string identifier for the target address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all target addresses.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Use this command to delete an entry in the SNMPv3 snmpTargetAddressTable.

**Example**
The following command deletes target address named A1:

```bash
configure snmpv3 delete target-addr A1
```

**History**
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on the “e” series platforms.
configure snmpv3 delete target-params

configure snmpv3 delete target-params [{\{hex <hex value>} <param name>} | all]

Description
Delete SNMPv3 target parameters.

Syntax Description

<table>
<thead>
<tr>
<th>hex</th>
<th>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>param name</td>
<td>Specifies the parameter name associated with the target.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to delete an entry in the SNMPv3 snmpTargetParamsTable. This table specifies the message processing model, security level, security model, and the storage parameters for messages to any target addresses associated with a particular parameter name.

Example
The following command deletes a target parameters entry named P1:

```
configure snmpv3 delete target-params P1
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 delete user

configure snmpv3 delete user [all-non-defaults | {hex <hex value>} <user name>]

Description
Delete an existing SNMPv3 user.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all-non-defaults</td>
<td>Specifies that all non-default (non-permanent) users are to be deleted.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name to add or to clone from.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to delete an existing user.

Use the all-non-defaults keyword to delete all users, except for the default (permanent) users. The default user names are: admin, initial, initialmd5, initialsha, initialmd5Priv, initialshaPriv.

Deleting a user will not implicitly remove the related group to user association from the VACMSecurityToGroupTable. To remove the association, use the following command:

class snmpv3 delete group {{hex} <group name>} user [all-non-defaults | {{hex} <user name> {sec-model [snmpv1|snmpv2c|usm]}}]

Example
The following command deletes all non-default users:

configure snmpv3 delete user all-non-defaults

The following command deletes the user guest:

configure snmpv3 delete user guest

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 engine-boots

configure snmpv3 engine-boots <(1-2147483647)>

Description
Configures the SNMPv3 Engine Boots value.

Syntax Description

| (1-2147483647) | Specifies the value of engine boots. |

Default
N/A.

Usage Guidelines
Use this command if the Engine Boots value needs to be explicitly configured. Engine Boots and Engine Time will be reset to zero if the Engine ID is changed. Engine Boots can be set to any desired value but will latch on its maximum, 2147483647.

Example
The following command configures Engine Boots to 4096:

```
configure snmpv3 engine-boots 4096
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 engine-id

configure snmpv3 engine-id <hex octet>

Description
Configures the SNMPv3 snmpEngineID.

Syntax Description

| hex octet | Specifies the colon delimited hex octet that serves as part of the snmpEngineID (5-32 octets). |

Default
The default snmpEngineID is the device MAC address.

Usage Guidelines
Use this command if the snmpEngineID needs to be explicitly configured. The first four octets of the ID are fixed to 80:00:07:7C, which represents Extreme Networks Vendor ID. Once the snmpEngineID is changed, default users will be reverted back to their original passwords/keys, while non-default users will be reset to the security level of no authorization, no privacy.

On “i” series platform only. In a chassis, the snmpEngineID will be generated using the MAC address of the MSM with which the switch boots first. For MSM hitless failover, the same snmpEngineID will be propagated to both of the MSMs.

Example
The following command configures the snmpEngineID to be 80:00:07:7C:00:0a:1c:3e:11:
configure snmpv3 engine-id 00:0a:1c:3e:11

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure snmpv3 extreme-target-addr-ext

configure snmpv3 extreme-target-addr-ext {hex <hex value>} <addr name> mode
[standard | enhanced] {ignore-mp-model} {ignore-event-community}

Description
Configure an entry in the extremeTargetAddrExtTable.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies a string identifier for the target address.</td>
</tr>
<tr>
<td>addr name</td>
<td>Specifies enhanced traps, which contain extra varbinds at the end.</td>
</tr>
<tr>
<td>enhanced</td>
<td>Specifies standard traps, which do not contain the extra varbinds.</td>
</tr>
<tr>
<td>standard</td>
<td>Sets the ignore message passing model flag</td>
</tr>
<tr>
<td>ignore-mp-model</td>
<td>Sets the use Event Community flag to false.</td>
</tr>
</tbody>
</table>

Default
The default values are:
- mode—enhanced
- ignore-mp-model—False, the mp-model is not ignored.
- ignore-event-community—False, the EventCommunity is not ignored.

Usage Guidelines
The command snmp add trapreceiver was retained when SNMPv3 support was added to ExtremeWare. This command allows you to set trap receivers without using the details of SNMPv3. However, when the command is executed, it internally sets a per-trap-receiver flag called ignore-mp-model, and ignore-event-community. This command is never uploaded to the switch, but its equivalent SNMPv3 command, configure snmpv3 add target-addr, is uploaded instead. The latter has no tokens for ignore-mp-model or ignore-event-community. Therefore, upon downloading the configuration, the setting for these objects is lost.

This separate command corresponds to a private SNMP table that was subsequently added. The table contains three objects, ignoreMPModel, useEventCommunity, and Mode. This private table, the extremeTargetAddrExtTable, is an extension to the standard snmpv3TargetAddrTable

Example
The following command that standard traps will be used:

configure snmpv3 target-addr-ext A1 mode standard

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure sntp-client server

configure sntp-client [primary | secondary] server <host name | ipaddress>

Description
Configures an NTP server for the switch to obtain time information.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Specifies a primary server name.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies a secondary server name.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies a host name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Queries are first sent to the primary server. If the primary server does not respond within 1 second, or if it is not synchronized, the switch queries the second server. If the switch cannot obtain the time, it restarts the query process. Otherwise, the switch waits for the sntp-client update interval before querying again.

Example
The following command configures a primary NTP server:

```
configure sntp-client primary server 10.1.2.2
```

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure sntp-client update-interval

    configure sntp-client update-interval <seconds>

Description
Configures the interval between polls for time information from SNTP servers.

Syntax Description

| seconds | Specifies an interval in seconds. |

Default
64 seconds.

Usage Guidelines
None.

Example
The following command configures the interval timer:
configure sntp-client update-interval 30

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure web login-timeout

    configure web login-timeout <seconds>

Description
Configures the timeout for user to enter username/password in the pop-up window.

Syntax Description

| seconds | Specifies an interval in seconds, where <seconds> can range from 30 seconds to 10 minutes (600 seconds). |

Default
30 seconds.

Usage Guidelines
The Show for this parameter is displayed by using the following command:

    show management

Example
The following command configures the interval timer:

    configure sntp-client update-interval 30

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable alt-queue-management

disable alt-queue-management

Description
Disables the alternate queue management.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
The following command enables alternate queue management:

```
enable alt-queue-management
```

To disable the alternative queue management feature for the next boot, use the following command:

```
disable alt-queue-management
```

Example
The following command disables alternate queue management:

```
disable alt-queue-management
```

History
This command was available in ExtremeWare 7.2.

Platform Availability
This command is only available on the “i” series platforms.
disable dhcp ports vlan

    disable dhcp ports <portlist> vlan <vlan name>

**Description**

Disables DHCP on a specified port in a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports for which DHCP should be disabled.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN on whose ports DHCP should be disabled.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

The DHCP server should be used with Network Login and not as a stand-alone DHCP server.

**Example**

The following command disables DHCP for port 9 in VLAN *corp*:

```
disable dhcp ports 9 vlan corp
```

**History**

This command was first available in ExtremeWare 7.1e.

**Platform Availability**

This command is only available on the “e” series platforms.
disable eapol-flooding

disable eapol-flooding

Description
Disables EAPOL flooding on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Per IEEE 802.1D, Summit “e” series switches do not forward EAPOL frames. Also, if network login is enabled, EAPOL flooding cannot be enabled.

Example
The following example disables EAPOL frame flooding on a Summit “e” series switch:

disable eapol-flooding

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is only available on the “e” series platforms.
disable snmp access

disable snmp access {snmp-v1v2c}

Description
Selectively disables SNMP on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>snmp-v1v2c</td>
<td>Disables SNMPv1/v2c access only; does not affect SNMPv3 access.</td>
</tr>
</tbody>
</table>

Default
Enabled.

Usage Guidelines
Disabling SNMP access does not affect the SNMP configuration (for example, community strings). However, if you disable SNMP access, you will be unable to access the switch using SNMP.

To allow access, use the following command:

```plaintext
enable snmp access
```

By using the enable and disable commands you can enable all SNMP access, no SNMP access, or only SNMPv3 access. You cannot enable only SNMPv1/v2c access. To enable SNMPv3 only access on the switch, use the following commands:

```plaintext
enable snmp access
disable snmp access {snmp-v1v2c}
```

Example
The following command disables all SNMP access on the switch:

disable snmp access

History
This command was first available in ExtremeWare 2.0.

The `snmp-v1v2c` keyword was added in ExtremeWare 7.1.0

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to add the `snmp-v1v2c` keyword.

Platform Availability
This command is available on all platforms.
disable snmp dot1dTpFdbTable

disable snmp dot1dTpFdbTable

Description
Disables SNMP GetNext responses for the dot1dTpFdbTable in the BRIDGE-MIB.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
SNMP Get responses are not affected by this command.

To view the configuration of the dot1dTpFdb table on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state the dot1dTpFdb table.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the disable snmp dot1dTpFdbTable command, use the unconfigure management command.

Example
The following command disables the dot1dTPFdb table:

disable snmp dot1dTpFdbTable

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable snmp traps

disable snmp traps

Description
Prevents SNMP traps from being sent from the switch.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
This command does not clear the SNMP trap receivers that have been configured. The command prevents SNMP traps from being sent from the switch even if trap receivers are configured.

Example
The following command prevents SNMP traps from being sent from the switch to the trap receivers:
disable snmp traps

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable snmp traps exceed-committed-rate ports

disable snmp traps exceed-committed-rate ports <portlist> {<Ingress QOS Profile>}

Description
Prevents SNMP traps from being sent from the indicated ports on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies a list of “3” series I/O module ports (in the form 2.*, 2:5, or 2:6-2:8).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ingress QOS Profile</td>
<td>Specifies an optional ingress QOS profile. If not specified, all ingress QOS profiles for the indicated ports will be affected.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
To see which ports have such traps enabled, use the show config command.

Example
The following command will prevent SNMP exceed-committed-rate traps from being sent for all ingress QOS profiles on ports 2:5 through 2:8.

disable snmp traps exceed-committed-rate ports 2:5-2:8

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available on “3” series I/O modules only.
disable snmp traps mac-security

disable snmp traps mac-security

Description
Prevents SNMP mac-security traps from being sent from the switch for all ports.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
This command should be used in conjunction with the configure ports <portlist> limit-learning command.
That command configures a limit on the number of MAC addresses that can be learned on a port(s).
After that limit has been reached on a particular port, a trap will be sent by the switch, if a new MAC
address appears on that port. In addition, a message will be generated in the syslog and the port will be
blackholed.

Example
The following command prevents SNMP mac-security traps from being sent from the switch.
disable snmp traps mac-security

History
This command was first available in ExtremeWare 7.0.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable snmp traps port-up-down

disable snmp traps port-up-down ports [all | mgmt | <portlist>]

Description
Prevents SNMP port up/down traps (also known as link up and link down traps) from being sent from the switch for the indicated ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that no link up/down traps should be sent for all ports. This does not include the management port which must be explicitly specified.</td>
</tr>
<tr>
<td>mgmt</td>
<td>Specifies that no link up/down traps should be sent for the management port. This option will only appear on platforms that have a management port, such as the Summit 400.</td>
</tr>
<tr>
<td>&lt;portlist&gt;</td>
<td>Specifies the list of ports.</td>
</tr>
</tbody>
</table>

Default
Enabled.

Usage Guidelines
This command is used to disable the sending of link up and link down traps for the specified ports. To see which ports do not have such traps disabled, use the show management command.

Example
The following command will prevent link up or link down traps from being sent for any port on the switch (except the management port if it has one).

disable snmp traps port-up-down all

History
This command was first available in ExtremeWare 6.2.2
This command was modified to include the management port in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable sntp-client

  disable sntp-client

Description
Disables the SNTP client.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. After the SNTP client has been enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean Time (GMT) offset and the use of Daylight Savings Time (DST).

Example
The following command disables the SNTP client:

disable sntp-client

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable system-watchdog

disable system-watchdog

Description
Disables the system watchdog timer.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
The watchdog timer reboots the switch if the CPU becomes trapped in a processing loop. If the watchdog timer is executed, the switch captures information on the cause of the reboot and posts it to the system log.

Example
The following command disables the watchdog timer:

disable system-watchdog

History
This command was first available in ExtremeWare 6.1.9.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable telnet

    disable telnet

Description
Disables Telnet services on the system.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
You must be logged in as an administrator to enable or disable Telnet.

Example
With administrator privilege, the following command disables Telnet services on the switch:

    disable telnet

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable web

disable web

Description
Disables web access to the switch.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
You can use this command to disable web access to the switch. If you are using ExtremeWare Vista for web access, you must create and configure an access profile before you can use this option. You create an access profile using the create access-profile type command. You configure an access profile using one of the configure access-profile commands.

Example
The following command disables web access to the switch:

disable web

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable alt-queue-management

enable alt-queue-management

Description
Enables the alternate queue management.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Use this command to configure the alternative queue management feature for the next boot. Configuring the feature does not affect the queue management current boot.

Use the `show switch` command to display the alternative queue management feature status, as shown in the following example:

MSM64:3 # show switch
SysName: MSM64
SysLocation: support@extremenetworks.com, +1 888 257 3000
System MAC: 00:01:30:12:2A:D0
License: Full L3
System Mode: 802.1Q EtherType is 8100 (Hex).
Diag Mode: Fast Post
RED Probability: 0 Marked Probability: 0
DLCS: Disabled
Backplane Ls: port-based
SysHealth Check: Enabled. Alarm Level = Log
Recovery Mode: None
Transceiver Diag: Enabled. Failure action: log only
Fdb-Scan Diag: Enabled. Failure action: sys-health-check
MSM Failover: take-links-down
System Watchdog: Enabled
Reboot Loop Prot: Disabled
Alter Queue Mgmt: Disabled       Next Boot: Disabled
Bus-stats: Disabled

Timezone: [Auto DST Enabled] GMT Offset: 0 minutes, name is GMT.
          DST of 60 minutes is currently not in effect, name is not set.
          DST begins every first Sunday April at 2:00
          DST ends every last Sunday October at 2:00

Press <SPACE> to continue or <Q> to quit:
Use the following command to disable alternate queue management:

`disable alt-queue-management`

**Example**

The following command configures alternate queue management:

`enable alt-queue-management`

**History**

This command was available in ExtremeWare 7.2.

**Platform Availability**

This command is only available on the “i” series platforms.
enable dhcp ports vlan

    enable dhcp ports <portlist> vlan <vlan name>

Description
Enables DHCP on a specified port in a VLAN.

Syntax Description

| portlist | Specifies the ports for which DHCP should be enabled. |
|-----------------------------|
| vlan_name | Specifies the VLAN on whose ports DHCP should be enabled. |

Default
N/A.

Usage Guidelines
None.

Example
The following command enables DHCP for port 9 in VLAN corp:

```
enable dhcp ports 9 vlan corp
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable eapol-flooding

enable eapol-flooding

Description
Enables EAPOL flooding on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Per IEEE 802.1D, Summit “e” series switches do not forward EAPOL frames. Also, if network login is enabled, EAPOL flooding cannot be enabled. However, under certain conditions, you might opt to change this behavior to support an upstream central authenticator by enabling the switch to flood the EAPOL frame on the VLAN associated with the ingress port.

Example
The following example enables EAPOL frame flooding on a Summit “e” series switch:

```
enable eapol-flooding
```

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is only available on the “e” series platforms.
enable snmp access

   enable snmp access

Description
Turns on SNMP support for SNMPv3 and v1/v2c on the switch.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
To have access to the SNMP agent residing in the switch, at least one VLAN must have an IP address assigned to it.

Any network manager running SNMP can manage the switch (for v1/v2c), provided the MIB is installed correctly on the management station. Each network manager provides its own user interface to the management facilities.

For SNMPv3, additional security keys are used to control access, so an SNMPv3 manager is required for this type of access.

This command enables both v1/v2c and v3 access, so the switch can be accessed with either method. Use the following commands to allow only v3 access:

   enable snmp access
disable snmp access {snmp-v1v2c}

Use the following command to prevent any SNMP access:

disable snmp access

There is no way to disable v3 access and allow v1/v2c access

Example
The following command enables all SNMP access for the switch:

   enable snmp access

History
This command was first available in ExtremeWare 2.0.

Support for SNMPv3 was added in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e. The “e” series of switches added support for SNMPv3 in ExtremeWare 7.2e.
Platform Availability

This command is available on all platforms.
enable snmp dot1dTpFdbTable

Description
Enables SNMP GetNext responses for the dot1dTpFdbTable in the BRIDGE-MIB.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
SNMP Get responses are not affected by this command.

To view the configuration of the dot1dTpFdb table on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state the dot1dTpFdb table.

To restore defaults to all SNMP-related entries, including the SNMP parameters modified using the enable snmp dot1dTpFdbTable command, use the unconfigure management command.

Example
The following command enables the dot1dTPFdb table:

```
enable snmp dot1dTpFdbTable
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable snmp traps

enable snmp traps

Description
Turns on SNMP trap support.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
An authorized trap receiver can be one or more network management stations on your network. The switch sends SNMP traps to all trap receivers.

Example
The following command enables SNMP trap support on the switch:

```
enable snmp trap
```

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable snmp traps exceed-committed-rate ports

    enable snmp traps exceed-committed-rate ports <portlist> {<Ingress QOS Profile>}

**Description**

Enables SNMP traps for the condition when ingress traffic has exceeded the configured committed-rate and is either being dropped, or is in danger of being dropped, on the indicated ports.

**Syntax Description**

| **portlist** | Specifies a list of "3" series I/O ports (in the form 2:, 2:5, or 2:6-2:8), for which the specified trap will apply. |
| **Ingress QOS Profile** | Specifies an optional ingress QOS profile. If not specified, all ingress QOS profiles for the indicated ports will be affected. |

**Default**

Disabled.

**Usage Guidelines**

This trap type was added to detect when ingress traffic exceeds the configured committed rate (CIR) or is dropped due to exceeding the configured Peak Rate (PR) or oversubscription. These conditions should also be evident via the `show port x:y ingress stats detail` command from the console. When either the Exceeds-CIR or Dropped-Bytes condition changes state, an SNMP trap will be sent to all registered trap receivers. Committed and peak rate violations will be written to the syslog when this trap is enabled. The trap that is sent to the SNMP application will consist of:

- **Trap Type** (1=Exceeded CIR, 2=Dropped Bytes)
- **Status** (1=event occurred, 0=event condition cleared)
- **Port**
- **Queue**
- **Byte count** (valid only for Status=0 to show the Exceeded/Dropped byte count)

This command affects ports on "3" series I/O Ethernet modules only, and is configurable per port (all queues) or per queue on specified ports. By default, this trap type is disabled for all queues on all ports.

This trap type applies only to "3" series I/O-based ingress rate-limiting and ingress oversubscription, and not to "3" series I/O-based egress rate-limiting.

To see which ports have such traps enabled, use the `show config` command.

**Example**

The following command will enable exceed-committed-rate traps for all ingress QOS profiles on ports 2:5 through 2:8.

    enable snmp traps exceed-committed-rate ports 2:5-2:8
History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available on “3” series I/O modules only.
enable snmp traps mac-security

   enable snmp traps mac-security

**Description**
Enables SNMP mac-security traps for all ports to be sent by the switch.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled.

**Usage Guidelines**
This command should be used in conjunction with the `configure ports <portlist> limit-learning` command. That command configures a limit on the number of MAC addresses that can be learned on a port(s). After that limit has been reached on a particular port, a trap will be sent by the switch, if a new MAC address appears on that port. In addition, a message will be generated in the syslog and the port will be blackholed.

**Example**
The following command allows SNMP mac-security traps to be sent from the switch.
```
enable snmp traps mac-security
```

**History**
This command was first available in ExtremeWare 7.0.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable snmp traps port-up-down

   enable snmp traps {port-up-down ports [all | mgmt | <portlist>]}
enable sntp-client

enable sntp-client

**Description**
Enables the SNTP client.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A.

**Usage Guidelines**
SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. After the SNTP client has been enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean Time (GMT) offset and the use of Daylight Savings Time (DST).

**Example**
The following command enables the SNTP client:
```
enable sntp-client
```

**History**
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable system-watchdog

enable system-watchdog

Description
Enables the system watchdog timer.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
The watchdog timer reboots the switch if the CPU becomes trapped in a processing loop. If the watchdog timer is executed, the switch captures information on the cause of the reboot and posts it to the system log.

Example
The following command enables the watchdog timer:

enable system-watchdog

History
This command was first available in ExtremeWare 6.1.9.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable telnet

```
enable telnet {access-profile [<access_profile> | none]} {port <tcp_port_number>}
```

**Description**
Enables Telnet access to the switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntactic Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile. (6.0, 6.1)</td>
</tr>
<tr>
<td>none</td>
<td>Cancels a previously configured access profile. (6.0, 6.1)</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a TCP port number. (6.0, 6.1)</td>
</tr>
</tbody>
</table>

**Default**
Telnet is enabled with no access profile and uses TCP port number 23.

**Usage Guidelines**
You must be logged in as an administrator to enable Telnet.

If you are using IP without a BOOTP server, you must enter IP parameters for the switch for the Telnet software to communicate with the device. To assign IP parameters to the switch, you must:

- Log in to the switch with administrator privileges.
- Assign an IP address and subnet mask to a VLAN.

The switch comes configured with a default VLAN named `default`. To use Telnet or an SNMP network manager, you must have at least one VLAN on the switch, and it must be assigned an IP address and subnet mask. IP addresses are always assigned to a VLAN. The switch can be assigned multiple IP addresses.

For version 6.0 and higher:

- Use an access profile to restrict Telnet access. An access profile permits or denies a named list of IP addresses and subnet masks. You must create and configure an access profile before you can use this option. You create an access profile using the `create access-profile type` command. You configure an access profile using the `configure access-profile` command.
- Use the `none` option to cancel a previously configured access-profile.
- Use the `port` option to specify a TCP port number.

**Example**
The following command applies the access profile managers to Telnet:

```
enable telnet access-profile managers
```
**History**

This command was first available in ExtremeWare 2.0.

Support for the `access profile`, `none`, and `port` parameters was introduced in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable web

   enable web {access-profile [<access_profile> | none]} {port <tcp_port_number>}

Description
Enables ExtremeWare Vista web access to the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile. (6.0, 6.1)</td>
</tr>
<tr>
<td>none</td>
<td>Cancels a previously configured access profile. (6.0, 6.1)</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a TCP port number. (6.0, 6.1)</td>
</tr>
</tbody>
</table>

Default
Enabled, using TCP port 80.

Usage Guidelines
By default, web access is enabled on the switch.

For version 6.0 and higher:
- By default, web access has no access profile and uses TCP port number 80.
- Use an access profile to restrict ExtremeWare Vista web access. An access profile permits or denies a named list of IP addresses and subnet masks. You must create and configure an access profile before you can use this option. You create an access profile using the create access-profile type command. You configure an access profile using the configure access-profile command. Apply an access profile only when ExtremeWare Vista is enabled.
- Use the none option to cancel a previously configured access-profile.
- Use the port option to specify a TCP port number.

Example
The following command applies the access profile administrators to the web:

```
enable web access-profile administrators
```

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.0 to include the access profile and port options.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
exit

Description
Logs out the session of a current user for CLI or Telnet.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Use this command to log out of a CLI or Telnet session.

Example
The following command logs out the session of a current user for CLI or Telnet:
exit

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on Summit switches.
logout

Description
Logs out the session of a current user for CLI or Telnet.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Use this command to log out of a CLI or Telnet session.

Example
The following command logs out the session of a current user for CLI or Telnet:

```plaintext
logout
```

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
quit

Description
Logs out the session of a current user for CLI or Telnet.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Use this command to log out of a CLI or Telnet session.

Example
The following command logs out the session of a current user for CLI or Telnet:

quit

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show eapol-flooding

Description
Displays the current EAPOL flooding state.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Per IEEE 802.1D, Summit “e” series switches do not forward EAPOL frames. Also, if network login is enabled, EAPOL flooding cannot be enabled. Also, if network login is enabled, EAPOL flooding cannot be enabled. However, under certain conditions, you might opt to change this behavior to support an upstream central authenticator by enabling the switch to flood the EAPOL frame on the VLAN associated with the ingress port.

Example
The following example displays EAPOL frame flooding on a Summit “e” series switch:

show eapol-flooding

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is available on the “e” series platforms.
show management

Description
Displays the SNMP settings configured on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines:
The following show management output is displayed:
- Enable/disable state for Telnet, SNMP, and web access
- SNMP community strings
- Authorized SNMP station list
- SNMP trap receiver list
- Login statistics

For ExtremeWare 4.0 and higher, the following show management output is also displayed:
- Enable/disable state for SSH2 and access profile information
- RMON polling configuration

For ExtremeWare 6.2.2 and higher, the enable/disable state of the port-up-down traps is also displayed.

For ExtremeWare 7.0.0 and higher, the enable/disable state of the mac-limit traps is also displayed.

For the “i” Series of Switches. For ExtremeWare 7.1.0 and higher, the SNMP access display item will show the additional states of v1, v2c disabled and v3 enabled. The flags field was enhanced to show the SNMP trap groups.

For the “e” Series of Switches. For ExtremeWare 7.2e and higher, the SNMP access display item will show the additional states of v1, v2c disabled and v3 enabled. The flags field was enhanced to show the SNMP trap groups.

Example
The following command displays configured SNMP settings on the switch:

show management

Following is the output from this command:
Commands for Managing the Switch

CLI idle timeouts: disabled
CLI Paging: enabled
CLI configuration logging: enabled
Telnet access: enabled tcp port: 23
Web access: enabled tcp port: 80
Web access login timeout: 30 secs
SSH Access: key invalid, disabled tcp port: 22
UDP Echo Server: disabled udp port: 7
SNMP Access: v1v2c disabled; v3 enabled
SNMP Read Only Communities: rykfcb
Total Read Only Communities: 1
SNMP Read Write Communities: r~`|kug
Total Read Write Communities: 1
SNMP dot1dTpFdbTable: disabled
RMON polling: disabled
SNMP Traps: enabled

SNMP v1/v2c Trap Receivers:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Community</th>
<th>Source IP Address</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.255.254.22 /16</td>
<td>public</td>
<td>2EA</td>
<td></td>
</tr>
<tr>
<td>111.111.111.111/16</td>
<td>ThisIsATestComm</td>
<td>2SA</td>
<td></td>
</tr>
</tbody>
</table>

Flags: Version: 1=v1 2=v2c
Mode: S=Standard E=Enhanced
Trap Groups: s=STP b=BGP p=OSPF v=VRRP y=System
e=Extreme m=Smart Traps a=Auth l=Link Up/Down r=RMON
c=Security
A=All

SNMP MAC Security traps: disabled
Link Up/Link Down traps enabled on ports: All, including MgmtPort

SNMP stats:
inPkts 301 outPkts 302 errors 0 authErrors 0
Gets 93 GetNexts 208 Sets 0

SNMP traps: sent 10 authTraps enabled

Login stats:
validLogins 3 badPasswords 0 unknownUSers 2 (last bad user: admin1)
Telnet: total 3 valid 1 invalid 2
HTTP: total 0 valid 0 invalid 0

Management access stats:

<table>
<thead>
<tr>
<th>Protocol</th>
<th>UDP/TCP</th>
<th>Port</th>
<th>Total packets</th>
<th>Rejected packets</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Sourse IP Address</th>
<th>UDP/TCP</th>
<th>Port</th>
<th>Time</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

History

This command was first available in ExtremeWare 2.0.

Support for the SSH2 state, access profile information and RMON polling configuration was introduced in ExtremeWare 4.0.

Additional information on traps configured per port port-up-down traps was added in ExtremeWare 6.2.2.

Additional information on mac-limit traps was added in ExtremeWare 7.0.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
show odometer

show odometer

Description
Displays a counter for each component of a switch that shows how long it has been functioning since it was manufactured.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
The output from this command displays how long each individual component in the whole switch has been functioning since it is manufactured. This odometer counter will be kept in the EEPROM of each monitored component. This means that even when the component is plugged into different chassis, the odometer counter will be available in the new switch chassis. The following components are monitored by the odometer:

- For the Black Diamond—MSM and I/O modules
- For the Alpine—SMM, I/O slots, and power supplies
- For stackable switches—the CPU

Example
The following command displays how long each component of a switch has been functioning since it’s manufacture date:

show odometer

The following is the output from this command from an “e” series switch:

* Summit300-24:13 # show odometer

<table>
<thead>
<tr>
<th>Unit</th>
<th>Service Days</th>
<th>First Recorded Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mainboard:</td>
<td>22</td>
<td>Jan-17-2065</td>
</tr>
</tbody>
</table>

The following is the output from this command from an “i” series switch:

* Alpine3804:4 # show odometers

<table>
<thead>
<tr>
<th>Field Replaceable Units</th>
<th>Service Days</th>
<th>First Recorded Start Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backplane:</td>
<td>145</td>
<td>Jan-22-2003</td>
</tr>
<tr>
<td>SMM:</td>
<td>145</td>
<td>Jan-22-2003</td>
</tr>
<tr>
<td>Slot 1:</td>
<td>Empty</td>
<td></td>
</tr>
</tbody>
</table>
show odometer

<table>
<thead>
<tr>
<th>Slot 2:</th>
<th>WM4T1</th>
<th>234</th>
<th>Oct-25-2002</th>
</tr>
</thead>
<tbody>
<tr>
<td>Slot 3:</td>
<td>FM8V</td>
<td>145</td>
<td>Jan-22-2003</td>
</tr>
<tr>
<td>Slot 4:</td>
<td>GM4X</td>
<td>145</td>
<td>Jan-22-2003</td>
</tr>
<tr>
<td>Upper PS:</td>
<td>PSU-A</td>
<td>292</td>
<td>Apr-12-2002</td>
</tr>
<tr>
<td>Lower PS:</td>
<td>PSU-B</td>
<td>N/A</td>
<td>N/A</td>
</tr>
</tbody>
</table>

**History**

This command was first available in ExtremeWare 6.2.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show session

show session

Description
Displays the currently active Telnet, console, and web sessions communicating with the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
The show session command displays the username and IP address of the incoming Telnet session, whether a console session is currently active, and the login time.

The following table displays the show session command field definitions.

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Indicates session number.</td>
</tr>
<tr>
<td>Login Time</td>
<td>Indicates login time of session.</td>
</tr>
<tr>
<td>User</td>
<td>Indicates the user logged in for each session.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the type of session.</td>
</tr>
<tr>
<td>Auth</td>
<td>Indicates how the user is logged in.</td>
</tr>
<tr>
<td>CLI Auth</td>
<td>Indicates the type of authentication (RADIUS and TACAS) if enabled.</td>
</tr>
<tr>
<td>Location</td>
<td>Indicates the location (IP address) from which the user logged in.</td>
</tr>
</tbody>
</table>

Example
The following command displays the active sessions on the switch:

show session

Following is the output from this command:

<table>
<thead>
<tr>
<th>#</th>
<th>Login Time</th>
<th>User</th>
<th>Type</th>
<th>Auth</th>
<th>CLI Auth</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Tue Feb 19 18:08:42 2002</td>
<td>admin</td>
<td>console</td>
<td>local</td>
<td>disabled</td>
<td>serial</td>
</tr>
<tr>
<td>5</td>
<td>Thu Feb 21 19:09:48 2002</td>
<td>admin</td>
<td>http</td>
<td>local</td>
<td>disabled</td>
<td>10.0.4.76</td>
</tr>
<tr>
<td>*</td>
<td>1028 Thu Feb 21 18:56:40 2002</td>
<td>admin</td>
<td>telnet</td>
<td>local</td>
<td>disabled</td>
<td>10.0.4.19</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 2.0.
Support for the Auth command field definition was introduced in ExtremeWare 4.0.
Support for the CLI Auth command field definition was introduced in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show snmpv3 access

  show snmpv3 access {hex <hex value>} | <group name>}

Description
Displays SNMPv3 access rights.

Syntax Description

<table>
<thead>
<tr>
<th>hex</th>
<th>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>group name</td>
<td>Specifies the name of the group to display.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The show snmpv3 access command displays the access rights of a group. If you do not specify a group name, the command will display details for all the groups.

This command displays the SNMPv3 VACMAccessTable entries.

Example
The following command displays all the access details:

  show snmpv3 access

Output from the command is similar to:

  Group Name       : admin
  Context Prefix   :
  Security Model   : USM
  Security Level   : Authentication Privacy
  Context Match    : Exact
  Read View        : defaultAdminView
  Write View       : defaultAdminView
  Notify View      : defaultNotifyView
  Storage Type     : Permanent
  Row Status       : Active

  Group Name       : initial
  Context Prefix   :
  Security Model   : USM
  Security Level   : No-Authentication No-Privacy
  Context Match    : Exact
  Read View        : defaultUserView
  Write View       :
  Notify View      : defaultNotifyView
  Storage Type     : Permanent
Row Status : Active

Group Name : initial
Context Prefix :
Security Model : USM
Security Level : Authentication No-Privacy
Context Match : Exact
Read View : defaultUserView
Write View : defaultUserView
Notify View : defaultNotifyView
Storage Type : Permanent
Row Status : Active

Group Name : v1v2c_ro
Context Prefix :
Security Model : snmpv1
Security Level : No-Authentication No-Privacy
Context Match : Exact
Read View : defaultUserView
Write View :
Notify View : defaultNotifyView
Storage Type : Permanent
Row Status : Active

Group Name : v1v2c_ro
Context Prefix :
Security Model : snmpv2c
Security Level : No-Authentication No-Privacy
Context Match : Exact
Read View : defaultUserView
Write View :
Notify View : defaultNotifyView
Storage Type : Permanent
Row Status : Active

Group Name : v1v2c_rw
Context Prefix :
Security Model : snmpv1
Security Level : No-Authentication No-Privacy
Context Match : Exact
Read View : defaultUserView
Write View :
Notify View : defaultNotifyView
Storage Type : Permanent
Row Status : Active

Group Name : v1v2c_rw
Context Prefix :
Security Model : snmpv2c
Security Level : No-Authentication No-Privacy
Context Match : Exact
Read View : defaultUserView
Write View :
Notify View : defaultNotifyView
Storage Type : Permanent
Row Status : Active
Group Name     : v1v2cNotifyGroup
Context Prefix  :
Security Model  : snmpv1
Security Level  : No-Authentication No-Privacy
Context Match   : Exact
Read View       :
Write View      :
Notify View     : defaultNotifyView
Storage Type    : Permanent
Row Status      : Active

Group Name     : v1v2cNotifyGroup
Context Prefix  :
Security Model  : snmpv2c
Security Level  : No-Authentication No-Privacy
Context Match   : Exact
Read View       :
Write View      :
Notify View     : defaultNotifyView
Storage Type    : Permanent
Row Status      : Active

Total num. of entries in vacmAccessTable : 9

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show snmpv3 context

Description
Displays information about the SNMPv3 contexts on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines:
This command displays the entries in the View-based Access Control Model (VACM) context table (VACMContextTable).

Example
The following command displays information about the SNMPv3 contexts on the switch:
show snmpv3 context

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show snmpv3 counters

Description
Displays SNMPv3 counters.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
The show snmpv3 counters command displays the following SNMPv3 counters:

- snmpUnknownSecurityModels
- snmpInvalidMessages
- snmpUnknownPDUHandlers
- usmStatsUnsupportedSecLevels
- usmStatsNotInTimeWindows
- usmStatsUnknownUserNames
- usmStatsUnknownEngineIDs
- usmStatsWrongDigests
- usmStatsDecryptionErrors

Issuing the command clear counters will reset all counters to zero.

Example
The following command displays all the SNMPv3 counters:

show snmpv3 counters

Output of the command is similar to:

snmpUnknownSecurityModels : 0
snmpInvalidMessages : 0
snmpUnknownPDUHandlers : 0
usmStatsUnsupportedSecLevels : 0
usmStatsNotInTimeWindows : 0
usmStatsUnknownUserNames : 0
usmStatsUnknownEngineIDs : 0
usmStatsWrongDigests : 0
usmStatsDecryptionErrors : 0
**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
show snmpv3 engine-info

    show snmpv3 engine-info

**Description**
Displays information about the SNMPv3 engine on the switch.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A.

**Usage Guidelines:**
The following show engine-info output is displayed:
- EngineID—Either the ID auto generated from MAC address of switch, or the ID manually configured.
- EngineBoots—Number of times the agent has been rebooted.
- EngineTime—Time since agent last rebooted, in centiseconds.
- Max. Message Size—Maximum SNMP Message size supported by the Engine (8192).

**Example**
The following command displays information about the SNMPv3 engine on the switch:
show snmpv3 engine-info

The following is output from this command:

```
SNMP Engine-ID : 80:00:07:7c:03:00:01:30:23:c1:00 'H'
SNMP Engine Boots : 4
SNMP Engine Time : 1852673
SNMP Max. Message Size : 8192
```

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
show snmpv3 extreme-target-addr-ext

show snmpv3 extreme-target-addr-ext {hex <hex value>} <addr name>

Description
Display information about SNMPv3 target addresses enhanced or standard mode.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated</td>
</tr>
<tr>
<td>addr name</td>
<td>Specifies a string identifier for the target address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to display entries in the SNMPv3 extremeTargetAddressExtTable.

Example
The following command displays the entry for the target address named v1v2cNotifyTAddr1:

show snmpv3 extreme-target-addr-ext v1v2cNotifyTAddr1

The output of the command is similar to:

Target Addr Name : v1v2cNotifyTAddr1
Mode             : Enhanced
IgnoreMPModel    : Yes
UseEventComm     : Yes

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show snmpv3 filter

    show snmpv3 filter {{hex <hex value>} <profile name> {{subtree} <object identifier>}

Description
Display the filters that belong a filter profile.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>hex</strong></td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td><strong>profile name</strong></td>
<td>Specifies the filter profile to display.</td>
</tr>
<tr>
<td><strong>object identifier</strong></td>
<td>Specifies a MIB subtree.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to display entries from the snmpNotifyFilterTable. If you specify a profile name and subtree, you will display only the entries with that profile name and subtree. If you specify only the profile name, you will display all entries for that profile name. If you do not specify a profile name, then all the entries are displayed.

Example
Use the following command to display the part of filter profile *filter1* that includes the MIB subtree 1.3.6.1.1.2:

```
show snmpv3 filter filter1 subtree 1.3.6.1.1.2
```

Output from the command is similar to:

```
Filter Profile Name : filter1
Subtree             : 1.3.6.1.1.2
Mask                :
Type                : Included
Storage Type        : NonVolatile
Row Status          : Active
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show snmpv3 filter-profile

show snmpv3 filter-profile {{hex <hex value>} <profile name>} {param {hex <hex value>} <param name>}

Description
Display the association between parameter names and filter profiles.

Syntax Description

<table>
<thead>
<tr>
<th>hex</th>
<th>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile name</td>
<td>Specifies the filter profile name.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies the parameter name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to display the snmpNotifyFilterProfileTable. This table associates a filter profile with a parameter name. The parameter name is associated with target addresses, and the filter profile is associated with a series of filters, so, in effect, you are associating a series of filters with a target address.

Example
Use the following command to display the entry with filter profile fpro1 with the parameter name param1:

```
show snmpv3 filter-profile fpro-1 param param1
```

Output from the command is similar to:

```
Filter Profile Params Name : param1
Name                      : fpro-1
Storage Type              : NonVolatile
Row Status                : Active
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show snmpv3 group

    show snmpv3 group {hex <hex value> | <group name>} {user {hex <hex value>} | <user name>}

Description
Displays the user name (security name) and security model association with a group name.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>group name</td>
<td>Specifies the group name to display.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name to display.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The `show snmpv3 group` command displays the details of a group with the given group name. If you do not specify a group name, the command will display details for all the groups.

Example
The following command displays information about all groups for every security model and user name:

    show snmpv3 group

The following command shows information about all groups:

    show snmpv3 group

The output of the command is similar to:

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Security Name</th>
<th>Security Model</th>
<th>Storage Type</th>
<th>Row Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1v2c_ro</td>
<td>v1v2c_ro</td>
<td>snmpv1</td>
<td>Permanent</td>
<td>Active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Security Name</th>
<th>Security Model</th>
<th>Storage Type</th>
<th>Row Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1v2c_rw</td>
<td>v1v2c_rw</td>
<td>snmpv1</td>
<td>Permanent</td>
<td>Active</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Group Name</th>
<th>Security Name</th>
<th>Security Model</th>
<th>Storage Type</th>
<th>Row Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1v2c_ro</td>
<td>v1v2c_ro</td>
<td>snmpv2c</td>
<td>Permanent</td>
<td></td>
</tr>
<tr>
<td>Row Status</td>
<td>Group Name</td>
<td>Security Name</td>
<td>Security Model</td>
<td>Storage Type</td>
</tr>
<tr>
<td>------------</td>
<td>------------</td>
<td>---------------</td>
<td>----------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Active</td>
<td>v1v2c_rw</td>
<td>v1v2c_rw</td>
<td>snmpv2c</td>
<td>Permanent</td>
</tr>
<tr>
<td>Active</td>
<td>admin</td>
<td>admin</td>
<td>USM</td>
<td>Permanent</td>
</tr>
<tr>
<td>Active</td>
<td>initial</td>
<td>initial</td>
<td>USM</td>
<td>Permanent</td>
</tr>
<tr>
<td>Active</td>
<td>initial</td>
<td>initialmd5</td>
<td>USM</td>
<td>Permanent</td>
</tr>
<tr>
<td>Active</td>
<td>initial</td>
<td>initialsha</td>
<td>USM</td>
<td>Permanent</td>
</tr>
<tr>
<td>Active</td>
<td>initial</td>
<td>initialmd5Priv</td>
<td>USM</td>
<td>Permanent</td>
</tr>
<tr>
<td>Active</td>
<td>initial</td>
<td>initialshaPriv</td>
<td>USM</td>
<td>Permanent</td>
</tr>
</tbody>
</table>

Total num. of entries in vacmSecurityToGroupTable : 10

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show snmpv3 mib-view

show snmpv3 mib-view {{hex <hex value>} | <view name>} {subtree <object identifier>}

Description
Displays a MIB view.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>view name</td>
<td>Specifies the name of the MIB view to display.</td>
</tr>
<tr>
<td>subtree</td>
<td>Specifies the object identifier of the view to display.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays a MIB view. If you do not specify a view name, the command will display details for all the MIB views. If a subtree is not specified, then all subtrees belonging to the view name will be displayed.

This command displays the SNMPv3 VACMViewsTreeFamilyTable.

Example
The following command displays all the view details:

```
show snmpv3 mib-view
```

The following command displays a view with the view name Roview and subtree 1.3.6.1.2.1.1:

```
show snmpv3 mib-view Roview subtree 1.3.6.1.2.1.1
```

Output from the command is similar to:

```
View Name     : defaultUserView
MIB Subtree   : 1
Mask          :
View Type     : Included
Storage Type  : Permanent
Row Status    : Active

View Name     : defaultUserView
MIB Subtree   : 1.3.6.1.6.3.16
Mask          :
View Type     : Excluded
Storage Type  : Permanent
Row Status    : Active
```
View Name     : defaultUserView  
MIB Subtree   : 1.3.6.1.6.3.18  
Mask          :  
View Type     : Excluded  
Storage Type  : Permanent  
Row Status    : Active  

View Name     : defaultUserView  
MIB Subtree   : 1.3.6.1.6.3.15.1.2.2.1.4  
Mask          :  
View Type     : Excluded  
Storage Type  : Permanent  
Row Status    : Active  

View Name     : defaultUserView  
MIB Subtree   : 1.3.6.1.6.3.15.1.2.2.1.6  
Mask          :  
View Type     : Excluded  
Storage Type  : Permanent  
Row Status    : Active  

View Name     : defaultUserView  
MIB Subtree   : 1.3.6.1.6.3.15.1.2.2.1.9  
Mask          :  
View Type     : Excluded  
Storage Type  : Permanent  
Row Status    : Active  

View Name     : defaultAdminView  
MIB Subtree   : 1  
Mask          :  
View Type     : Included  
Storage Type  : Permanent  
Row Status    : Active  

View Name     : defaultNotifyView  
MIB Subtree   : 1  
Mask          :  
View Type     : Included  
Storage Type  : Permanent  
Row Status    : Active  

Total num. of entries in vacmViewTreeFamilyTable : 8

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show snmpv3 notify

    show snmpv3 notify {hex <hex value>} <notify name>

**Description**
Display the notifications that are set. This command displays the snmpNotifyTable.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies the parameter name associated with the target.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Use this command to display entries from the SNMPv3 snmpNotifyTable. This table lists the notify tags that the agent will use to send notifications (traps).

If no notify name is specified, all the entries are displayed.

**Example**
The following command displays the notify table entry for N1:

```
show snmpv3 notify N1
```

**History**
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
show snmpv3 target-addr

    show snmpv3 target-addr {{hex <hex value>} | <addr name>}

**Description**
Display information about SNMPv3 target addresses.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>addr name</td>
<td>Specifies a string identifier for the target address.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Use this command to display entries in the SNMPv3 snmpTargetAddressTable. If no target address is specified, the entries for all the target addresses will be displayed.

**Example**
The following command displays the entry for the target address named `tgtaddr1`:

```
show snmpv3 target-addr tgtaddr1
```

Output of the command is similar to:

```
Target Addr Name    : tgtaddr1
TDomain             : 1.3.6.1.6.1.1
TAddress            : 10.36.11.187, 162
TMask               : 
Timeout             : 1500
Retry Count         : 0
Tag List            : defaultNotify
Params              : param1
Storage Type        : NonVolatile
Row Status          : 
```

**History**
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
show snmpv3 target-params

show snmpv3 target-params [{hex <hex value>} | <param name>}

Description
Display the information about the options associated with the parameter name.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>param name</td>
<td>Specifies the parameter name to display.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to display entries from the SNMPv3 snmpTargetParamsTable. This table specifies the message processing model, security level, security model, and the storage parameters for messages to any target addresses associated with a particular parameter name.

If no parameter name is specified, all the entries are displayed.

Example
The following command displays the target parameter entry named param1:

show snmpv3 target-params param1

Output from the command is similar to:

Target Params Name : param1
MP Model : snmpv3
Security Model : USM
User Name : user1
Security Level : No-Authentication No-Privacy
Storage Type : NonVolatile
Row Status : Active

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show snmpv3 user

    show snmpv3 user {{hex <hex value>} <user name>}

Description
Displays detailed information about the user.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies that the value to follow is to be supplied as a colon separated string of hex octets.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name to display.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The show snmpv3 user command displays the details of a user. If you do not specify a user name, the command will display details for all the users. The authentication and privacy passwords and keys will not be displayed.

The user entries in SNMPv3 are stored in the USMUserTable, so the entries are indexed by EngineID and user name.

Example
The following command lists all user entries:

    show snmpv3 user

The following command lists details for the specified user, admin:

    show snmpv3 user admin

Output from the command is similar to:

| Engine-ID         | 80:00:07:7c:03:00:e0:2b:80:07:00 'H' |
| User Name         | admin                                |
| Security Name     | admin                                |
| Authentication    | HMAC-MD5                              |
| Privacy           | DES                                   |
| Storage Type      | Permanent                             |
| Row Status        | Active                                |

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show sntp-client

Description
Displays the DNS configuration.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Displays configuration and statistics information of SNTP client.

Example
The following command displays the DNS configuration:
show sntp-client

Following is the output from this command:

SNTP client is enabled
SNTP time is valid
Primary server: 172.17.1.104
Secondary server: 172.17.1.104
Query interval: 64
SNTPC Statistics:
Packets transmitted:
to primary server: 1
to secondary server: 0
Packets received with valid time:
from Primary server: 1
from Secondary server: 0
from Broadcast server: 0
Packets received without valid time:
from Primary server: 0
from Secondary server: 0
from Broadcast server: 0
Replies not received to requests:
from Primary server: 0
from Secondary server: 0

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
show vlan dhcp-address-allocation

    show vlan <vlan name> dhcp-address-allocation

Description
Displays DHCP address allocation information about VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Summary information for all VLANs on the device.

Usage Guidelines
Display the IP address, MAC address, and time assigned to each end device.

Example
The following command displays DHCP address allocation information about VLAN temp:

    show vlan temp dhcp-address-allocation

Output from the command is similar to:

========================================================================
<table>
<thead>
<tr>
<th>IP</th>
<th>MAC</th>
<th>Lease Renewal Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.0.0.15</td>
<td>00:08:A1:5F:9B:30</td>
<td>00:00:09</td>
</tr>
</tbody>
</table>
========================================================================

History
This command was first available in ExtremeWare 6.2.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show vlan dhcp-config

    show vlan <vlan-name> dhcp-config

Description
Displays the DHCP configuration for a specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN for which the DHCP configuration is to be displayed. If no VLAN name is specified, summary configuration information is shown for all VLANs on the device.</td>
</tr>
</tbody>
</table>

Default
If no VLAN name is specified, summary information is displayed by default or all VLANs on the device.

Usage Guidelines
This command displays the DHCP configuration for the specified VLAN.

With the multinetting feature it is possible to configure DHCP address ranges belonging to the local subnet (primary subnet/secondary subnet) and also remote subnets. The output for this command has groups and displays DHCP address ranges (Primary DHCP Address Range followed by Secondary and Remote Subnet Ranges). In addition, the output displays lease timer values in the beginning of the output (“Netlogin Lease Timer: (and) DHCP Lease Timer:”)

Example
The following example shows output for the show vlan dhcp-config command, where the VLAN named vlantest3 is configured with a primary DHCP address range, a secondary subnet DHCP address range, and is also configured to provide addresses for a remote subnet.: 

show vlan vlantest3 dhcp-config

Following is sample output from this command:

Netlogin Lease Timer: Not configured (Default = 10 secs)
DHCP Lease Timer: Not configured (Default = 7200 secs)
Primary DHCP Range: 11.3.3.5->11.3.3.20
Secondary DHCP Range 1: 11.4.3.5->11.4.3.20
Remote DHCP Range: 99.0.0.5->99.0.0.10
Ports DHCP Enabled: 25

History
The output for this command has been changed to accommodate the multinetting feature by including DHCP address ranges for primary/secondary and remote subnets. This modified command was made available in ExtremeWare 7.3.0.
Platform Availability

This command is available on the “i” series platform only.
### telnet

```
telnet [<ipaddress> | <hostname>] {<port_number>}
```

**Description**

Allows you to Telnet from the current command-line interface session to another host.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the host.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the name of the host. (4.x and higher)</td>
</tr>
<tr>
<td>port_number</td>
<td>Specifies a TCP port number. (4.x and higher)</td>
</tr>
</tbody>
</table>

**Default**

Enabled. If the TCP port number is not specified, the Telnet session defaults to port 23.

**Usage Guidelines**

Only VT100 emulation is supported.

Any workstation with a Telnet facility should be able to communicate with the switch over a TCP/IP network.

You need to configure the switch IP parameters.

Up to eight active Telnet sessions can access the switch concurrently. If idletimeouts are enabled, the Telnet connection will time out after 20 minutes of inactivity. If a connection to a Telnet session is lost inadvertently, the switch terminates the session within two hours.

Before you can start a Telnet session, you need to configure the switch IP parameters. To open a Telnet connection, you must specify the host IP address or the host name of the device you wish to manage. Check the user manual supplied with the Telnet facility if you are unsure of how to do this.

To view the status of Telnet on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for Telnet.

For version 4.x and higher:

- You must configure DNS in order to use the `hostname` option.

For version 2.0:

- The `hostname` parameter is not available.

**Example**

The following command configures Telnet communication with a host at IP address 123.45.67.8:

```
telnet 123.45.67.8
```
**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.x to support the `hostname` and `port number` parameters.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
unconfigure management

unconfigure management

Description
Restores default values to all SNMP-related entries.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command restores default values to all SNMP-related entries on the switch:
unconfigure management

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
This chapter describes:

- Commands related to enabling, disabling, and configuring individual ports
- Commands related to configuring port speed (Fast Ethernet ports only) and half- or full-duplex mode
- Commands related to creating load-sharing groups on multiple ports
- Commands related to displaying port statistics
- Commands related to enabling and disabling loopback detection

By default, all ports on the switch are enabled. After you configure the ports to your specific needs, you can select which ports are enabled or disabled.

Fast Ethernet ports can connect to either 10Base-T or 100Base-T networks. By default, the ports autonegotiate (automatically determine) the port speed. You can also configure each port for a particular speed (either 10 Mbps or 100 Mbps).

Gigabit Ethernet ports are statically set to 1 Gbps, and their speed cannot be modified.

The switch comes configured to use autonegotiation to determine the port speed and duplex setting for each port. You can select to manually configure the duplex setting and the speed of 10/100 Mbps ports, and you can manually configure the duplex setting on Gigabit Ethernet ports.

All ports on the switch can be configured for half-duplex or full-duplex operation. The ports are configured to autonegotiate the duplex setting, but you can manually configure the duplex setting for your specific needs.

Flow control is supported only on "i" series Gigabit Ethernet ports. It is enabled or disabled as part of autonegotiation. If autonegotiation is set to off, flow control is disabled. When autonegotiation is turned on, flow control is enabled.

Load sharing with Extreme Networks switches allows you to increase bandwidth and resilience between switches by using a group of ports to carry traffic in parallel between switches. The sharing algorithm allows the switch to use multiple ports as a single logical port. For example, VLANs see the load-sharing group as a single logical port. The algorithm also guarantees packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.
Load sharing is most useful in cases where the traffic transmitted from the switch to the load-sharing group is sourced from an equal or greater number of ports on the switch. For example, traffic transmitted to a two-port load-sharing group should originate from a minimum of two other ports on the same switch.

You can view port status on the switch using the `show ports` commands. These commands, when used with specific keywords and parameters, allow you to view various issues such as real-time collision statistics, link speed, and packet size. On the “i” series of switches, flow control can also be viewed with the `show ports` command.

Commands that require you to enter one or more port numbers use the parameter `<portlist>` in the syntax. On a modular switch, a `<portlist>` can be a list of slots and ports. On a stand-alone switch, a `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Link Aggregation Control Protocol (LACP) is an extension to the existing sharing implementation. It provides several features:

- LACP protocol control of sets of links
- Loopback detection
- Configuration verification for systems connected using LACP
clear slot

clear slot <slot>

Description
Clears a slot of a previously assigned module type.

Syntax Description

| slot | Specifies a modular switch slot number. |

Default
N/A

Usage Guidelines
All configuration information related to the slot and the ports on the module is erased. If a module is present when you issue this command, the module is reset to default settings.

If a slot is configured for one type of module, and a different type of module is inserted, the inserted module is put into a mismatch state (where the inserted module does not match the configured slot), and is not brought online. To use the new module type in a slot, the slot configuration must be cleared or configured for the new module type. Use the configure slot command to configure the slot.

For version 6.0 and later:
• This command is available on modular switches.

For version 4.0:
• This command is available on BlackDiamond switches only.

Example
The following command clears slot 2 of a previously assigned module type:
clear slot 2

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on modular switches only.
configure backplane-ls-policy

configure backplane-ls-policy [address-based | port-based | round-robin]

**Description**

Selects a load-sharing policy for the backplane on a BlackDiamond switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address-based</td>
<td>Specifies address-based algorithm.</td>
</tr>
<tr>
<td>port-based</td>
<td>Specifies port-based algorithm.</td>
</tr>
<tr>
<td>round-robin</td>
<td>Specifies round-robin algorithm.</td>
</tr>
</tbody>
</table>

**Default**

Port-based

**Usage Guidelines**

On BlackDiamond switches, you can specify the backplane load-sharing policy to use. There are multiple paths that a packet can travel from the MSM to an I/O module, so this command sets the algorithm used to choose the path for each packet crossing the backplane. Selecting a policy for a particular situation will depend on the type of traffic and network topology, however, for many situations an address-based policy will enhance performance over other policies. You must save for changes to be saved across reboots.

**Example**

The following command sets the backplane load-sharing policy to address-based:

```
configure backplane-ls-policy address-based
```

**History**

This command was first available in ExtremeWare 6.2.2.

**Platform Availability**

This command is available only on BlackDiamond switches.
configure ip-mtu vlan

configure ip-mtu <number> vlan <vlan name>

Description
Sets the maximum transmission unit (MTU) for the VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>number</th>
<th>Specifies the IP MTU value. Range is from 1500 to 9194.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
The default IP MTU size is 1500.

Usage Guidelines
Use this command to enable jumbo frame support or for IP fragmentation with jumbo frames. Jumbo frames are Ethernet frames that are larger than 1522 bytes, including 4 bytes used for CRC. Both endstations involved in the transfer must be capable of supporting jumbo frames. The switch does not perform IP fragmentation or participate in MTU negotiation on behalf of devices that do not support jumbo frames.

When enabling jumbo frames and setting the MTU size for the VLAN, keep in mind that some network interface cards (NICs) have a configured maximum MTU size that does not include the additional 4 bytes of CRC included in a jumbo frame configuration. Ensure that the NIC maximum MTU is at or below the maximum MTU size configured on the switch. Frames that are larger than the MTU size configured on the switch are dropped at the ingress port.

If you use IP fragmentation with jumbo frames and you want to set the MTU size greater than 1500, all ports in the VLAN must have jumbo frames enabled.

For MPLS modules: Fragmentation is based on either the minimum value of the configured MPLS IP MTU size or the configured IP MTU size for the egress VLAN.

Example
The following command sets the MTU size to 1500 for VLAN sales:

```
configure ip-mtu 1500 vlan sales
```

The following command increases the MTU size on the MPLS VLANs to accommodate the MPLS shim header:

```
configure ip-mtu 1550 vlan vlan1
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability

This command is available on all platforms.
configure jumbo-frame size

    configure jumbo-frame size <number>

Description
This command sets the maximum jumbo frame size for the switch chassis.

Syntax Description

| number    | Specifies a maximum transmission unit (MTU) size for a jumbo frame. |

Default
The default setting is 9216.

Usage Guidelines

Jumbo frames are used between endstations that support larger frame sizes for more efficient transfers of bulk data. Both endstations involved in the transfer must be capable of supporting jumbo frames.

The number keyword describes the maximum jumbo frame size “on the wire,” and includes 4 bytes of cyclic redundancy check (CRC) plus another 4 bytes if 802.1Q tagging is being used.

To enable jumbo frame support, you must configure the maximum transmission unit (MTU) size of a jumbo frame that will be allowed by the switch.

Some network interface cards (NICs) have a configured maximum MTU size that does not include the additional 4 bytes of CRC. Ensure that the NIC maximum MTU size is at or below the maximum MTU size configured on the switch. Frames that are larger than the MTU size configured on the switch are dropped at the ingress port.

For MPLS modules: You should enable jumbo frame support on the ports that are members of an MPLS VLAN. The jumbo frame size should be set to accommodate the addition of a maximally-sized label stack. For example, a jumbo frame size of at least 1530 bytes is needed to support a two-level label stack on a tagged Ethernet port and a jumbo frame size of at least 1548 bytes is needed to support a TLS encapsulated MPLS frame.

The MPLS module supports the MTU size configured using the configure jumbo-frame size command.

For version 6.1 and later:
- The jumbo_frame_mtu range is between 1523 through 9216.

For version 6.0:
- The jumbo_frame_mtu range is between 1522 through 9216.

Example
The following command configures the maximum MTU size of a jumbo frame size to 5500:

    configure jumbo-frame size 5500
History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on the “i” series platforms and on the Summit 400-48t.
configure mirroring add

configure mirroring add [<mac_address> | vlan <vlan name> {ports <port number>} | ports <portnumber> {vlan <vlan name>}]}

Description
Adds a particular mirroring filter definition on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address. (Supported in versions 2.0 - 4x only)</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portnumber</td>
<td>Specifies a port or slot and port.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
On a modular switch, <portnumber> is a slot and port in the form <slot>:<port>. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

You must enable port-mirroring using the enable mirroring command before you can configure the mirroring filter definitions.

Up to eight mirroring definitions can be added. You can mirror traffic from a VLAN, a physical port, or a specific VLAN/port combination.

Port-mirroring configures the switch to copy all traffic associated with one or more ports to a monitor port on the switch. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. The switch uses a traffic filter that copies a group of traffic to the monitor port. The traffic filter can be defined based on one of the following criteria:

- **Physical port**—All data that traverses the port, regardless of VLAN configuration, is copied to the monitor port.
- **VLAN**—All data to and from a particular VLAN, regardless of the physical port configuration, is copied to the monitor port.
- **Virtual port**—All data specific to a VLAN on a specific port is copied to the monitor port.

Up to eight mirroring filters and one monitor port can be configured on the switch. Once a port is specified as a monitor port, it cannot be used for any other function. Frames that contain errors are not mirrored.
For version 2.0 and 4.0:
In addition to the physical port, VLAN, and virtual port, the traffic filter can be defined based on the following criteria:

- **MAC source address/destination address** — All data sent to or received from a particular source or destination MAC address is copied to the monitor port.

For MAC mirroring to work correctly, the MAC address must already be present in the forwarding database (FDB). You need to enable and configure FDB for MAC mirroring to work correctly. See “FDB Commands” for more details.

**Example**

The following example sends all traffic coming into or out of a stand-alone switch on port 1 and the VLAN `default` to the mirror port:

```
configure mirroring add ports 1 vlan default
```

The following example sends all traffic coming into or out of a modular switch on slot 3, port 2 and the VLAN `default` to the mirror port:

```
configure mirroring add ports 3:2 vlan default
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.0 to discontinue support for the MAC address parameter.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to add filtering for VLANs, MAC addresses, and virtual ports.

**Platform Availability**

This command is available on all platforms.
configure mirroring delete

configure mirroring delete [mac_address | vlan <vlan name> {ports <portnumber>} | ports <portnumber> {vlan <vlan name>}] 

Description
Deletes a particular mirroring filter definition on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address. (Supported in versions 4.0 and 6.0 only)</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portnumber</td>
<td>Specifies a port or slot and port.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
On a modular switch, <portnumber> must be a slot and port in the form <slot>:<port>. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

For version 6.0:
- No longer supports using a MAC address to specify mirroring.

Example
The following example deletes the mirroring filter on a stand-alone switch defined for port 1 on VLAN default:
configure mirroring delete ports 1 vlan default

The following example deletes the mirroring filter on a modular switch defined for slot 3, port 2 on VLAN default:
configure mirroring add ports 3:2 vlan default

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.0 to discontinue support for the MAC address parameters.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to add support for VLANs and MAC addresses.
Platform Availability

This command is available on all platforms.
configure msm-failover link-action

configure msm-failover link-action [keep-links-up {preserve-state [l2 | l2_l3]} | take-links-down]

Description
Configures external port response when MSM failover occurs.

Syntax Description

<table>
<thead>
<tr>
<th>keep-links-up</th>
<th>Configures the external ports to not be reset when MSM failover occurs.</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>preserve-state</td>
<td>Configures the preservation of the link up and down states.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the MSM-3.</td>
<td></td>
</tr>
<tr>
<td>l2</td>
<td>Preserves layer 2 FDB and states (MAC FDB, load sharing, STP, EAPS, and ESRP)</td>
</tr>
<tr>
<td>l2_l3</td>
<td>Preserves layer 2 FDB and states plus layer 3 states (IPFDB, ARP, access lists, etc.)</td>
</tr>
<tr>
<td>take-links-down</td>
<td>Configures the external ports to be reset when MSM failover occurs.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
</tbody>
</table>

Default
Take-links-down

Usage Guidelines

When MSM failover occurs, external ports will not be reset if the keep-links-up option is configured.
When the keep-links-up option is configured, peer connections will not notice a link-down indication.

The keep-links-up and take-links-down options are available on the “i” series switches only.

The preserve-state option is available on the MSM-3 only.

If you enter l2, additional ESRP configuration is required to preserve the ESRP state. By default, the ESRP failover action is none. Configuring the slave to “inherit” the master’s configuration and setting the preserve state to l2 or l2_l3 is not sufficient to preserve the ESRP state.

If you enter l2_l3, the unicast hardware IP FDB is also preserved, but the full route table and routing protocol databases for OSPF, BGP, RIP, etc. are not preserved.

After a hitless failover has completed, the routing protocols initialize like they do on a full reboot. The neighboring routers see that the router has restarted and the neighbors re-route IP traffic to alternate routes until the switch has reestablished it’s routing databases.

Since existing IP traffic flows are preserved in the FDB, data continues to be forwarded for these flows during the start of the hitless failover and the traffic re-route. This has the effect of shortening or eliminating traffic hits for these flows.

The design of the neighboring router and/or the network traffic load determines whether a network re-routing operation is or is not hitless.
If you enter `l2_13`, you also need to configure ESRP for hitless failover to preserve the ESRP state.

**Example**
The following command prevents external ports from being reset when an MSM failover occurs:
```
configure msm-failover link-action keep-links-up
```

**History**
This command was first available in ExtremeWare 6.2.2.

This command was modified to add the preserve-state option in ExtremeWare 7.1.1.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure msm-failover slave-config

configure msm-failover slave-config [inherited | flash]

Description
Configures the slave MSM-3 to inherit the software configuration from the master MSM-3.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>inherited</td>
<td>Specifies that the slave MSM-3 inherits the software configuration maintained by the current master MSM-3 (this supports hitless failover).</td>
</tr>
<tr>
<td>flash</td>
<td>Specifies that the slave MSM-3 use the configuration stored in its flash memory (this is the default and does not support hitless failover).</td>
</tr>
</tbody>
</table>

Default
Flash

Usage Guidelines
If you enter the flash keyword, you cannot use the preserve-state option of the configure msm-failover link-action command.

Example
The following command configures the slave MSM-3 to inherit the software configuration from the current master MSM-3:

```
configure msm-failover slave-config inherited
```

History
This command was first available in ExtremeWare 7.1.1.

Platform Availability
This command is available on the BlackDiamond switch only.
configure msm-failover timeout

configure msm-failover timeout <time>

Description
Configures the failover timer.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time</td>
<td>Specifies the failover time. By default, the failover time is 60 seconds, and the range is 30 to 300 seconds.</td>
</tr>
</tbody>
</table>

Default
60 seconds

Usage Guidelines
For switch management functions to hitlessly transition between the master and the slave, timer expiration is required. When you initiate hitless failover, the failover timer begins.

The failover timer configures the time it takes from when hitless failover begins until the relearned layer 3 databases are linked to the FDB. All FDB entries that are not linked to one of the databases at the timeout are deleted.

The `time` parameter specifies the failover time. By default, the failover time is 60 seconds, and the range is 30 to 300 seconds.

This command is supported only on the MSM-3.

Example
The following command configures the failover time to be 120 seconds:

```
configure msm-failover timeout 120
```

History
This command was first available in ExtremeWare 7.1.1.

Platform Availability
This command is available only on the MSM-3 in the BlackDiamond switch.
configure port aggregate-bandwidth percent

configure port <portnumber> aggregate-bandwidth percent <bandwidth>

Description
Controls the egress bandwidth of a particular port by restricting it to the specified percentage.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portnumber</td>
<td>Specifies a port or slot and port.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Specifies a percentage number (1-99) of restricted aggregate bandwidth.</td>
</tr>
</tbody>
</table>

Default
The default percentage of egress bandwidth of a port is 100%.

Usage Guidelines
Port aggregate bandwidth control lets you control aggregate bandwidth of all queues of a specific port. This feature is useful if you use several queues for classifying traffic (e.g., importance, delay sensitivity, burst) and you want to restrict total bandwidth for all queues to a certain amount, while preserving the previously classified queues’ configuration.

Example
The following command restricts the egress bandwidth of port 3 on slot 1 to 20%.

```plaintext
configure port 1:3 aggregate-bandwidth percent 20
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is only available on the “i” series platforms.
configure port interpacket-gap

configure port <slot:port> interpacket-gap <byte_time>

**Description**
Configures the Interpacket Gap for a 10 Gigabit port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>byte_time</td>
<td>Specifies the Interpacket Gap byte time.</td>
</tr>
</tbody>
</table>

**Default**
The default value of the byte time is 12.

**Usage Guidelines**
The standard compliant Interpacket Gap for 10 Gigabit Ethernet interfaces is 12. Some vendors' 10 Gigabit Ethernet interfaces drop packets when packets are transmitted using a value of 12. Thus, by increasing the Interpacket Gap, packet transmission is slowed and packet loss can be minimized or prevented. The Interpacket Gap value need not be modified when interconnecting Extreme Networks switches over 10 Gigabit Ethernet links.

The allowable range for the byte time is 12-1023.

**Example**
The following command configures Interpacket Gap to 48:

```
configure port 2:1 interpacket-gap 48
```

**History**
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms that support 10 Gigabit ports.
configure ports

configure ports [<portlist> vlan <vlan name> | all] [limit-learning <number> | lock-learning | unlimited-learning | unlock-learning]

Description
Configures virtual ports for limited or locked MAC address learning.

Syntax Description

| portlist  | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8. |
| all       | Specifies that all virtual ports should be configured as indicated. |
| vlan name | Specifies the name of the VLAN. |
| limit-learning <number> | Specifies a limit on the number of MAC addresses that can be dynamically learned on the specified ports. |
| lock-learning | Specifies that the current FDB entries for the specified ports should be made permanent (static), and no additional learning should be allowed. |
| unlimited-learning | Specifies that there should not be a limit on MAC addresses that can be learned. |
| unlock-learning | Specifies that the port should be unlocked (allow unlimited, dynamic learning). |

Default
Unlimited, unlocked learning.

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Limited learning. The limited learning feature allows you to limit the number of dynamically-learned MAC addresses per VLAN. When the learned limit is reached, all new source MAC addresses are blackholed at both the ingress and egress points. This prevent these MAC addresses from learning and responding to Internet control message protocol (ICMP) and address resolution protocol (ARP) packets.

If the limit you configure is greater than the current number of learned entries, all the current learned entries are purged.

Dynamically learned entries still get aged, and can be cleared. If entries are cleared or aged out after the learning limit has been reached, new entries will then be able to be learned until the limit is reached again.

Permanent static and permanent dynamic entries can still be added and deleted using the create fdbentry and delete fdbentry commands. These override any dynamically learned entries.

For ports that have a learning limit in place, the following traffic will still flow to the port:

- Packets destined for permanent MACs and other non-blackholed MACs
- Broadcast traffic
EDP traffic

Traffic from the permanent MAC and any other non-blackholed MACs will still flow from the virtual port.

If you configure a MAC address limit on VLANS that have ESRP enabled, you should add an additional back-to-back link (that has no MAC address limit on these ports) between the ESRP-enabled switches. Doing so prevents ESRP PDU from being dropped due to MAC address limit settings.

**Port lockdown.** The port lockdown feature allows you to prevent any additional learning on the virtual port, keeping existing learned entries intact. This is equivalent to making the dynamically-learned entries permanent static, and setting the learning limit to zero. All new source MAC addresses are blackholed.

Locked entries do not get aged, but can be deleted like any other permanent FDB entries. The maximum number of permanent lockdown entries is 1024. Any FDB entries above will be flushed and blackholed during lock down.

For ports that have lockdown in effect, the following traffic will still flow to the port:
- Packets destined for the permanent MAC and other non-blackholed MACs
- Broadcast traffic
- EDP traffic

Traffic from the permanent MAC will still flow from the virtual port.

Once the port is locked down, all the entries become permanent and will be saved across reboot. When you remove the lockdown using the unlock-learning option, the learning-limit is reset to unlimited, and all associated entries in the FDB are flushed.

To verify the MAC security configuration for the specified VLAN or ports, use the following commands:

```
show vlan <vlan name> security
show ports <portlist> info detail
```

**Example**

The following command limits the number of MAC addresses that can be learned on ports 1, 2, 3, and 6 in a VLAN named *accounting*, to 128 addresses:

```
configure ports 1, 2, 3, 6 vlan accounting learning-limit 128
```

The following command locks ports 4 and 5 of VLAN *accounting*, converting any FDB entries to static entries, and prevents any additional address learning on these ports:

```
configure ports 4,5 vlan accounting lock-learning
```

The following command removes the learning limit from the specified ports:

```
configure ports 1, 2, vlan accounting unlimited-learning
```

The following command unlocks the FDB entries for the specified ports:

```
configure ports 4,5 vlan accounting unlock-learning
```
**History**
This command was first available in ExtremeWare 6.2.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure ports auto-polarity

configure ports [<portlist> | all] auto-polarity [off | on]

Description
Configures the autopolarity detection feature on the specified Ethernet ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports on the switch. May be in the form 1, 2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all of the ports on the switch.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the autopolarity detection feature on the specified ports.</td>
</tr>
<tr>
<td>on</td>
<td>Enables the autopolarity detection feature on the specified ports.</td>
</tr>
</tbody>
</table>

Default
The autopolarity detection feature is on.

Usage Guidelines
Use the all keyword to enable or disable the autopolarity detection feature on all of the Ethernet ports.

When autopolarity is disabled on one or more Ethernet ports, you can verify that status by using the command:

```
show configuration
```

This command will list the ports for which the feature has been disabled.

To verify the current autopolarity status, use the `show ports {mgmt | <portlist>| vlan <vlan name>} info {detail}` command.

Example
The following command disables the autopolarity detection feature on ports 3-5 on a Summit 200 switch:

```
configure ports 3-5 auto off
```

The following command enables the autopolarity detection feature on ports 3-5 on the Summit48si switch:

```
configure ports 3-5 auto-polarity on
```

History
This command was first available in ExtremeWare 6.2.2b108.

Platform Availability
This command is available on all platforms.
configure ports auto off

configure ports [<portlist> | all | mgmt] auto off {speed [10 | 100 | 1000]} duplex [half | full]

Description
Manually configures port speed and duplex setting configuration on one or more ports on a switch.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:a, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all configured ports on the switch. (6.1 and later) See “Usage Guidelines” for more information.</td>
</tr>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>speed [100]</td>
<td>Specifies 100 Mbps ports.</td>
</tr>
<tr>
<td>speed [1000]</td>
<td>Specifies 1000 Mbps ports. (6.1 and later)</td>
</tr>
<tr>
<td>duplex [half]</td>
<td>Specifies half duplex; transmitting and receiving data one direction at a time.</td>
</tr>
<tr>
<td>duplex [full]</td>
<td>Specifies full duplex; transmitting and receiving data at the same time.</td>
</tr>
</tbody>
</table>

Default
Auto on

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

You can manually configure the duplex setting and the speed of 10/100 Mbps ports, and you can manually configure the duplex setting on Gigabit Ethernet ports.

Fast Ethernet ports can connect to either 10BASE-T or 100BASE-T networks. By default, the ports autonegotiate port speed. You can also configure each port for a particular speed (either 10 Mbps or 100 Mbps).

Gigabit Ethernet ports are statically set to 1 Gbps, and their speed cannot be modified.

All ports on a stand-alone switch can be configured for half-duplex or full-duplex operation. By default, the ports autonegotiate the duplex setting.

In certain interoperability situations, it is necessary to turn autonegotiation off on a Gigabit Ethernet port. Even though a Gigabit Ethernet port runs only at full duplex and gigabit speeds, the command that turns off autonegotiation must still include the duplex setting.

For “I” series only. Gigabit Ethernet ports support flow control only when autonegotiation is turned on. When autonegotiation is turned off, flow control is not supported.
For version 6.1:

- The `all` parameter specifies all ports on the switch.
- The `1000` parameter specifies 1000 Mbps ports.

**Example**

The following example turns autonegotiation off for port 4 (a Gigabit Ethernet port) on a stand-alone switch:

```
configure ports 4 auto off duplex full
```

The following example turns autonegotiation off for slot 2, port 1 on a modular switch:

```
configure ports 2:1 auto off duplex full
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.1 to support the `all` parameter.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the `all` and `mgmt` keywords.

**Platform Availability**

This command is available on all platforms.
configure ports auto on

configure ports [<portlist> | mgmt | all] auto on

Description
Enables autonegotiation for the particular port type.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Specified one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3:5, 2:* , 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>mgmt</td>
<td>Specifies all configured ports on the switch. (6.1 and later) See “Usage Guidelines” for more information.</td>
</tr>
</tbody>
</table>

Default
Auto on

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The type of ports enabled for autonegotiation are 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.

For “i” series only: Flow control is supported on Gigabit Ethernet ports only. It is enabled or disabled as part of autonegotiation. If autonegotiation is set to off, flow control is disabled. When autonegotiation is turned on, flow control is enabled.

For version 6.1: The all parameter specifies all ports on the switch.

Example
The following command configures the switch to autonegotiate for ports 4 and 6 on a stand-alone switch:

```
configure ports 4,6 auto on
```

The following command configures the switch to autonegotiate for slot 1, ports 2 and 4 on a modular switch:

```
configure ports 1:2, 1:4 auto on
```
History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support the \texttt{all} parameter.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the \texttt{all} and \texttt{mgmt} keywords.

Platform Availability
This command is available on all platforms.
configure ports display-string

configure ports [<portlist> | mgmt] display-string <alphanumeric string>

Description
Configures a user-defined string for a port or group of ports.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies a user-defined display string.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The display string can be up to 16 characters. Display strings do not need to be unique for each port—you can assign the same string to multiple ports. For example, you could give all the ports that connected to a particular department a common display string.

The string is displayed in certain commands such as the show ports info command.

Example
The following command configures the user-defined string corporate for port 1 on a stand-alone switch:
configure ports 1 display-string corporate

The following command configures the user-defined string corporate for ports 3, 4, and 5 on slot 1 on a modular switch:
configure ports 1:3-5 display-string corporate

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the all and mgmt keywords.
**Platform Availability**

This command is available on all platforms.
configure ports link-detection-level

configure ports <portlist> link-detection-level <link-detection-level>

Description
Configures the link detection level.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more primary ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>link-detection-level</td>
<td>Specifies a link detection level.</td>
</tr>
</tbody>
</table>

Default
The default link detection level is 2.

Usage Guidelines
The range is 1 - 4. Table 9 lists the behavior of the switch at each level.

Table 9: Link detection level behavior

<table>
<thead>
<tr>
<th>Level</th>
<th>ISR</th>
<th>Middle Layer Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>off</td>
<td>off</td>
</tr>
<tr>
<td>2</td>
<td>on</td>
<td>off</td>
</tr>
<tr>
<td>3</td>
<td>off</td>
<td>on</td>
</tr>
<tr>
<td>4</td>
<td>on</td>
<td>on</td>
</tr>
</tbody>
</table>

Example
The following command configures the link detection level for port 3 to 4:

configure ports 3 link-detection-level 4

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is only available on the “i” series platform.
configure ports preferred-medium

configure ports <nnn> preferred-medium {copper} | {fiber} | [force]

Description
Configures the primary uplink port to use a preferred medium.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>nnn</td>
<td>Specifies the port number. Valid port numbers are 1X to 4X for fiber and ports 1 to 4 for copper.</td>
</tr>
<tr>
<td>copper</td>
<td>Specifies that the switch should always use the 10/100/1000 connection whenever a link is established, regardless whether a fiber link is also present.</td>
</tr>
<tr>
<td>fiber</td>
<td>Specifies that the switch should always use the 1 Gigabit fiber connection whenever a link is established, regardless whether a copper link is also present.</td>
</tr>
<tr>
<td>force</td>
<td>Forces the switch to switch over to the selected media type immediately (if it has link). NOTE: This option is not available on the Summit 300-24.</td>
</tr>
</tbody>
</table>

Default
The default is determined at cable installation time.

Usage Guidelines
By specifying either copper or fiber, the switch starts the assignment with that medium and uses this preferred medium the next time the switch is rebooted. However, when a failure occurs and the uplinks are swapped, the switch continues to keep that uplink assignment until another failure occurs or until the assignment is changed using the CLI. To require that the switch revert to the preferred-medium, use the force option.

Examples
The following Summit 400-48t example establishes port 4 as the primary uplink and port 4X as the redundant uplink port:

```
configure ports 4 preferred-medium copper
```

Port 4 becomes the primary uplink until a failure occurs on that link. At that time, port 4X becomes the primary uplink and port 4 becomes the redundant port. This assignment stays in place until the next failure.

The following example forces the switch to use the fiber port whenever it has a link:

```
configure ports 3 preferred-medium fiber force
```

In this example, port 3X becomes the primary uplink port until a failure occurs on the link. At that time, port 3 becomes the primary uplink and port 3X becomes the redundant port. When port 3X re-establishes the link, port 3X becomes the primary uplink port again.

History
This command was first available in ExtremeWare 7.2.e.
Platform Availability

This command is only available on Summit 300-24 and Summit 400-48t switches.
configure ports redundant

configure ports [<portlist> | <portid>] redundant [<portlist> | <portid>]

Description
Configures a software-controlled redundant port.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more primary ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>portid</td>
<td>Specifies a primary port using the display string configured for the port. If this option is used to identify the port, the redundant port must also be specified using a port id (display string).</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more redundant ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>portid</td>
<td>Specifies a redundant port using the display string configured for the port. This option may be used to identify the redundant port of the primary port was specified using the port id (display string).</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The first port list specifies the primary ports. The second port list specifies the redundant ports.

A software-controlled redundant port is configured to backup a specified primary port. The redundant port tracks the link state of the associated primary port, and if the link on the primary port fails, the redundant port establishes a link and becomes active. You can back up a specified Ethernet port with a redundant, dedicated Ethernet port. You can also back up a load-shared group of Ethernet ports with a set of load-shared redundant Ethernet ports. If a link in the active load-shared group fails, the entire group fails over to the redundant group.

The following criteria must be considered when configuring a software-controlled redundant port:

- Redundant port configuration is model-specific. See your Consolidated Hardware Installation Guide for specific switch information.
- You must manually configure the primary and redundant ports identically in terms of VLANs, QoS settings, access lists, and so on.
- Auto-negotiation must be enabled on both the primary and redundant port.
- You cannot configure hardware redundant ports (such as ports 49 and 50 on a Summit48i) as software controlled redundant ports.
- Only one side of the link should be configured as redundant. For example, if ports 1 and 2 are connected between switches A and B, only switch A should be configured with redundant ports.
- Software redundant ports are not supported on 1000BASE-T ports.

Software redundant port only cover failures where both the TX and RX paths fail. If a single strand of fiber is pulled, the software redundant port cannot correctly recover from the failure.

**Example**

The following command configures a software-controlled redundant port on a stand-alone switch:

```plaintext
configure ports 3 redundant 4
```

The following command configures a software-controlled redundant port on a modular switch:

```plaintext
configure ports 1:3 redundant 2:3
```

The following command configures a software-controlled redundant port using the port display strings corp1 and corp5 to identify the ports:

```plaintext
configure ports corp1 redundant corp5
```

**History**

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure ports vdsl

configure ports <portlist> vdsl [5meg | 10meg | etsi]

Description
Configures VDSL ports.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. Can specify a list of slots and ports, and may be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>5meg</td>
<td>Specifies 5 Mbps.</td>
</tr>
<tr>
<td>10meg</td>
<td>Specifies 10 Mbps</td>
</tr>
<tr>
<td>etsi</td>
<td>Specifies ETSI Plan 997</td>
</tr>
</tbody>
</table>

Default
The default configuration for VDSL ports is 10 Mbps.

Usage Guidelines
Select the configuration that interoperates with the associated VDSL customer premises equipment (CPE). A lower rate may support a longer cable distance, depending on the installation.

Example
The following command configures all the VDSL ports on slot 2 to 5 Mbps:
configure ports 2:* vdsl 5meg

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on all platforms that support VDSL ports.
configure sharing address-based

For “i” series switches:

configure sharing address-based [L2 | L2_L3 | L2_L3_L4]

For “e” series switches:

configure sharing address-based [ip-dest | ip-source | ip-source-dest | mac-dest | mac-source | mac-source-dest]

Description

Configures the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
</table>
| L2     | Indicates that the switch should examine the MAC source and destination address. 
        NOTE: This option is only available on “i” series switches. |
| L2-L3  | Indicates that the switch should examine the MAC and IP source and destination address. 
        NOTE: This option is only available on “i” series switches. |
| L2-L3-L4 | Indicates that the switch should examine the MAC and IP address, and the UDP or TCP well-know port number. 
          NOTE: This option is only available on “i” series switches. |
| ip-dest | Indicates that the switch should examine the IP destination address. 
          NOTE: This option is only available on “e” series switches. |
| ip-source | Indicates that the switch should examine the IP source address. 
             NOTE: This option is only available on “e” series switches. |
| ip-source-dest | Indicates that the switch should examine the IP source and destination addresses. 
                  NOTE: This option is only available on “e” series switches. |
| mac-dest | Indicates that the switch should examine the MAC destination address. 
            NOTE: This option is only available on “e” series switches. |
| mac-source | Indicates that the switch should examine the MAC source address 
                NOTE: This option is only available on “e” series switches.. |
| mac-source-dest | Indicates that the switch should examine the MAC source and destination addresses. 
                   NOTE: This option is only available on “e” series switches. |

Default

N/A

Usage Guidelines

This feature is available using the address-based load-sharing algorithm only. The address-based load-sharing algorithm uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:

- IP packets—Uses the source and destination MAC and IP address, and the TCP port number.
- IPX packets—Uses the source and destination MAC address and IPX identifiers.
- All other packets—Uses the source and destination MAC address.

To verify your configuration, use the `show sharing address-based` command. The show sharing address-based output displays the addressed-based configurations on the switch.

**Example**
The following examples configures the switch to examine the MAC source and destination address.

On the “i” series of switches:

```
configure sharing address-based l2
```

On the “e” series of switches:

```
configure sharing address-based mac-source-dest
```

**History**
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure slot

configure slot <slot> module <module name>

Description
Configures a slot for a particular I/O module in a modular switch.

Syntax Description

<table>
<thead>
<tr>
<th>slot</th>
<th>Specifies the slot number.</th>
</tr>
</thead>
</table>
| module name | Specifies the type of module for which the slot should be configured. The list of modules you can enter will vary depending on the type of switch and version of ExtremeWare you are running. Certain modules are supported only with specific ExtremeWare Technology Releases. The following are some of the modules you may specify for a BlackDiamond switch: 10gigir—Specifies a 10 Gigabit Ethernet, 1-port, long-range, fiber module. f32fi—Specifies a Fast Ethernet, 32-port, fiber module, “i” chipset. f48t—Specifies a Fast Ethernet, 48-port, copper module. f96t—Specifies a Fast Ethernet, 96-port, copper module. g8t—Specifies a Gigabit Ethernet, 8-port, copper module. g8x—Specifies a Gigabit Ethernet, 8-port, copper module. g12sx—Specifies a Gigabit Ethernet, 12-port, fiber module. g12tx—Specifies a Gigabit Ethernet, 12-port, copper module. g16x—Specifies a Gigabit Ethernet, 16-mini-GBIC port, oversubscribed, fiber module g24t—Specifies a Gigabit Ethernet, 24-port, oversubscribed, copper module. WDMI—Specifies a Gigabit Ethernet WAN module. arm—Specifies an Accounting and Routing Module (ARM). a3c—Specifies an Asynchronous Transfer Mode (ATM) module. mpls—Specifies a MultiProtocol Label Switching (MPLS) module. p3c—Specifies an OC-3 PoS module. p12c—Specifies an OC-12 PoS module. The following are some of the modules you can specify for an Alpine switch: fm8v—Specifies a VDSL module. fm24t—Specifies a Fast Ethernet, 24-port, copper module. fm24mf—Specifies a Fast Ethernet, 24-port, multi-mode, fiber module. fm24sf—Specifies a Fast Ethernet, 24-port, single mode, fiber module. fm32pi—Specifies a Fast Ethernet, 32-port, copper power-port module. fm32t—Specifies a Fast Ethernet, 32-port, copper module. gm4s—Specifies Gigabit Ethernet, 4-port, fiber module. gm4t—Specifies a Gigabit Ethernet, 4-port, copper module. gm4x—Specifies a Gigabit Ethernet, 4-port, GBIC module. gm16x—Specifies a Gigabit Ethernet, 16-mini-GBIC port, oversubscribed, fiber module gm16t—Specifies a Gigabit Ethernet, 16-port, oversubscribed, copper module. wdmi—Specifies a Gigabit Ethernet WAN module. (6.1 or later)
Commands for Configuring Slots and Ports on a Switch

Default
If a slot has not been configured for a particular type of I/O module, then any type of module is accepted in that slot, and a default port and VLAN configuration is automatically generated.

Usage Guidelines
The `configure slot` command displays different module parameters depending on the type of modular switch you are configuring and the version of ExtremeWare running on the switch.

You can also preconfigure the slot before inserting the module. This allows you to begin configuring the module and ports before installing the module in the chassis.

If a slot has not been configured for a particular type of I/O module, then any type of module is accepted in that slot, and a default port and VLAN configuration is automatically generated. If a slot is configured for one type of module, and a different type of module is inserted, the inserted module is put into a mismatch state, and is not brought online. To use the new module type in a slot, the slot configuration must be cleared or configured for the new module type.

Upon powering up the chassis, or when an I/O module is hot-swapped, ExtremeWare automatically determines the system power budget and protects the BlackDiamond switch from any potential overpower configurations. If power is available, ExtremeWare powers on and initializes the module. When ExtremeWare detects that a module will cause an overpower condition, the module remains powered down, and is not initialized. An entry is made to the system log indicating the condition.

For version 4.0:  •This command is available on BlackDiamond switches only.

Example
The following command configures the slot for a Fast Ethernet, 32-port, copper module:
```plaintext
configure slot 2 module F32T
```

History
This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 7.0.1 to support the oversubscribed Alpine and BlackDiamond I/O modules.

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.8b12 to support MPLS modules.

This command was modified in ExtremeWare 6.1 to support the PoS modules and additional Alpine I/O modules.

This command was modified in ExtremeWare 6.0 to support the Alpine and additional BlackDiamond F48T, G8X, and G12X I/O modules.
Platform Availability

This command is available on modular switches only.
disable card-scan

disable card-scan

Description
Disables the card-scan feature on MSM slots in the BlackDiamond switch.

Syntax Description
This command has no arguments or variables.

Default
By default, card-scan is enabled.

Usage Guidelines
On certain BlackDiamond switches running earlier releases of ExtremeWare, hot insertion of a slave
MSM causes one or more of the following conditions:

- Some or all of the I/O modules are reset.
- The front panel links go down on some or all of the I/O modules.
- The backplane links go down on some or all of the I/O modules.

The card-scan feature discovers and repairs this condition, thus preventing the need for a manual reset
of the switch. When card-scan is enabled, the system logs one of the following messages if a problem
occurs when the MSM is inserted:

Cardscan (msm insert) Attempting to fix broken BP connection for slot x
Cardscan (msm insert) Attempting to fix packet missed for slot x
Cardscan (msm insert) Attempting to fix card x in reset (y)
Cardscan (timer) Attempting to fix card x in reset (y)

In these messages, x represents a slot number and y represents debugging information.

Example
The following command disables card-scan:

disable card-scan

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available only on BlackDiamond switches.
disable edp ports

    disable edp ports [<portlist> | all]

Description
Disables the Extreme Discovery Protocol (EDP) on one or more ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description: portlist</th>
<th>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports on the switch. See “Usage Guidelines” for more information.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

You can use the disable edp ports command to disable EDP on one or more ports when you no longer need to locate neighbor Extreme Networks switches.

For version 6.1:
• The all parameter specifies all ports on the switch.

For Version 6.0 and later:
• SummitLink is not supported.

For version 2.0 and 4.0:
• EDP cannot be disabled on a port that has SummitLink enabled, nor on ports that are connected to a Summit Virtual Chassis.

Example
The following command disables EDP on port 4 and port 6 on a stand-alone switch:

disable edp ports 4,6

The following command disables EDP on slot 1, ports 2 and 4 on a modular switch:

disable edp ports 1:2, 1:4
History
This command was first available in ExtremeWare 2.0.
This command was modified in ExtremeWare 4.0 to support modular switches.
This command was modified in ExtremeWare 6.1 to support the all parameter.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2e to support the all keyword.

Platform Availability
This command is available on all platforms.
disable flooding ports

    disable flooding ports <portlist>

**Description**
Disables packet flooding on one or more ports.

**Syntax Description**

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*", 2:5, 2:6-2:8. |

**Default**
Enabled

**Usage Guidelines**
Flooding configures the specified ports to act like a hub. Disabling flooding means that only broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number, are forwarded.

Disabling flooding does not automatically enable learning on the port: use the `enable learning ports` command to re-enable learning on the specified ports.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

**Example**
The following command disables flooding on ports 6, 7, and 8 on a stand-alone switch:

```
disable flooding ports 6,7,8
```

**History**
This command was first available in ExtremeWare 6.2.1.

**Platform Availability**
This command is available on “i” series platforms only.
disable jumbo-frame ports

    disable jumbo-frame ports [<portlist> | all]

**Description**
Disables jumbo frame support on a port.

**For PoS modules.** This command applies to PoS ports when disabling jumbo-frame support changes the negotiated maximum receive unit (MRU) size.

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>portlist</strong></th>
<th>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>all</strong></td>
<td>Specifies all ports on the switch.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Guidelines**
On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Use the `disable jumbo-frame ports` command when you no longer need jumbo frame support.

**Example**
The following command disables jumbo frame support on port 4 on a stand-alone switch:

```
    disable jumbo-frame ports 4
```

The following command disables jumbo frame support on slot 1, port 2 on a BlackDiamond switch:

```
    disable jumbo-frame 1:2
```

**History**
This command was first available in ExtremeWare 6.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
disable lbdetect port

    disable lbdetect port <portlist>

Description
Disables the detection of loops between ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports to be grouped to the master port. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:, 2:5, 2:6-2:8. |

Default
Disabled

Usage Guidelines
Each port may enable loop detection. This optional feature detects that a port has been looped back to the local system. If a loopback is detected, the port is disabled. Note that loopbacks may exist between different ports. The feature will disable any port that both has the feature enabled, and receives an LACP message that was sent from the local system.

Example
The following example disables loopback detection on ports 9 through 12:

disable lbdetect port 9-12

History
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
disable learning ports

disable learning ports <portlist>

Description
Disables MAC address learning on one or more ports for security purposes.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8. |

Default
Enabled

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

If MAC address learning is disabled, only broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number, are forwarded.

Use this command in a secure environment where access is granted via permanent forwarding databases (FDBs) per port.

NOTE
Disabling port learning does not disable forwarding once L3 forwarding and the corresponding learning of FDB and IPFDB tables has been turned ON. Forwarding of traffic through a particular port does not stop even after port learning is disabled for that port. This characteristic is a known behavior of ExtremeWare.

Example
The following command disables MAC address learning on port 4 on a stand-alone switch:

disable learning ports 4

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable mirroring

  disable mirroring

Description
Disables port-mirroring.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
Use the disable mirroring command to stop configured copied traffic associated with one or more ports.

Example
The following command disables port-mirroring:

  disable mirroring

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ports

disable ports [<portlist> | all | {vlan} <vlan name>]

Description
Disables one or more ports on the switch.

For PoS modules. Brings down the PPP link on the specified port and changes the port status LED to blinking green.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports on the switch.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, the <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Use this command for security, administration, and troubleshooting purposes.

Even though a port is disabled, the link remains enabled for diagnostic purposes. To enable or re-enable a port, use the enable ports [<portlist> | all | (vlan) <vlan name>] command.

Example
The following command disables ports 3, 5, and 12 through 15 on a stand-alone switch:

disable ports 3,5,12-15

The following command disables slot 1, ports 3, 5, and 12 through 15 on a modular switch:

disable ports 1:3,1:5,1:12-1:15

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

The all option was first available for the Summit 300-48 in ExtremeWare 7.3e.
The command was modified in ExtremeWare 7.3 and ExtremeWare 7.3e to support the `vlan` option.

**Platform Availability**

This command is available on all platforms.
enable sharing

disable sharing [port]

Description
Disables a load-sharing group of ports.

Syntax Description

<table>
<thead>
<tr>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disabled</td>
</tr>
</tbody>
</table>

Usage Guidelines
This command increases bandwidth tracking and resiliency.

On a modular switch, port is specified as <slot>:<port number>. On a stand-alone switch, port is the port configured as the load-sharing master port. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

When sharing is disabled, the master port retains all configuration including VLAN membership. Configuration for all other member ports is reset to default values. Member ports are removed from all VLANs to prevent loops.

Example
The following command disables sharing on master logical port 9, which contains ports 9-12 on a stand-alone switch:

disable sharing 9

The following command disables sharing on master logical port 9 in slot 3, which contains ports 9 through 12 on a modular switch:

disable sharing 3:9

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable slot

disable slot [all | msm-a | msm-b | <slot number>]

Description
Disables one or all slots on a BlackDiamond or Alpine switch, and leaves the module in a power-down state.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Species that all slots in the device should be disabled.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies that MSM-A should be disabled.</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies that MSM-B should be disabled.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot to be disabled.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
This command allows the user to disable a slot. When the user types this command, the I/O module in that particular slot number is brought down, and the slot is powered down. The LEDs on the module go OFF.

A disabled slot can be re-enabled using the enable slot command.

The show slot command, if invoked after the user disables the slot, shows this slot state as “Disabled.” The user can either disable a slot individually or use the disable slot all to disable all the slots.

If there is no I/O module present in a slot when the user disables the slot, the slot still goes to the “Disable” state. If a module is inserted in a slot that has been disabled, the module does not come up and stays in the “disabled” state until the slot is enabled by using the enable slot command. below.

If you do not save the configuration before you do a switch reboot, the slot will be re-enabled upon reboot. If you save the configuration after disabling a slot, the slot will remain disabled after a reboot.

Example
The following command disables slot 5 on the switch:

disable slot 5

History
This command was first available in ExtremeWare 6.2.1.

Platform Availability
This command is available on BlackDiamond and Alpine switches only.
disable smartredundancy

disable smartredundancy [<portlist>]

Description
Disables the smart redundancy feature.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2-6:2-8. |

Default
Disabled

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Use with Extreme Networks switches that support privacy and backup uplinks.

When smartredundancy is disabled, the switch changes the active link only when the current active link becomes inoperable.

Example
The following command disables the smart redundancy feature on ports 1-4:

disable smartredundancy 1-4

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e

Platform Availability
This command is available on all platforms.
enable card-scan

enable card-scan

declaration
Enables the card-scan function on MSM slots in the BlackDiamond switch.

Syntax Description
This command has no arguments or variables.

Default
By default, card-scan is enabled.

Usage Guidelines
On certain BlackDiamond switches running earlier releases of ExtremeWare, hot insertion of a slave
MSM causes one or more of the following conditions:

- Some or all of the I/O modules are reset.
- The front panel links go down on some or all of the I/O modules.
- The backplane links go down on some or all of the I/O modules.

The card-scan feature discovers and repairs this condition, thus preventing the need for a manual reset
of the switch. When card-scan is enabled, the system logs one of the following messages if a problem
occurs when the MSM is inserted:

- Cardscan (msm insert) Attempting to fix broken BP connection for slot x
- Cardscan (msm insert) Attempting to fix packet missed for slot x
- Cardscan (msm insert) Attempting to fix card x in reset (y)
- Cardscan (timer) Attempting to fix card x in reset (y)

In these messages, x represents a slot number and y represents debugging information.

Example
The following command enables card-scan:

enable card-scan

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available only on BlackDiamond switches.
enable edp ports

   enable edp ports [<portlist> | all]

Description

Enables the Extreme Discovery Protocol (EDP) on one or more ports.

Syntax Description

<table>
<thead>
<tr>
<th>param</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports on the switch.</td>
</tr>
</tbody>
</table>

Default

Enabled

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

EDP is useful when Extreme Networks switches are attached to a port.

The EDP is used to locate neighbor Extreme Networks switches and exchange information about switch configuration. When running on a normal switch port, EDP is used to by the switches to exchange topology information with each other. Information communicated using EDP includes the following:

- Switch MAC address (switch ID)
- Switch software version information
- Switch IP address
- Switch VLAN-IP information
- Switch port number

For version 2.0 and 4.0: Information communicated using EDP also includes the following:

- Virtual chassis identifier and port number
- Listing of all virtual chassis identifiers

Example

The following command enables EDP on port 7 on a stand-alone switch:

   enable edp ports 7

The following command enables EDP on slot 1, port 3 on a modular switch:

   enable edp ports 1:3
History
This command was first available in ExtremeWare 2.0.
This command was modified in ExtremeWare 4.0 to support modular switches.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e

Platform Availability
This command is available on all platforms.
enable flooding ports

   enable flooding ports <portlist>

Description
Enables packet flooding on one or more ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* 2:5, 2:6-2:8. |

Default
Ports are enabled for learning, not flooding.

Usage Guidelines

This command configures the specified ports to act like a hub. When flooding is enabled on a particular port, all frames and packets are passed on to other member ports that have flooding enabled. This includes all broadcast, multicast, known unicast and unknown unicast packets (including EDP). To make effective use of this feature you should have flooding enabled on more than one port.

When ports are configured for flooding, the FDB will be flushed for the entire system, which means all the entries in the dynamic FDB must be relearned.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Example
The following command enables flooding on ports 6, 7, and 8 on a stand-alone switch:

   enable flooding ports 6,7,8

History
This command was first available in ExtremeWare 6.2.1.

Platform Availability
This command is available on “i”-series platforms.
enable jumbo-frame ports

enable jumbo-frame ports [<portlist> | all]

Description
Enables support on the physical ports that will carry jumbo frames.

For PoS modules. Enables jumbo-frame support to specific PoS ports when jumbo-frame support changes the negotiated maximum receive unit (MRU) size.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6:2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports on the switch.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Increases performance to back-end servers or allows for VMAN 802.1q encapsulations.

You must configure the maximum MTU size of a jumbo frame before you can use the enable jumbo-frame ports command. Use the configure jumbo-frame size command to configure the MTU size.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Example
The following command enables jumbo frame support on port 5 on a stand-alone switch:

```
enable jumbo-frame ports 5
```

The following command enables jumbo frame support on slot 3, port 5 on a modular switch:

```
enable jumbo-frame ports 3:5
```

History
This command was first available in ExtremeWare 6.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable lbdetect port

    enable lbdetect port <portlist> [retry-timeout<seconds>]

Description
Enables the system to detect loops between ports. If a port is looped, it disables the port. Every \( n \) seconds, it re-enables the port and tries again, unless "none" is specified

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports to be grouped to the master port. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>retry-timeout</td>
<td>Specifies a time in seconds to check for loops on the ports.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines

Each port may enable loop detection. This optional feature detects that a port has been looped back to the local system. If a loopback is detected, the port is disabled. Note that loopbacks may exist between different ports. The feature will disable any port that both has the feature enabled, and receives an LACP message that was sent from the local system.

If no timeout is specified, the port is disabled permanently if there is a loop detected. Otherwise, the port is periodically re-enabled, and tested for loops every \( N \) seconds.

Example
The following example enables loopback detection on ports 9 through 12:

```
enable lbdetect port 9-12
```

History

This command was first available in ExtremeWare 7.0.0.

This command was added to the Summit "e" series of switches in ExtremeWare 7.3e.

Platform Availability

This command is available on all platforms.
enable learning ports

   enable learning ports <portlist>

Description
Enables MAC address learning on one or more ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*", 2:5, 2:6-2:8. |

Default
Enabled

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Example
The following command enables MAC address learning on ports 7 and 8 on a stand-alone switch:

   enable learning ports 7,8

The following command enables MAC address learning on slot 1, ports 7 and 8 on a modular switch:

   enable learning ports 1:7-8

History
This command was first available in ExtremeWare 2.0.
This command was modified in ExtremeWare 4.0 to support modular switches.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable mirroring to port

    enable mirroring to port [<port>] [tagged | untagged]

Description
Dedicates a port on the switch to be the mirror output port.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Specifies the port to be the mirror output port.</td>
</tr>
<tr>
<td>tagged</td>
<td>Configures the port as tagged.</td>
</tr>
<tr>
<td>untagged</td>
<td>Configures the port as untagged.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Port-mirroring configures the switch to copy all traffic associated with one port to a monitor port on the switch. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. The switch uses a traffic filter that copies a group of traffic to the monitor port. The traffic filter can be defined based on one of the following criteria:

- **Physical port**—All data that traverses the port, regardless of VLAN configuration, is copied to the monitor port.
- **VLAN**—All data to and from a particular VLAN, regardless of the physical port configuration, is copied to the monitor port.
- **Virtual port**—All data specific to a VLAN on a specific port is copied to the monitor port.

Up to eight mirroring filters and one monitor port can be configured on the switch. After a port has been specified as a monitor port, it cannot be used for any other function. Frames that contain errors are not mirrored.

For version 6.0 and later:
- tagged and untagged are added to the command syntax.

For version 4.0 and later:
- to is added to the command syntax.
- Supports modular switches.

For version 2.0 and 4.0:
- In addition to the physical port, VLAN, and virtual port, the traffic filter can be defined based on the following criteria:
  - **MAC source address/destination address**—All data sent to or received from a particular source or destination MAC address is copied to the monitor port.

For MAC mirroring to work correctly, the MAC address must already be present in the forwarding database (FDB).
Example
The following example selects port 3 as a tagged mirror port on a stand-alone switch:
```
enable mirroring to port 3 tagged
```

The following example selects slot 1, port 3 as the mirror port on a modular switch:
```
enable mirroring to port 1:3
```

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support the `tag | untagged` keywords and modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable ports

    enable ports [<portlist> | all | {vlan} <vlan name>]

**Description**
Enables a port.

**For PoS modules.** Enables the PPP link on the specified port, and changes the port status LED to solid green (if no other problems exist).

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2*, 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports on the switch.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
</tbody>
</table>

**Default**
All ports are enabled.

**Usage Guidelines**
Use this command to enable one or more ports if you previously disabled the port(s) for security, administration, or troubleshooting.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, the `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

**Example**
The following command enables ports 3, 5, and 12 through 15 on the stand-alone switch:

```
enable ports 3,5,12-15
```

The following command enables slot 1, ports 3, 5, and 12 through 15 on the modular switch:

```
enable ports 1:3, 1:5, 1:12-1:15
```

**History**
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 4.0 to support the modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

The command was modified in ExtremeWare 7.3 and ExtremeWare 7.3e to support the `vlan` option.
Platform Availability

This command is available on all platforms.
enable sharing grouping

For “i” series switches:

```
enable sharing <port> grouping <portlist> {dynamic | algorithm {port-based
 | address-based | round-robin}}
```

For “e” series switches:

```
enable sharing <port> grouping <portlist> {dynamic | algorithm
(address-based))
```

Description

This command enables the switch to configure static port load sharing or dynamic port load sharing. When configuring dynamic port load sharing, LACP will be used to detect and set up for the remote side’s load sharing capabilities.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Specifies the master port for a loadsharing group.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports to be grouped to the master port. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5,1-5, 2-6-2-8.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Specifies dynamic sharing by using LACP.</td>
</tr>
<tr>
<td>algorithm</td>
<td>Specifies sharing by port-based, address-based, or round-robin algorithms.</td>
</tr>
</tbody>
</table>

NOTE: The port-based and round-robin algorithm options are only supported on “i” series switches.

Default

Disabled

Usage Guidelines

On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Load sharing allows you to increase bandwidth and availability between switches by using a group of ports to carry traffic in parallel between switches. The sharing algorithm allows the switch to use multiple ports as a single logical port or a “master” port. For example, VLANs see the load-sharing group as a single logical port. The algorithm also guarantees packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.

Load sharing must be enabled on both ends of the link, or a network loop will result.

While LACP is based on industry standard, this feature is supported between Extreme Networks switches only. However, it may be compatible with third-party “trunking” or sharing algorithms. Check with an Extreme Networks technical representative for more information.

Modular switch load-sharing groups are defined according to the following rules:
The first port in the load-sharing group is configured to be the “master” logical port. This is the reference port used in configuration commands. It can be thought of as the logical port representing the entire port group.

A master port can be a member of a Spanning Tree Domain (STPD), but the other ports assigned to a load-sharing group cannot.

When using load sharing, you should always reference the master logical port of the load-sharing group when configuring or viewing VLANs. VLANs configured to use other ports in the load-sharing group will have those ports deleted from the VLAN when load sharing becomes enabled.

A load-sharing group can include a maximum of eight ports.

**BlackDiamond only**—The ports in a load-sharing group on a BlackDiamond 6816, and on a BlackDiamond 6804 and 6808 that do not use the MSM-3, must all be on the same I/O module. Groups can span multiple modules with other chassis.

Dynamic load sharing (LACP) cannot be used for groups that span multiple modules.

When using load sharing with the ESRP HA feature, configure all ports in the same load-sharing group as host attach ports. When using load sharing with the ESRP don’t count feature, configure all ports in the same load-sharing group as don’t count ports.

There are two broad categories of load sharing supported on Extreme Network switches:

**Dynamic load sharing**—A grouping of ports that will use IEEE 802.3ad load sharing to dynamically determine if load sharing is possible, and will automatically configure load sharing when possible. Uses Link Aggregation Control Protocol (LACP), part of the IEEE 802.3ad standard, to allow the switch to dynamically reconfigure the sharing groups. The group is only enabled when LACP detects that the other side is also using LACP, and wants these ports to be in a group.

**Static load sharing (on “i” series only)**—A grouping of ports specifically configured to load share. The switch ports at each end must be configured as part of a load-sharing group. Additionally, you can choose the load-sharing algorithm used by the group. This feature is supported between Extreme Networks switches only, but may be compatible with third-party trunking or link-aggregation algorithms. Check with an Extreme Networks technical representative for more information.

Load-sharing algorithms allow you to select the distribution technique used by the load-sharing group to determine the output port selection. Algorithm selection is not intended for use in predictive traffic engineering. You can only choose the algorithm used in static load sharing. There is no option to choose an algorithm when you use dynamic load sharing.

**Address-based**—Uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:

- **IP packets**—Uses the source and destination MAC and IP addresses, and the TCP port number.
- **IPX packets (on “i” series only)**—Uses the source and destination MAC address, and IPX network identifiers.
- **All other packets**—Uses the source and destination MAC address.

**NOTE**

Stacked switches support only address-based load sharing.

**Port-based**—Uses the ingress port to determine which physical port in the load-sharing group is used to forward traffic out of the switch. Port-based algorithms are available only on “i” series switches.
• **Round-robin**—When the switch receives a stream of packets, it forwards one packet out of each physical port in the load-sharing group using a round-robin scheme. The round-robin algorithm is available only on "i" series switches.

Using the round-robin algorithm, packet sequencing between clients is not guaranteed.

If you do not explicitly select an algorithm, the port-based scheme is used. However, the address-based algorithm has a more even distribution and is the recommended choice.

**Example**

The following example defines a load-sharing group that contains ports 9 through 12, and uses the first port in the group as the master logical port on a stand-alone switch:

```
enable sharing 9 grouping 9-12
```

The following example defines a load-sharing group that contains ports 9 through 12 on slot 3, ports 7 through 10 on slot 5, and uses the first port on slot 3 as the master logical port 9 on a modular switch:

```
enable sharing 3:9 grouping 3:9-3:12, 5:7-5:10
```

In this example, logical port 3:9 represents physical ports 3:9 through 3:12 and 5:7 through 5:10.

**History**

This command was first available in ExtremeWare 2.0.

The command was modified in ExtremeWare 4.0 to support modular switches.

The command was modified in ExtremeWare 6.0 to support the `algorithm` parameter.

The command was modified in ExtremeWare 7.0.0 to support the `dynamic` parameter.

The command was modified in ExtremeWare 7.1.1 to support cross-module trunking on BlackDiamond switches.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable slot

   enable slot [all | msm-a | msm-b | <slot number>]

Description
Enables one or all slots on a BlackDiamond or Alpine switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Species that all slots in the device should be enabled.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies that MSM-A should be enabled.</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies that MSM-B should be enabled.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot to be enabled.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
This command allows the user to enable a slot that has been previously disabled using the disable slot command.

When you enter the enable command, the disabled I/O module in the specified slot is brought up, and the slot is made operational, if possible, or goes to the appropriate state as determined by the card state machine. The LEDs on the module are brought ON as usual. You can either enable a slot individually, or use the enable slot all command to enable all the slots.

After you enable the slot, the show slot command shows the state as “Operational” or will display the appropriate state if the module could not be brought up successfully. Note that there is no card state named “Enable” and the module goes to the appropriate states as determined by the card state machine when the enable slot command is invoked.

Only slots that have their state as “disabled” can be enabled using this command. If this command is used on slots that are in states other than “disabled,” the card state machine takes no action on these slots.

Example
The following command enables slot 5 on the switch:

```
enable slot 5
```

History
This command was first available in ExtremeWare 6.2.1.

Platform Availability
This command is available on BlackDiamond and Alpine switches only.
enable smartredundancy

    enable smartredundancy <portlist>

Description
Enables the Smart Redundancy feature on the redundant Gigabit Ethernet port.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
When the Smart Redundancy feature is enabled, the switch always uses the primary link when the primary link is available.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Example
The following command enables the Smart Redundancy feature on port 4 on a switch:

    enable smartredundancy 4

The following command enables the Smart Redundancy feature on slot 1, port 4 on a BlackDiamond switch:

    enable smartredundancy 1:4

History
This command was first available in ExtremeWare 2.0.

Support for modular switches was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
**restart ports**

```
restart ports [<portlist>]
```

**Description**
Resets autonegotiation for one or more ports by resetting the physical link.

**For PoS modules.** Causes the PPP link to be renegotiated.

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</th>
</tr>
</thead>
</table>

**Default**
N/A

**Usage Guidelines**

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

**Example**
The following command resets autonegotiation on port 4 on a stand-alone switch:
```
restart ports 4
```
The following command resets autonegotiation on slot 1, port 4 on a modular switch:
```
restart ports 1:4
```

**History**
This command was first available in ExtremeWare 4.0.
This command was modified in ExtremeWare 6.1 to support PoS modules.
This command was modified by removing the `mgmt` option in ExtremeWare 6.22.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
run msm-failover
  run msm-failover

Description
Causes a user-specified MSM failover.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command causes a user-specified MSM failover:
run msm-failover

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is available on the BlackDiamond switch only.
show edp

    show edp {vlan <portlist> <vlan name>}

Description
Displays connectivity and configuration information for neighboring Extreme Networks switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Use the show edp command to display neighboring switches and configurations. This is most effective with Extreme Networks switches.

Example
The following command displays the connectivity and configuration of neighboring Extreme Networks switches:

```
show edp
```

Following is the output from this command:

```
Port 1:  EDP is enabled
      Remote-system: Summit5i (Version 6.2.2)
      Remote-ID=00:00:00:01:30:e9:ef:00
      Remote-Port=1:1   Age=37
      Remote-Vlans:
            Mgmt(4094, 10.45.208.223) test1(0) Default(1)
            MacVlanDiscover(0)

Port 3:  EDP is enabled
      Remote-system: Summit7i (Version 6.2.2)
      Remote-ID=00:00:00:e0:2b:99:fe:00
      Remote-Port=1:3   Age=35
      Remote-Vlans:
            Mgmt(4094) Default(1) MacVlanDiscover(0)

Port 5:  EDP is enabled
      Remote-system: Alpine3808 (Version 6.2.2)
      Remote-ID=00:00:00:01:30:31:55:00
      Remote-Port=1:1   Age=47
      Remote-Vlans:
            Mgmt(4094, 10.45.208.226) Default(1) MacVlanDiscover(0)
```
History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show mirroring

show mirroring

Description
Displays the port-mirroring configuration on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
You must configure mirroring on the switch to display mirroring statistics. Use the show mirroring command to configure mirroring.

You can use this command to display mirroring statistics and determine if mirroring is enabled or disabled on the switch.

To view the status of port-mirroring on the switch, use the show mirroring command. The show mirroring command displays information about the enable/disable state for port-mirroring.

Example
The following command displays switch mirroring statistics:
show mirroring

Following is the output from this command:
Mirror port: 5 is up
port number 1 in all vlans

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show msm-failover

show msm-failover

Description
Displays hitless failover statistics.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays MSM failover statistics:

```
show msm-failover
```

The output displays the following:

- Current state of the MSM
- Software image information (primary/secondary image, version)
- Cause of the last failover
- Failover configuration (link action, preserve state, slave configuration, timeout)
- ESRP failover mode
- Failover status for the supported subsystems (configuration, layer 2 hardware, layer 3 hardware, STP, EAPS, ARP, ESRP)

Each of the supported subsystems display one of the following states:
- disable—Hitless failover is disabled. This is also the initial state.
- initial—Hitless failover is enabled, but the downloading of the subsystem state has not yet started for a particular subsystem.
- xfr—The subsystem’s state is in the process of being transferred to the slave. The state transfer includes all of the state for that subsystem.
- ready—The subsystem has received its state download. In the ready state, it may receive updates to its internal states.
- failed—The subsystem encountered a failure. To clear the failure, reboot the slave MSM.
- unknown—If this state is displayed, contact Extreme Networks® Technical Support.
- <not available>—The state and reason for the current slave shows this if the slave is in the process of being rebooted or is not present in the chassis.
After a reboot or insertion of a slave MSM-3, use this command to ensure that the slave is ready before initiating a hitless failover.

**History**
This command was first available in ExtremeWare 7.1.1.

**Platform Availability**
This command is available on the BlackDiamond switch only.
show ports vlan stats

    show ports <portlist> | vlan <vlan_name> vlan stats

Description
Displays port VLAN statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8.</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Specifies to display VLAN statistics from the VLAN with this name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command displays VLAN information for the corp VLAN:
show ports vlan corp vlan stats

The output of the command is similar to:

Port-Based Vlan Statistics Sun Sep 12 19:19:50 2004
PORT Rx Rx Rx Rx Byte Tx Tx Tx Tx Byte
VLAN Ucast Mcast Bcast Count Ucast Mcast Bcast Count
================================================================================
    7
    8
    9
    10
================================================================================
======
0->Clear Counters U->page up D->page down ESC->exit

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the “e” series platforms only.
show ports collisions

show ports {mgmt | <portlist>} collisions

Description
Displays real-time collision statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, collision statistics are displayed for all ports.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

This status information may be useful for your technical support representative if you have a network problem.

Example
The following command displays real-time collision statistics on port 7 on a stand-alone switch:

```
show ports 7 collisions
```

The following command displays real-time collision statistics on slot 1, ports 1-16 on a modular switch:

```
show ports 1:1-1:16 collisions
```

Following is the output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Link Status</th>
<th>Collision Histogram</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16</td>
</tr>
<tr>
<td>1</td>
<td>A</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>2</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>3</td>
<td>A</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>5</td>
<td>A</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>6</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>7</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>8</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>9</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
<tr>
<td>10</td>
<td>R</td>
<td>0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0</td>
</tr>
</tbody>
</table>
History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
show ports configuration

show ports {mgmt | <portlist>| vlan <vlan name>} configuration

Description
Displays port configuration statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*; 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

If you do not specify a port number or range of ports, configuration statistics are displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

This command displays port configuration, which includes:

- Port state
- Link state
- Link speed
- Duplex mode
- Flow control (on “i” series only)
- Load sharing information
- Link media information

For version 6.0 and later:
- Auto on/off

Example
The following command displays the port configuration statistics for all ports on a switch:

show ports config
Following is the output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Port</th>
<th>Link</th>
<th>Auto</th>
<th>Speed</th>
<th>Duplex</th>
<th>Flow</th>
<th>Ld Share</th>
<th>Media</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Status</td>
<td>Neg</td>
<td>Cfg Actual</td>
<td>Cfg Actual</td>
<td>Ctrl</td>
<td>Master</td>
<td>Pri</td>
<td>Red</td>
</tr>
<tr>
<td>1:1</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>1000</td>
<td>AUTO</td>
<td>FULL</td>
<td>NONE</td>
</tr>
<tr>
<td>1:2</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>1:3</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>1:4</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>1:5</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>1:6</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>1:7</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>1:8</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>2:1</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:2</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:3</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:4</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:5</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:6</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:7</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>2:8</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:1</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:2</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:3</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:4</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:5</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:6</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:7</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:8</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:9</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:10</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:11</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>3:12</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>1000</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SX</td>
<td></td>
</tr>
<tr>
<td>4:1</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>622</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SMF</td>
<td></td>
</tr>
<tr>
<td>4:2</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>622</td>
<td>AUTO</td>
<td>AUTO</td>
<td>SMF</td>
<td></td>
</tr>
<tr>
<td>5:1</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>5:2</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>5:3</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
<tr>
<td>5:4</td>
<td>ENABLED</td>
<td>R</td>
<td>ON</td>
<td>AUTO</td>
<td>AUTO</td>
<td>AUTO</td>
<td>UTP</td>
<td></td>
</tr>
</tbody>
</table>

---

**Link Status:** A-Active R-Ready D-Disabled NP-Not Present LB-Loopback
U->page up D->page down ESC->exit

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
show ports info

    show ports {mgmt | <portlist>| vlan <vlan name>} info {detail}

**Description**
Displays detailed system-related information.

**For PoS modules.** Displays port information that includes new DiffServ and RED configuration parameters.

**For "3" series module.** If you specify the `detail` keyword, the output displays the flow control state and the ingress QoS profile, ingress IPTOS replacement, and egress rate limiting configurations.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port, such as the Summit 400.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*; 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies detailed port information. (6.0 and later)</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command displays the following:

- Port number
- Diagnostics
- Port configuration
  - RED state (on "i" series only)
  - Admin state
  - Link state
  - Link counter
  - VLAN configuration
  - STP configuration
  - Aggregate bandwidth control percentage
  - Trunking
  - EDP
  - DLCS (on "i" series only)
  - Load balancing
  - Learning
— Flooding
— QoS profiles

If you do not specify a port number or range of ports, detailed system-related information is displayed for all ports. The data is displayed in a table format.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

This status information may be useful for your technical support representative if you have a network problem.

For version 6.0 and later: The `detail` parameter is used to provided more specific port information. The data is called out with written explanations versus displayed in a table format.

For version 6.2.2 and later: The detailed output displays a link filter counter. The link filter counter is calculated at the middle layer on receiving an event. The link filter up indicates the number of link transitions from down to up at the middle layer filter. The link filter down indicates the number of link transitions from up to down at the middle layer filter.

**NOTE**

*If you telnet to the switch and use the show ports info detail command, the line feeds might not be recognized, resulting in output lines overwriting previous lines.*

**Example**

The following command displays port system-related information:

```plaintext
show ports info
```

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Diag Flags</th>
<th>Link State</th>
<th>Link Num</th>
<th>Link STP</th>
<th>VLAN Proto Size</th>
<th>Jumbo QOS</th>
<th>Load Profile Mast</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:1</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:2</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:3</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:4</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:5</td>
<td>P e--m-----E ready</td>
<td>0 1 1 1</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2:6</td>
<td>P e--m-----E ready</td>
<td>0 1 1 1</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_7</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_8</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_9</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_10</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_11</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_12</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_13</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iL2_14</td>
<td>P e--m-----D ready</td>
<td>0 0 0 0</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:1</td>
<td>P e--m-----E ready</td>
<td>0 1 1 1</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:2</td>
<td>P e--m-----E ready</td>
<td>0 1 1 1</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:3</td>
<td>P e--m-----E ready</td>
<td>0 1 1 1</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3:4</td>
<td>P e--m-----E ready</td>
<td>0 1 1 1</td>
<td>9216</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flags: (a) Load Sharing Algorithm address-based, (d) DLCS Enabled
(D) Port Disabled, (dy) Dynamic Load Sharing
(e) Extreme Discovery Protocol Enabled, (E) Port Enabled
(f) Flooding Enabled, (g) Egress TOS Enabled, (G) SLB GoGo Mode
(h) Hardware Redundant Phy, (j) Jumbo Frame Enabled
(i) Load Sharing Enabled, (m) MAC Learning Enabled
(n) Ingress TOS Enabled, (o) Dot1p Vlan Priority Replacement Enabled
(p) Load Sharing Algorithm port-based, (P) Software Primary Port
(q) Background QoS Monitoring Enabled
(r) Load Sharing Algorithm round-robin, (R) Software Redundant Port

Diag: (P) Passed, (F) Failed
Port: (iL) Internal Loopback

The following command displays more specific information for slot 2, port 6 in a modular switch:

```
show ports 2:6 info detail
```

Following is sample output from this command:

```
Port 2:6:
  Type:           UTP
  Diagnostic:     passed
  Random Early Drop: Disabled
  Admin state:    Enabled, with auto-duplex auto-speed sensing
  Link state:     Ready
  Link counter:   Up 0 time(s), Down 0 times(s)
  VLAN cfg:       Default [Internal Tag=0001,Mac-Limit:Cfg=No-limit,LRN=0,BlkHole=0]
  STP cfg:        s0(disable), Tag=(none), Mode=802.1D, State=FORWARDING
  Aggregate B/W: Configured [ 25]%
  Trunking:       Load sharing is not enabled
  Protocol:       VLAN=Default Vpri=0   Protocol=ANY [EtherType:ffff]
  EDP:            enabled
  DLCS:           disabled
  lbdetect:       disabled
  Learning:       enabled
  Flooding:       disabled
  Jumbo:          Disabled
  BG QoS monitor: disabled
  Ingress Rate Shaping:
  QoS profile:    None configured
  Queue:  Q0 using QP1 MinBw=0% MaxBw=100% Pri=0.
           Q1 using QP2 MinBw=0% MaxBw=100% Pri=1.
           Q2 using QP3 MinBw=0% MaxBw=100% Pri=2.
           Q3 using QP4 MinBw=0% MaxBw=100% Pri=3.
           Q4 using QP5 MinBw=0% MaxBw=100% Pri=4.
           Q5 using QP6 MinBw=0% MaxBw=100% Pri=5.
           Q6 using QP7 MinBw=0% MaxBw=100% Pri=6.
           Q7 using QP8 MinBw=0% MaxBw=100% Pri=7.
  Ingress IPTOS: Examination is disabled
  IPTOS->QoSProfile mapping:
          00->QP1 01->QP1 02->QP1 03->QP1 04->QP1 05->QP1 06->QP1 07->QP1
          08->QP2 09->QP2 10->QP2 11->QP2 12->QP2 13->QP2 14->QP2 15->QP2
```
Commands for Configuring Slots and Ports on a Switch

16->QP3 17->QP3 18->QP3 19->QP3 20->QP3 21->QP3 22->QP3 23->QP3
24->QP4 25->QP4 26->QP4 27->QP4 28->QP4 29->QP4 30->QP4 31->QP4
32->QP5 33->QP5 34->QP5 35->QP5 36->QP5 37->QP5 38->QP5 39->QP5
40->QP6 41->QP6 42->QP6 43->QP6 44->QP6 45->QP6 46->QP6 47->QP6
48->QP7 49->QP7 50->QP7 51->QP7 52->QP7 53->QP7 54->QP7 55->QP7
56->QP8 57->QP8 58->QP8 59->QP8 60->QP8 61->QP8 62->QP8 63->QP8

Egress IPTOS: Replacement is disabled

802.1p Pri->IPTOS mapping:
  0->00 1->08 2->16 3->24 4->32 5->40 6->48 7->56

802.1p: Disabled marking of priority field based on queue number

Smart Redundancy: Enabled

VLANs monitored for stats:
Software redundant port: disabled
jitter-tolerance: enabled
link filtering: isr filter = yes, middle layer filter = no

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.0 to support the detail keyword.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 6.2.2 to indicate disabled or enabled status.

This command was modified in Extreme Ware 7.0.1 to support the "3" series modules.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

This command was modified in Extreme Ware 7.3.0 to support port aggregate bandwidth control.

The command was modified in ExtremeWare 7.3.0 and ExtremeWare 7.3e to support the vlan option.

Platform Availability

This command is available on all platforms.
show ports packet

    show ports {mgmt | <portlist>| vlan <vlan name>} packet

Description
Displays a histogram of packet statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port Supported only for switches that provide a management port, such as the Summit 400.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, a histogram is displayed for all ports.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

This status information may be useful for your technical support representative if you have a network problem.

The following packet statistics are displayed:

- port number
- link status
- packet size

Example
The following command displays packet statistics for ports 1 through 6 on a stand-alone switch:

```
show ports 1-6 packet
```

```
Receive Packet Statistics
Sun Sep 12 14:48:59 2004
Port       Link Status  0-64  65-127  128-255  256-511  512-1023 1024-1518   Jumbo
================================================================================
  1      A     410465  3548292  97395  51257  7390    1547785        0
  2      A     397578  1724578  94290  49422  10469   2491883        0
  3      R         0         0         0         0         0         0         0
  4      A     394646  2485133  102640  52893  5945    1537346        0
  5      A     394141  2439441  89201  49095  4141    1532115        0
  6      A     394741  2099487  67017  40001  4143    2540292        0
Sun Sep 12 14:48:40 2004=================================================================
```
The following command displays packet statistics for slot 1, ports 1 through 8, slot 2, ports 1 through 8, and slot 3, port 1 on a modular switch:

```
show ports 1:1-1:8, 2:1-2:8, 3:1 packet
```

Following is the output from this command:

```
Port Link Packet Sizes
Status 0-64 65-127 128-255 256-511 512-1023 1024-1518 Jumbo
================================================================================
1:1 R 0 0 0 0 0 0 0
1:2 R 0 0 0 0 0 0 0
1:3 R 0 0 0 0 0 0 0
1:4 R 0 0 0 0 0 0 0
1:5 R 0 0 0 0 0 0 0
1:6 R 0 0 0 0 0 0 0
1:7 R 0 0 0 0 0 0 0
1:8 R 0 0 0 0 0 0 0
2:1 R 0 0 0 0 0 0 0
2:2 R 0 0 0 0 0 0 0
2:3 R 0 0 0 0 0 0 0
2:4 R 0 0 0 0 0 0 0
2:5 R 0 0 0 0 0 0 0
2:6 R 0 0 0 0 0 0 0
2:7 R 0 0 0 0 0 0 0
2:8 R 0 0 0 0 0 0 0
3:1 R 0 0 0 0 0 0 0
================================================================================
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

The command was modified in ExtremeWare 7.3.0 and ExtremeWare 7.3e to support the `vlan` option.

**Platform Availability**

This command is available on all platforms.
show ports redundant

Description
Displays detailed information about redundant ports.

Syntax Description
This command does not have any parameters or variables.

Default
N/A

Usage Guidelines
An asterisk appears when an individual link is active and an exclamation point when the link is disabled.

Example
The following examples gives information about redundant ports:
show ports redundant

The output of the command is similar to:

Primary  *5  Redundant  7  
Primary  *6  Redundant  25  

Flags: (*) Active, (!) Disabled

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the “e” series platforms.
show ports sharing

show ports <portlist> sharing

Description
Displays port loadsharing groups.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following example shows all of the load sharing groups on the Summit 400:

* Summit400-48t:46 # show ports sharing
Load Sharing Monitor
Config Master Current Ld Share Type Group Status Ups
Configuration List
37 37 a 37 A 1
a 38 R 0
a 39 A 1
a 40 A 1
a 41 A 1
a 42 A 1

Link Status: (A) Active, (D) Disabled, (LB) Loopback, (ND) Not Distributing (NP) Not Present, (R) Ready

Ld Share Type: (a) address based

The next example shows dynamic load sharing configured on a Summit 300-24:

* Summit300-24:29 # show ports sharing
Load Sharing Monitor
Config Master Current Ld Share Type Group Status Ups
Configuration List
1 1 dy 1 ND 1
dy 2 D 0

Link Status: (A) Active, (D) Disabled, (LB) Loopback, (ND) Not Distributing (NP) Not Present, (R) Ready
The following command displays the port loadsharing group configured for port 5:4; the current master has shifted to port 7:4 since both ports 5:4 and 5:5 of the group are not active links:

```
show ports 5:4 sharing
```

The following is the output from this command:

```
* admin:3 # sh port 5:4 sharing
Load Sharing Monitor
Config  Current  Ld Share  Ld Share  Link  Link
Master  Master  Type     Group     Status  Ups
==========================================================================
5:4     7:4      r         5:4      NP     1
r       5:5      NP       1
r       7:4      A        2
r       7:5      A        1
```

Link Status: (A) Active, (D) Disabled, (ND) Not Distributing
(NP) Not Present, (R) Ready

Ld Share Type: (a) address based, (p) port based, (r) round robin
(dy) dynamic

**History**

This command was first available in ExtremeWare 6.2.2.

This command was modified in ExtremeWare 7.0.0 to support the `dynamic` algorithm.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show ports utilization

    show ports {mgmt | <portlist>| vlan <vlan name>} utilization

Description
Displays real-time port utilization information.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port, such as the Summit 400.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2.*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use the [Spacebar] to toggle between packet, byte, and bandwidth utilization information.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, the <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

If you do not specify a port number or range of ports, port utilization information is displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

Example
The following command displays utilization statistics for port 1 on a stand-alone switch:
show ports 1 utilization

The following command displays utilization statistics for slot 3, port 1 on a modular switch:
show ports 3:1 utilization
The following examples show the output from the show ports utilization command for all ports on the switch. The three displays show the information presented when you use the spacebar to toggle through the display types. The first display shows utilization in terms of packets:

<table>
<thead>
<tr>
<th>Port</th>
<th>Link</th>
<th>Receive packet/sec</th>
<th>Peak Rx pkt/sec</th>
<th>Transmit pkt/sec</th>
<th>Peak Transmit pkt/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>43</td>
<td>255</td>
<td>4</td>
<td>14</td>
</tr>
<tr>
<td>2</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Link Status: A-Active R-Ready D-Disabled NP-Not Present

The second display shows utilization in terms of bytes:

<table>
<thead>
<tr>
<th>Port</th>
<th>Link</th>
<th>Receive bytes/sec</th>
<th>Peak Rx bytes/sec</th>
<th>Transmit bytes/sec</th>
<th>Peak Transmit bytes/sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>1102</td>
<td>69555</td>
<td>536</td>
<td>2671</td>
</tr>
<tr>
<td>2</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Link Status: A-Active R-Ready D-Disabled NP-Not Present

The third display shows bandwidth utilization:

<table>
<thead>
<tr>
<th>Port</th>
<th>Link Speed</th>
<th>Link % bandwidth</th>
<th>Link % bandwidth</th>
<th>Link % bandwidth</th>
<th>Link % bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A 100</td>
<td>0.00</td>
<td>0.60</td>
<td>0.00</td>
<td>0.02</td>
</tr>
<tr>
<td>2</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>3</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>4</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>5</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>6</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>7</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
<tr>
<td>8</td>
<td>R 0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
</tr>
</tbody>
</table>

Link Status: A-Active R-Ready D-Disabled NP-Not Present
Commands for Configuring Slots and Ports on a Switch

History
This command was first available in ExtremeWare 2.0.
This command was modified in ExtremeWare 4.0 to support modular switches.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ports vlan info

    show ports <portlist> | vlan <vlan_name> vlan info

Description
Displays port VLAN information.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8.</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Specifies to display VLAN information from the VLAN with this name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command displays VLAN information for port 2:
show ports 2 vlan info

The following is the output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Name</th>
<th>VID</th>
<th>Protocol</th>
<th>Addr</th>
<th>Flags</th>
<th>Proto</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>v1</td>
<td></td>
<td>4093</td>
<td></td>
<td>------</td>
<td>-------</td>
<td>-------</td>
<td>-------</td>
</tr>
</tbody>
</table>

#
#

Flags:  (C) Domain-masterVlan, (c) Domain-memberVlan, (d) DVMRP Enabled
    (E) ESRP Slave, (f) IP Forwarding Enabled, (G) GVRP Enabled
    (i) ISIS Enabled, (I) IP Forwarding lpm-routing Enabled
    (L) Loopback Enabled, (M) ESRP Master, (m) IPmc Forwarding Enabled
    (N) GNS Reply Enabled, (o) OSPF Enabled (P) IPX SAP Enabled
    (p) PIM Enabled, (R) SubVLAN IP Range Configured, (r) RIP Enabled
    (S) SuperVlan, (s) SubVlan, (T) Member of STP Domain
    (v) VRRP Enabled, (V) VPLS/TLS Enabled, (X) IPX RIP Enabled
    (Z) Translation-Vlan, (z) Member-Vlan
    (2) IPX Type 20 Forwarding Enabled

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.
Platform Availability
This command is available on all platforms.
show sharing address-based

Description
Displays the address-based load sharing configuration.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This feature is available using the address-based load-sharing algorithm only. The address-based load-sharing algorithm uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:

- IP packets—Uses the source and destination MAC and IP address, and the TCP port number.
- IPX packets (on “i” series only)—Uses the source and destination MAC address and IPX identifiers.
- All other packets—Uses the source and destination MAC address.

To verify your configuration, use the `show sharing address-based` command. The show sharing address-based output displays the addressed-based configurations on the switch.

Example
The following example displays the address-based load sharing configuration on the switch:
```
show sharing address-based
```

Following is the output from this command:
```
Sharing address-based = L2_L3_L4
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on the “i” and “e” series platforms and the Alpine 3800 series switch modules.
show slot

show slot <slot number>

Description
Displays slot-specific information.

For ARM, ATM, MPLS, PoS, and WAN modules. Displays information that includes data about the software images loaded on the module, as well as status information on the module’s processors.

For stacked switches. Displays information about a Summit switch configured in a stack. Some of the fields in the command output provide clues to stack related problems.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot number</td>
<td>Specifies a slot on a modular switch or a location in a stack.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

The show slot command displays the following information:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>The state of the slot as it comes up.</td>
</tr>
<tr>
<td></td>
<td>• Initialization—The first state of the switch. Hardware and data structures are initialized in this state.</td>
</tr>
<tr>
<td></td>
<td>• Diag—This state applies mostly to remote switches, which are placed in this state until diagnostics are run and are available through RPC. Local switches receive diagnostic information immediately and are only in this state briefly.</td>
</tr>
<tr>
<td></td>
<td>• Mismatch—The switch was not allowed to join the stack because of the corresponding member supports certain features that are not compatible with the licensing of the manager and the other stack members.</td>
</tr>
<tr>
<td></td>
<td>• Operational—The switch is operating and has joined a stack of switches.</td>
</tr>
<tr>
<td></td>
<td>• Disable—The switch is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Power Down</td>
</tr>
<tr>
<td>Serial Number</td>
<td>Modules only: The serial number of the module.</td>
</tr>
<tr>
<td>H/W Module Type</td>
<td>The Summit model of the switch.</td>
</tr>
<tr>
<td>Manager/Member</td>
<td>Stacked Switches only: Indicates whether the switch is a stack manager (master) or a member (slave).</td>
</tr>
<tr>
<td>Primary ExtremeWare Version</td>
<td>Stacked Switches only: ExtremeWare version of the primary software image.</td>
</tr>
</tbody>
</table>
If you do not specify a slot number, information for all slots is displayed.

**For ARM, ATM, MPLS, PoS and WAN (E1, T1, and T3) modules:** The ExtremeWare technology release that supports these modules includes multiple software packages. One software package runs on the MSM or SMMi module while another package runs on each ARM, ATM, MPLS, PoS, or WAN module. You must download the software packages independently using the ExtremeWare `download image` command. Each software package has an associated version number that you can display using the `show version` command. It is recommended (not required), that the ExtremeWare software package and the ARM, ATM, MPLS, PoS, or WAN module software package be the same version.

**For ARM, ATM, MPLS and PoS modules:** To ensure compatibility, the MSM performs an automatic compatibility check before a ARM, ATM, MPLS or PoS module is activated. If the versions of the software packages are incompatible, the ARM, ATM, MPLS or PoS ports on the module will not come up and the `show slot` command will indicate that the software on the ARM, ATM, MPLS or PoS module is incompatible with ExtremeWare.

Assuming the ARM, ATM, MPLS or PoS module has no problems, the command `show slot <slot>` (where “<slot>” is the number of the slot where you installed the module) displays that ExtremeWare has detected the module and set it to the OPERATIONAL state.

As the module progresses through its initialization, the `show slot <slot>` command displays the general purpose processor (GPP) subsystem change state to OPERATIONAL, and then each of the network processors will change state to OPERATIONAL.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secondary ExtremeWare Version</td>
<td><strong>Stacked Switches only:</strong> ExtremeWare version of the secondary software image.</td>
</tr>
<tr>
<td>Image Selected</td>
<td><strong>Stacked Switches only:</strong> The image selected on the switch.</td>
</tr>
<tr>
<td>Image Booted</td>
<td><strong>Stacked Switches only:</strong> The running image of the switch.</td>
</tr>
<tr>
<td>Configuration Selected</td>
<td><strong>Stacked Switches only:</strong> The configuration selected for the switch.</td>
</tr>
<tr>
<td>Configuration Booted</td>
<td><strong>Stacked Switches only:</strong> The configuration that is active.</td>
</tr>
<tr>
<td>Primary Configuration</td>
<td><strong>Stacked Switches only:</strong> The configuration saved as primary.</td>
</tr>
<tr>
<td>Secondary Configuration</td>
<td><strong>Stacked Switches only:</strong> The configuration saved as secondary.</td>
</tr>
<tr>
<td>Configured Type</td>
<td>The model number as configured by the user. This field is used to detect the mismatches between the configured and actual model number.</td>
</tr>
<tr>
<td>Inline Power</td>
<td>Power consumption.</td>
</tr>
<tr>
<td>UTP Ports Available</td>
<td>Displays a list of ports. On stacked switches, the stacking ports are enclosed in brackets. Port numbers with active and down links are listed.</td>
</tr>
<tr>
<td>• Link Active</td>
<td></td>
</tr>
<tr>
<td>• Link Down</td>
<td></td>
</tr>
<tr>
<td>• GBIC Missing</td>
<td></td>
</tr>
</tbody>
</table>
When the GPP subsystem completes its initialization cycle and the subsystem state is OPERATIONAL, use the `show diagnostics {<slot>}` command to check the results of the module power-on self test (POST).

If the STATUS LED on the ARM, ATM, MPLS or PoS module turns amber and blinks, use the `show slot {<slot>}` command to display the slot status information. The `show slot {<slot>}` command also displays operational information related to the ARM, ATM, MPLS or PoS module. Information displayed includes the BlackDiamond switch fabric card state (module state), Network Processor status, General Purpose Processor status, hardware serial number and type, and image version and boot settings.

For the ARM, ATM, MPLS, PoS, and WAN modules, the information displayed by this command includes data about the software images loaded on the module and information about the operational status and backplane connections of the module.

For stacked switches. Displays information about a Summit switch configured in a stack. Some of the fields in the command output provide clues to stack related problems. For example:

- The slot state must be operational after the stack becomes active. If the slot is in any other state, then the stack is not completely up. If the slot state indicates mismatch, then the member is not allowed to join the stack because of operational vector problems. Operational vector mismatch indicate that the corresponding slot supports certain features, which are not compatible with the stack manager. For example, the member might be supporting an Advance-Edge license where the manager supports only an Edge license. In this case, you must reconfigure the member corresponding to the slot appropriately and must insert the member back into the stack.
- The ports field indicates the link status of ports on the slot. If the stacking ports are not active, the stack might be split at this point (based on the redundant link). You must ensure that the cables are connected appropriately to the stacking ports.
- The command also includes information regarding ExtremeWare versions, configuration and image selected and booted for the particular slot. If the image versions mismatch the member is not allowed to join the stack. You must ensure that all switches in the stack run compatible versions of ExtremeWare while bringing up the stack.

Example 1—Non-stacked

The following example displays module information for all slots:

```
show slot
```

Following is the output from this command:

```
Slot 1 information:
State:           Operational
Serial number:   701028-06-0026F38445
HW Module Type:  G8Ti

Configured Type: Not configured
UTP ports available:
Link Active:     Link Down: 01 02 03 04 05 06 07 08

Slot 2 information:
State:           Operational
Serial number:   701024-19-0125F06190
```
HW Module Type:     G8Xi

Configured Type:    Not configured
Gigabit ports available:
  Link Active:
  Link Down:      01
  GBIC missing:   02 03 04 05 06 07 08

Slot 3 information:
  State:              Operational
  Serial number:      701020-11-0032F51006
  HW Module Type:     G12SXi

Configured Type:    Not configured
Gigabit ports available:
  Link Active:
  Link Down:      01 02 03 04 05 06 07 08
  Link Down:      09 10 11 12

Slot 4 information:
  State:              Operational
  Network Processor 1 : Operational
  Network Processor 2 : Operational
  General Purpose Proc: Operational
  Serial number:      701039-04-0128F07843
  HW Module Type:     P12ci
  Optics: Single-mode Fiber
  NP 1:   Rev C0
  NP 2:   Rev C0

Configured Type:    Not configured
Bootrom Version: 1.18
Software image booted:   secondary
Software image configured:   secondary
Primary software version:
  7.0.0 (Build 44) (oc12) by Beta_Master on Sat 10/12/2002 06:16p

Secondary software version:
  7.0.0 (Build 44) (oc12) by Beta_Master on Sat 10/12/2002 06:16p

POS ports available:
  Link Up:
  Link Down:      01 02

Slot 5 information:
  State:              Operational
  Serial number:      701026-10-0142F70250
  HW Module Type:     F48Ti

Configured Type:    Not configured
UTP ports available:
  Link Active:
  Link Down:      01 02 03 04 05 06 07 08
Slot 6 information:
  State: Empty
  HW Module Type: Empty
  Configured Type: Not configured

Slot 7 information:
  State: Empty
  HW Module Type: Empty
  Configured Type: Not configured

Slot 8 information:
  State: Empty
  HW Module Type: Empty
  Configured Type: Not configured

Example 2—Stack of Switches

The following example shows slot information for a stack of switches:

* Stk Master:13 # show slot

Slot 1 information:
  State: Operational
  Serial number: --
  HW Module Type: S400-24P
  Master: 00:04:96:1F:A7:3A
  Primary EW Ver: 7.4e.0.28 [non-ssh]
  Secondary EW Ver: 7.4e.0.10 branch-McastExtn_v74e0b10-r2 [non-ssh]
  Image Selected: Primary
  Image Booted: Primary
  Config Selected: Primary
  Config Booted: Primary
  Primary Config: Created By EW Version: 7.4.0.26
  Secondary Config: Empty

  Configured Type: Not configured
  Inline-power:
    Total Common: 376W
    Consumed: 0.0W
  UTP ports available:
    Link Active:
      [26]
    Link Down:
      01 02 03 04 05 06 07 08
      09 10 11 12 13 14 15 16
      17 18 19 20 21 22 23 24
      [25]
Slot 8 information:

State: Operational
Serial number: --
HW Module Type: S400-24P
Slave: 00:04:96:1F:A7:3F
Primary EW Ver: 7.4e.0.28 [non-ssh]
Secondary EW Ver: 7.4e.0.10 branch-McastExtn_v74e0b10-r2 [non-ssh]
Image Selected: Primary
Image Booted: Primary
Config Selected: Primary
Config Booted: Primary
Primary Config: Empty
Secondary Config: Empty

Configured Type: Not configured
Inline-power:
  Total Common: 376W
  Consumed: 0.0W
UTP ports available:
  Link Active: [25]
  Link Down: 01 02 03 04 05 06 07 08
  09 10 11 12 13 14 15 16
  17 18 19 20 21 22 23 24

[26]

History
This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 7.0.0 to support WAN modules.

This command was modified in ExtremeWare 7.4 to support the details option and stacking on Summit switches.

Platform Availability
This command is available on modular switches and Summit 200, Summit 300-24, and Summit 400 switches configured in a stack.
As the module progresses through its initialization, the `show slot <slot>` command displays the general purpose processor (GPP) subsystem change state to OPERATIONAL, and then each of the network processors will change state to OPERATIONAL.

When the GPP subsystem completes its initialization cycle and the subsystem state is OPERATIONAL, use the `show diagnostics {<slot>}` command to check the results of the module power-on self test (POST).

If the STATUS LED on the ARM, ATM, MPLS or PoS module turns amber and blinks, use the `show slot <slot>` command to display the slot status information. The `show slot <slot>` command also displays operational information related to the ARM, ATM, MPLS or PoS module. Information displayed includes the BlackDiamond switch fabric card state (module state), Network Processor status, General Purpose Processor status, hardware serial number and type, and image version and boot settings.

For the ARM, ATM, MPLS, PoS, and WAN modules, the information displayed by this command includes data about the software images loaded on the module and information about the operational status and backplane connections of the module.

Example

The following example displays module information for all slots:

```
show slot
```

Following is the output from this command:

```
Slot 1 information:
  State:              Operational
  Serial number:      701028-06-0026F38445
  HW Module Type:     G8Ti

  Configured Type:    Not configured
  UTP ports available:
    Link Active:          01 02 03 04 05 06 07 08

Slot 2 information:
  State:              Operational
  Serial number:      701024-19-0125F06190
  HW Module Type:     G8Xi

  Configured Type:    Not configured
  Gigabit ports available:
    Link Active:          01
    Link Down:            GBIC missing:   02 03 04 05 06 07 08

Slot 3 information:
  State:              Operational
  Serial number:      701020-11-0032F51006
  HW Module Type:     G12SXi

  Configured Type:    Not configured
```
show slot

Gigabit ports available:
  Link Active: 01 02 03 04 05 06 07 08 09 10 11 12

Slot 4 information:
  State: Operational
  Network Processor 1: Operational
  Network Processor 2: Operational
  General Purpose Proc: Operational
  Serial number: 701039-04-0128F07843
  HW Module Type: P12ci
  Optics: Single-mode Fiber
  NP 1: Rev C0
  NP 2: Rev C0
  Configured Type: Not configured
  Bootrom Version: 1.18
  Software image booted: secondary
  Software image configured: secondary
  Primary software version:
    7.0.0 (Build 44) (oc12) by Beta_Master on Sat 10/12/2002 06:16p

  Secondary software version:
    7.0.0 (Build 44) (oc12) by Beta_Master on Sat 10/12/2002 06:16p

POS ports available:
  Link Up: 01 02

Slot 5 information:
  State: Operational
  Serial number: 701026-10-0142F70250
  HW Module Type: F48Ti

  Configured Type: Not configured
  UTP ports available:
  Link Active:
  Link Down: 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48

Slot 6 information:
  State: Empty
  HW Module Type: Empty
  Configured Type: Not configured

Slot 7 information:
  State: Empty
HW Module Type: Empty
Configured Type: Not configured

Slot 8 information:
  State: Empty
  HW Module Type: Empty
  Configured Type: Not configured

History
This command was first available in ExtremeWare 4.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 7.0.0 to support WAN modules.

This command was modified in ExtremeWare 7.4 to support the details option and stacking on Summit switches.

Platform Availability
This command is available on modular switches and Summit 200, Summit 300-24, and Summit 400 switches configured in a stack.
unconfigure msm-failover

Description
Disables hitless failover.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
The following occurs after you execute this command:

- The external ports are reset when an MSM failover occurs
- No state is preserved when a failover occurs
- The MSM failover timeout returns to 60 seconds
- The new master uses the configuration file kept in its flash memory upon failover

Example
The following command disables hitless failover and returns factory defaults:

unconfigure msm-failover

History
This command was first available in ExtremeWare 7.1.1.

Platform Availability
This command is available on BlackDiamond switches only.
unconfigure port aggregate-bandwidth

unconfigure port <portnumber> aggregate-bandwidth

Description
Restores the egress bandwidth of a particular port to 100%.

Syntax Description

| portnumber | Specifies a port or slot and port. |

Default
None

Usage Guidelines
None

Example
The following command restores the egress bandwidth of port 3 on slot 1 to 100%.
unconfigure port 1:3 aggregate-bandwidth

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on the “i” series platform.
unconfigure ports display string

unconfigure ports <portlist> display-string

Description
Clears the user-defined display string from one or more ports.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;portlist&gt;</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2-*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command removes the display string that you configured using the configure ports display-string command.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Example
The following command clears the user-defined display from port 4 on a stand-alone switch:
unconfigure ports 4 display-string

The following command clears the user-defined display string from slot 2, port 4 on a modular switch:
unconfigure ports 2:4 display-string

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure ports redundant

unconfigure ports [portlist] | <port id> redundant

Description
Clears a previously configured software-controlled redundant port.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8. |
| portid   | Specifies a port using the display string configured for the port. Only one port can be specified using this method. |

Default
N/A

Usage Guidelines
On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The <port id> is the display string configured for the port. Use the configure ports <portnumber> display-string <string> command to configure a display string for the port.

The list of port numbers or the port display string specifies the redundant port(s).

Example
The following command unconfigures a software-controlled redundant port on a stand-alone switch:

unconfigure ports 5 redundant

The output of the command is similar to:

Unconfig Redundant on Port 5
* Summit400-48t:33 # 07/24/2004 04:50:36.42 <Info:SYST> serial admin: unconfigure ports 5 redundant

The following command unconfigures a software-controlled redundant port on a modular switch:

unconfigure ports 2:3 redundant

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure slot

    unconfigure slot <slot number>

Description
Clears a slot of a previously assigned module type.

Syntax Description

| slot number | Specifies a slot on a modular switch. |

Default
N/A

Usage Guidelines
None

Example
The following command clears slot 4 of a previously assigned module type:
unconfigure slots 4

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on modular switches only.
This chapter describes the following commands:

- Commands for creating and deleting VLANs and performing basic VLAN configuration
- Commands for defining protocol filters for use with VLANs
- Commands for enabling or disabling the use of Generic VLAN Registration Protocol (GVRP) information on a switch and its ports

VLANs can be created according to the following criteria:

- Physical port—A port-based VLAN consists of a group of one or more ports on the switch. A port can be a member of only one port-based VLAN, and is by default a member of the VLAN named Default.
- 802.1Q tag—Tagging is most commonly used to create VLANs that span switches.
- Ethernet, LLC SAP, or LLC/SNAP Ethernet protocol type—Protocol-based VLANs are most often used in situations where network segments contain hosts running multiple protocols.

**NOTE**

Protocol-based VLANs are supported only on the "i" series and Summit 400 series switches.

- MAC address—MAC-based VLANs allow physical ports to be mapped to a VLAN based on the source MAC address learned in the FDB.
- A combination of these criteria.

The Generic VLAN Registration Protocol (GVRP) allows switches to learn some VLAN information automatically instead of requiring manual configuration in each switch. A VLAN can provide GVRP information about its VLANs and accept information about VLANs from other GVRP-enabled switches. Depending on the circumstances, information learned in this manner may cause ports to be added to VLANs already existing on the switch, or may cause new tagged VLANs to be created automatically.

**NOTE**

GVRP is not supported in ExtremeWare versions 6.1 or later, nor is it supported on the “e” series switches.
configure dot1q ethertype

configure dot1q ethertype <ethertype>

Description
Configures an IEEE 802.1Q Ethertype.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ethertype</td>
<td>Specifies an Ethertype value.</td>
</tr>
</tbody>
</table>

Default
Ethertype value of 8100.

Usage Guidelines
Use this command if you need to communicate with a switch that supports 802.1Q, but uses an Ethertype value other than 8100. This feature is useful for VMAN tunneling. Extreme Networks recommends the use of IEEE registered Ethertype 0x88a8 for deploying vMANs.

Extreme switches assume an Ethertype value of 8100.

You must reboot the switch for this command to take effect.

Example
The following command, followed by a switch reboot, changes the Ethertype value to 9100:

```
configure dot1q ethertype 9100
```

History
This command was first available in ExtremeWare 1.0.

Platform Availability
This command is available only on the “i” series platforms.
configure gvrp port

configure gvrp \{listen | send | both | none\} port <portlist>

Description
Configures the sending and receiving of Generic VLAN Registration Protocol (GVRP) information on a port.

**NOTE**
This command is available only on “i” series switches running ExtremeWare version 6.0 or earlier.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>listen</td>
<td>Enables the receipt of GVRP packets on the specified port(s).</td>
</tr>
<tr>
<td>send</td>
<td>Enables sending of GVRP packets on the specified port(s).</td>
</tr>
<tr>
<td>both</td>
<td>Enables both sending and receiving of GVRP packets.</td>
</tr>
<tr>
<td>none</td>
<td>Disables the port from participating in GVRP operation.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Both sending and receiving.

Usage Guidelines
GVRP must be enabled on the switch as a whole before GVRP data can be sent or received on individual ports.

If GVRP is enabled, **send** causes information (GVRP packets) about tagged VLANs on the switch to be sent on the specified ports, to neighboring GVRP-enabled switches.

If GVRP is enabled, **listen** means that the switch will receive and act on GVRP information it receives on the specified ports, from neighboring GVRP-enabled switches.

Example
The following commands configure port 3 to receive GVRP information only (by default it can send and listen) and then enables GVRP:

```
configure gvrp listen port 3
enable gvrp
```

If the switch receives GVRP information on this port, it will do one of the following:

- If a tagged VLAN already exists with a VLANid that matches the VLANid in the GVRP data, and port 3 is not already a member of that VLAN, add it as a tagged port.
- If no VLAN exists with a VLANid that matches the VLANid in the GVRP data, create a VLAN with the VLANid specified in the GVRP data, and add port 3 as a tagged member port.
VLAN Commands

History
This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 and later.

Platform Availability
This command is available only on the “i” series platforms running ExtremeWare version 6.0 or earlier.
configure mac-vlan add mac-address

configure mac-vlan add mac-address [any | <mac_address>] mac-group [any | <group_number>] vlan <vlan name>

Description
Adds a MAC address as a potential member of a MAC-based VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>The MAC address to be added to the specified VLAN. Specified in the form nn:nn:nn:nn:nn:nn. any indicates that any MAC-address associated with the specified MAC group may be a member.</td>
</tr>
<tr>
<td>group_number</td>
<td>The group number that should be associated with the specified MAC address. Specified as an integer any indicates that this MAC address can be associated with any MAC group.</td>
</tr>
<tr>
<td>vlan name</td>
<td>The name of the VLAN with which this MAC address should associated.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The specified MAC address must be associated with an end station or host only, not a layer 2 repeater device.

Adding a MAC address means that when the specified address is detected on a member port, as specified by its group membership, it can participate in the VLAN.

At least one port must be enabled to use the MAC-based VLAN algorithm before any MAC addresses can be added.

The group number is an integer in the range 1 – 65535. A group number of 0 (zero) is equivalent to specifying the group number as any.

Example
Given ports enabled for MAC-based VLANs as follows:
enable mac-vlan mac-group any ports 16,17
enable mac-vlan mac-group 10 ports 11,12

The following command sets up the end-station with MAC address 00:00:00:00:00:01 to participate in VLAN engineering via the MAC-enabled ports 16 or 17:
configure mac-vlan add mac-address 00:00:00:00:00:01 mac-group any vlan engineering

MAC address 00:00:00:00:00:01 cannot get access via ports 11 or 12 because it is not configured for mac-group 10.
The following command sets up the end-station 00:00:00:00:00:02 to participate in VLAN engineering through the ports in group 10 (ports 11 or 12) or through ports 16 or 17 (enabled for any mac-group):

```bash
configure mac-vlan add mac-address 00:00:00:00:00:02 mac-group 10 vlan engineering
```

**History**
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure mac-vlan delete

configure mac-vlan delete [all | mac-address [<mac_address> | any]]

**Description**
Removing a MAC address from any MAC-based VLANs with which it was associated.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Indicates that all MAC addresses should be removed from all VLANs.</td>
</tr>
<tr>
<td>mac-address any</td>
<td>will match all the source MAC addresses that are not matched by specific MAC addresses given for the MAC group.</td>
</tr>
</tbody>
</table>

**Default**
NA

**Usage Guidelines**
None

**Examples**
The following command removes the end-station with MAC address 00:00:00:00:00:02 from participating in any MAC-based VLANs.

```bash
configure mac-vlan delete mac-address 00:00:00:00:00:02
```

The following command removes all MAC addresses from participating in any VLANs:

```bash
configure mac-vlan delete all
```

**History**
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure ports monitor vlan

configure ports <portlist> monitor vlan <vlan name>

Description
Configures VLAN statistic monitoring on a per-port basis.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
When per-port monitoring is configured, the show ports command displays the latest statistics directly from the hardware in real time. This information is not logged.

Examples
The following command configures per-port monitoring for a set of ports on slot 8 for the VLAN named accounting:

configure ports 8:1-8:6 monitor vlan accounting

You can monitor up to four VLANs on the same port by issuing the command four times. For example, if you want to monitor VLANs dog1, dog2, dog3, and dog4 on slot 1, use the following commands:

configure ports 1:* monitor vlan dog1
configure ports 1:* monitor vlan dog2
configure ports 1:* monitor vlan dog3
configure ports 1:* monitor vlan dog4

After you have configured the ports for monitoring, you can use the show ports vlan statistics command to display information for the configured ports:

show ports 1:* vlan statistics

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available only on the “i” series platforms.
configure protocol add

    configure protocol <protocol_name> add <protocol_type> <hex_value>
    {<protocol_type> <hex_value>} ...

Description
Configures a user-defined protocol filter.

NOTE

This command is available only on the “i” series switches and the Summit 400-48t.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol_name</td>
<td>Specifies a protocol filter name.</td>
</tr>
</tbody>
</table>
| protocol_type | Specifies a protocol type. Supported protocol types include:  
                  • etype – IEEE Ethertype.  
                  • llc – LLC Service Advertising Protocol.  
                  • snap – Ethertype inside an IEEE SNAP packet encapsulation.                  |
| hex_value   | Specifies a four-digit hexadecimal number between 0 and FFFF that represents:  
                  • The Ethernet protocol type taken from a list maintained by the IEEE.  
                  • The DSAP/SSAP combination created by concatenating a two-digit LLC Destination SAP (DSAP) and a two-digit LLC Source SAP (SSAP).  
                  • The SNAP-encoded Ethernet protocol type.                                     |

Default
N/A

Usage Guidelines

A maximum of 15 protocol filters, each containing a maximum of six protocols, can be defined.

The protocol filter must already exist before you can use this command: use the create protocol command to create the protocol filter.

On the “i” series switches, all fifteen protocol filters can be active and configured for use. On the Summit 400-48t switches, no more than seven protocols can be active and configured for use.

Example

The following command configures a protocol named Fred by adding protocol type LLC SAP with a value of FFEF:

```
configure protocol fred add llc feff
```

History

This command was first available in ExtremeWare 1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability

This command is available on the “i” series platforms and the Summit 400-48t.
configure protocol delete

configure protocol <protocol_name> delete <protocol_type> <hex_value> {<protocol_type> <hex_value>} ...

Description
Deletes the specified protocol type from a protocol filter.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>protocol_name</td>
<td>Specifies a protocol filter name.</td>
</tr>
<tr>
<td>protocol_type</td>
<td>Specifies a protocol type. Supported protocol types include:</td>
</tr>
<tr>
<td></td>
<td>• etype – IEEE Ethertype.</td>
</tr>
<tr>
<td></td>
<td>• llc – LLC Service Advertising Protocol.</td>
</tr>
<tr>
<td></td>
<td>• snap – Ethertype inside an IEEE SNAP packet encapsulation.</td>
</tr>
<tr>
<td>hex_value</td>
<td>Specifies a four-digit hexadecimal number between 0 and FFFF that represents:</td>
</tr>
<tr>
<td></td>
<td>• The Ethernet protocol type taken from a list maintained by the IEEE.</td>
</tr>
<tr>
<td></td>
<td>• The DSAP/SSAP combination created by concatenating a two-digit LLC Destination SAP (DSAP) and a two-digit LLC Source SAP (SSAP).</td>
</tr>
<tr>
<td></td>
<td>• The SNAP-encoded Ethernet protocol type.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command deletes protocol type LLC SAP with a value of FFEF from protocol fred:
configure protocol fred delete llc feff

History
This command was first available in ExtremeWare 1.0.

Platform Availability
This command is available on the “i” series platforms and on the Summit 400-48t.
configure vlan add member-vlan

configure vlan <translation vlan name> add member-vlan <vlan name>

Description
Adds a member VLAN to a translation VLAN.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>translation vlan name</td>
<td>Specifies a translation VLAN.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN to add to the translation VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command adds a member VLAN to a translation VLAN. The 802.1Q tags for member VLANs are translated to the single tag of the translation VLAN. Then the layer 2 traffic from the member VLANs is carried by a single VLAN, improving VLAN scaling.

Traffic is switched locally between client devices on the same member VLANs, just as on normal VLANs. Traffic cannot be switched between clients on separate member VLANs. Traffic from any member VLAN destined for the translation VLAN is switched and the VLAN tag is translated appropriately. Traffic from the translation VLAN destined for any member VLAN is switched and the VLAN tag is translated.

The added VLAN cannot have an IP address configured or already be a member VLAN or a translation VLAN; it must contain only “i” series module Ethernet ports. In addition, ESRP, Network Login, or DHCP cannot be enabled on any ports belonging to either the member VLAN or the translation VLAN.

Example
The following command adds the member VLAN named v101 to the translation VLAN named v1000:

```plaintext
configure vlan v1000 add member-vlan v101
```

History
This command was first available in ExtremeWare 7.1.0.

Platform Availability
This command is available only on the “i” series platforms.
configure vlan add ports

For “i” series switches:

    configure vlan <vlan name> add ports <portlist> {tagged | untagged} {nobroadcast} {soft-rate-limit}

For “e” series switches:

    configure vlan <vlan name> add ports <portlist> {tagged | untagged}

**Description**

Adds one or more ports in a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>tagged</td>
<td>Specifies the ports should be configured as tagged.</td>
</tr>
<tr>
<td>untagged</td>
<td>Specifies the ports should be configured as untagged.</td>
</tr>
<tr>
<td>nobroadcast</td>
<td>Prevents broadcasts, multicasts, and unknowns from being transmitted on these ports.</td>
</tr>
<tr>
<td>soft-rate-limit</td>
<td>Specifies that these ports should be added as rate-shaped ports. (ExtremeWare 6.0)</td>
</tr>
</tbody>
</table>

**Default**

Untagged

**Usage Guidelines**

The VLAN must already exists before you can add or delete ports: use the `create vlan` command to create the VLAN.

If the VLAN uses 802.1Q tagging, you can specify tagged or untagged port(s). If the VLAN is untagged, the ports cannot be tagged.

Untagged ports can only be a member of a single VLAN. By default, they are members of the default VLAN named Default. To add untagged ports to a different VLAN, you must first remove them from the default VLAN. You do not need to do this to add them to another VLAN as tagged ports.

You must configure a loopback port with a unique loopback VLAN tag ID before adding rate-shaped ports.

This command is not supported on SONET modules.

**Example**

The following command assigns tagged ports 1, 2, 3, and 6 to a VLAN named `accounting`:

    configure vlan accounting add ports 1, 2, 3, 6 tagged
VLAN Commands

**History**
This command was first available in ExtremeWare 1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2e to support rate limiting with the `soft-rate-limit` keyword.

**Platform Availability**
This command is available on all platforms. It is not supported on SONET modules.
configure vlan add ports loopback-vid

configure vlan <vlan name> add ports <portlist> loopback-vid <vlan-id>

Description
Adds a loopback port to a VLAN.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a loopback port for the VLAN.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Specifies a unique loopback VLAN tag.</td>
</tr>
</tbody>
</table>

Default
Untagged

Usage Guidelines
The VLAN must already exist before you can add or delete ports. Use the create vlan command to create the VLAN.

You must configure a loopback port with a unique loopback VLAN tag ID before adding rate-shaped ports.

This command is not supported on SONET modules.

Example
The following example sets up bi-directional rate shaping using a loopback port and a rate-shaped port.

First, create the VLAN that will have rate-shaped ports as members:
create vlan ratelimit

Create the loopback port to rate-shape ingress traffic:
configure vlan ratelimit add ports 1 loopback-vid 100

Configure the user port that will be rate-shaped:
configure vlan ratelimit add ports 2 soft-rate-limit

Configure rate-shaping to be at 5% maximum bandwidth for ingress and egress traffic:
configure qosprofile QP1 minbw 0 % maxbw 5 % priority low 1,2
**History**
This command was first available in ExtremeWare 6.0.

**Platform Availability**
This command is available only on the “i” series platforms.
configure vlan add secondary-ip

configure vlan <vlan-name> add secondary-ip <sec-ip-address> {<sec-ip-mask> | <mask-length>}

Description
Configures the secondary IP address for the selected VLAN.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be configured.</td>
</tr>
<tr>
<td>add-secondary-ip</td>
<td>Specifies that the secondary IP address is to be configured.</td>
</tr>
<tr>
<td>sec-ip-address</td>
<td>Specifies the secondary IP address for the VLAN.</td>
</tr>
<tr>
<td>sec-ip-mask</td>
<td>(Optional) Specifies the network mask.</td>
</tr>
<tr>
<td>mask-length</td>
<td>(Optional) Specifies the network mask in bits.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to configure a secondary IP address for the specified VLAN.

Secondary IP addresses specify a local subnet on the switch and must be unique.

Multinetworking must have been globally enabled before a secondary IP address is configured for a VLAN.

You can configure a maximum of 64 secondary IP addresses.

A secondary IP address can be configured only if a primary IP address has been configured already for the VLAN.

Secondary IP addresses cannot be modified. They must be deleted and added again. Use the following command to delete a secondary IP address:

`configure vlan delete secondary-ip`

Example
The following command configures the secondary IP address for the VLAN named `test1`:

`configure vlan test1 add secondary-ip 95.0.0.1/24`
History
This command was enhanced for multinetting and made available in ExtremeWare 7.3.0. In earlier releases of ExtremeWare the secondary IP addresses must fall in the same subnet as the primary IP address. With ExtremeWare 7.3.0, secondary IP addresses specify local subnets in the switch and must be unique.

When a secondary IP address configuration of a pre-ExtremeWare 7.3.0 release is restored with an ExtremeWare 7.3.0 image, the following syslog message will be logged:

<WARN:IPRT> Secondary IP Address <x.x.x.x>/32 will not be used.

Platform Availability
This command is available only on the “i” series platforms.
configure vlan delete member-vlan

    configure vlan <translation vlan name> delete member-vlan [<vlan name> | all]

Description
Deletes a member VLAN from a translation VLAN.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>translation vlan name</td>
<td>Specifies a translation VLAN.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN to add to the translation VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes a member VLAN from a translation VLAN. Use the all keyword to delete all the member VLANs from the specified translation VLAN.

Example
The following command deletes the member VLAN named v101 from the translation VLAN named v1000:
configure vlan v1000 delete member-vlan v101

History
This command was first available in ExtremeWare 7.1.0.

Platform Availability
This command is available only on the "i" series platforms.
configure vlan delete port

configure vlan <vlan name> delete port [all | <portlist>]

Description
Deletes one or more ports in a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>A list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes ports 1, 2, 3, and 6 from a VLAN named accounting:

configure accounting delete port 1, 2, 3, 6

History
This command was first available in ExtremeWare 1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure vlan delete secondary-ip

configure vlan <vlan-name> delete secondary-ip {<sec-ip-address> | all}

Description
Deletes a secondary IP address from the specified VLAN.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be configured.</td>
</tr>
<tr>
<td>sec-ip-address</td>
<td>Specifies the secondary IP address to be deleted.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all secondary IP addresses must be deleted.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to delete a secondary IP address from the specified VLAN.
A secondary IP address cannot be deleted from a VLAN if VRRP IDs are associated with the secondary IP address.
Deletion of a secondary IP address automatically deletes the DHCP address ranges associated with the secondary IP address.

Example
The following command deletes a secondary IP address from the VLAN named test1:
configure vlan test1 delete secondary-ip 95.0.0.1/24

History
This command was modified to enhance the multinetting implementation. It was made available in ExtremeWare 7.3.0.

Platform Availability
This command is available only on the “i” series platforms.
configure vlan ipaddress

configure vlan <vlan name> ipaddress <ipaddress> {<netmask> | <mask length>}

Description
Assigns an IP address and an optional subnet mask to the VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a subnet mask in dotted-quad notation (for example, 255.255.255.0).</td>
</tr>
<tr>
<td>mask length</td>
<td>Specifies a subnet mask as the number of bits (for example, /24).</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The VLAN must already exist before you can assign an IP address. Use the create vlan command to create the VLAN.

⚠️ NOTE
If you plan to use the VLAN as a control VLAN for an EAPS domain, do NOT configure the VLAN with an IP address.

Example
The following commands are equivalent; both assign an IP address of 10.12.123.1 to a VLAN named accounting:

- `configure vlan accounting ipaddress 10.12.123.1/24`
- `configure vlan accounting ipaddress 10.12.123.1 255.255.255.0`

History
This command was first available in ExtremeWare 1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure vlan name

configure vlan <old_name> name <new_name>

Description
Renames a previously configured VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>old_name</td>
<td>Specifies the current (old) VLAN name.</td>
</tr>
<tr>
<td>new_name</td>
<td>Specifies a new name for the VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You cannot change the name of the default VLAN Default.

Example
The following command renames VLAN vlan1 to engineering:
configure vlan vlan1 name engineering

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure vlan protocol

configure vlan <vlan name> protocol [<protocol_name> | any]

Description
Configures a VLAN to use a specific protocol filter.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>protocol_name</td>
<td>Specifies a protocol filter name. This can be the name of a predefined protocol filter or one you have defined. The following protocol filters are predefined:</td>
</tr>
<tr>
<td></td>
<td>• IP</td>
</tr>
<tr>
<td></td>
<td>• IPX</td>
</tr>
<tr>
<td></td>
<td>• NetBIOS</td>
</tr>
<tr>
<td></td>
<td>• DECNet</td>
</tr>
<tr>
<td></td>
<td>• IPX_8022</td>
</tr>
<tr>
<td></td>
<td>• IPX_SNAP</td>
</tr>
<tr>
<td></td>
<td>• AppleTalk</td>
</tr>
<tr>
<td>any</td>
<td>Indicates that this VLAN should act as the default VLAN for its member ports.</td>
</tr>
</tbody>
</table>

Default
Protocol any

Usage Guidelines
If the keyword any is specified, all packets that cannot be classified into another protocol-based VLAN are assigned to this VLAN as the default for its member ports.

Use the configure protocol command to define a custom protocol filter.

Example
The following command configures a VLAN named accounting as an IP protocol-based VLAN:

configure accounting protocol ip

History
This command was first available in ExtremeWare 1.0.

Platform Availability
This command is available on the “i” series platforms and on the Summit 400-48t.
configure vlan tag

    configure vlan <vlan name> tag <vlan tag>

**Description**

Assigns a unique 802.1Q tag to the VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>vlan tag</td>
<td>Specifies a value to use as an 802.1Q tag. The valid range is from 2 to 4,095.</td>
</tr>
</tbody>
</table>

**Default**

The default VLAN uses an 802.1Q tag (and an internal VLANid) of 1.

**Usage Guidelines**

If any of the ports in the VLAN will use an 802.1Q tag, a tag must be assigned to the VLAN. The valid range is from 2 to 4,095. (Tag 1 is assigned to the default VLAN.)

The 802.1Q tag will also be used as the internal VLANid by the switch.

You can specify a value that is currently used as an internal VLANid on another VLAN; it will become the VLANid for the VLAN you specify, and a new VLANid will be automatically assigned to the other untagged VLAN.

**Example**

The following command assigns a tag (and internal VLANid) of 120 to a VLAN named `accounting`:

```
configure accounting tag 120
```

**History**

This command was first available in ExtremeWare 1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
create protocol

create protocol <protocol_name>

Description
Creates a user-defined protocol filter.

NOTE
This command is available only on the “i” series switches and the Summit 400-48t.

Syntax Description

| protocol_name | Specifies a protocol filter name. The protocol filter name can have a maximum of 31 characters. |

Usage Guidelines
Protocol-based VLANs enable you to define packet filters that the switch can use as the matching criteria to determine if a particular packet belongs to a particular VLAN.

After you create the protocol, you must configure it using the configure protocol add command. To assign it to a VLAN, use the configure vlan protocol command.

Example
The following command creates a protocol named fred:
create protocol fred

History
This command was first available in ExtremeWare 1.0.

This command was added to the Summit 400-48t switch in ExtremeWare 7.2e.

Platform Availability
This command is available on the “i” series platforms and the Summit 400-48t.
create vlan

    create vlan <vlan name>

Description
Creates a named VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name (up to 32 characters).</td>
</tr>
</tbody>
</table>

Default
A VLAN named Default exists on all new or initialized Extreme switches:

- It initially contains all ports on a new or initialized switch, except for the management port(s), if there are any.
- It has an 802.1Q tag of 1.
- The default VLAN is untagged on all ports.
- It uses protocol filter any.

An untagged VLAN named MacVlanDiscover exists on all new or initialized Extreme switches:

- It initially contains no ports.
- It does not initially use an 802.1Q tag, and is assigned the next available internal VLANid starting with 4095.

A VLAN named Mgmt exists on switches that have management modules or management ports.

- It initially contains the management port(s) on the switch.
- It is assigned the next available internal VLANid as an 802.1Q tag.

Usage Guidelines
A newly created VLAN has no member ports, is untagged, and uses protocol filter “any” until you configure it otherwise. Use the various `configure vlan` commands to configure the VLAN to your needs.

Internal VLANids are assigned automatically using the next available VLANid starting from the high end (4095) of the range.

Each VLAN name can be up to 32 standard alphanumeric characters, but must begin with an alphabetical letter. Quotation marks can be used to enclose a VLAN name that does not begin with an alphabetical character, or that contains a space, comma, or other special character.

VLAN names are locally significant. That is, VLAN names used on one switch are meaningful only to that switch. If another switch is connected to it, the VLAN names have no significance to the other switch.
Example
The following command creates a VLAN named *accounting*:
```
create vlan accounting
```

History
This command was first available in ExtremeWare 1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
delete protocol

delete protocol <protocol_name>

Description
Deletes a user-defined protocol.

Syntax Description

| protocol_name | Specifies a protocol name. |

Default
N/A

Usage Guidelines
If you delete a protocol that is in use by a VLAN, the protocol associated with that VLAN becomes “none.”

Example
The following command deletes a protocol named fred:

delete protocol fred

History
This command was first available in ExtremeWare 1.0.

Platform Availability
This command is available on the “i” series platforms and on the Summit 400-48t.
delete vlan

   delete vlan <vlan name>

Description
Deletes a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you delete a VLAN that has untagged port members, and you want those ports to be returned to the default VLAN, you must add them back explicitly using the `configure vlan add ports` command.

**NOTE**
The default VLAN cannot be deleted.

Example
The following command deletes the VLAN accounting:

delte accounting

History
This command was first available in ExtremeWare 1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable gvrp

disable gvrp

Description
Disables the Generic VLAN Registration Protocol (GVRP).

NOTE
This command is available only on the “i” series switches running ExtremeWare version 6.0 or earlier.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command globally disables GVRP functionality on the switch. It does not change the GVRP configuration of individual ports, but GVRP will no longer function on these ports.

GVRP is not supported in ExtremeWare version 6.1 or later.

Example
The following command disables GVRP functionality:

disable gvrp

History
This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 or later.

Platform Availability
This command is available only on the “i” series platforms running ExtremeWare 6.0 or earlier.
**disable mac-vlan port**

```
disable mac-vlan port <portlist>
```

**Description**
Disables a port from using the MAC-based VLAN algorithm.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6:2:8.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**
Disabling a port removes it from the MacVlanDiscover VLAN, but does not automatically return it to the default VLAN. If you need this port to be a member of the default VLAN, you must explicitly add it back.

**Example**
The following command disables ports 16 and 17 from using the MAC-based VLAN algorithm:

```
disable mac-vlan port 16,17
```

**History**
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
enable gvrp

enable gvrp

Description
Enables the Generic VLAN Registration Protocol (GVRP).

NOTE
This command is available only on the “i” series switches running ExtremeWare version 6.0 or earlier.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
The GVRP protocol allows switches to automatically discover some of the VLAN information that would otherwise have to be manually configured in each switch.

GVRP must be enabled on individual ports before GVRP information will be sent or received.

By default, GVRP is enabled for both sending and receiving on all ports, so executing this command will normally “turn on” GVRP functionality.

GVRP is not supported in ExtremeWare version 6.1 or later.

Example
The following command enables GVRP functionality:

```
enable gvrp
```

History
This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 or later.

Platform Availability
This command is available only on the “i” series platforms running ExtremeWare version 6.0 or earlier.
enable mac-vlan mac-group port

    enable mac-vlan mac-group [any | <group_number>] port <portlist>

Description
Enables a port to use the MAC-based VLAN algorithm.

Syntax Description

<table>
<thead>
<tr>
<th>group_number</th>
<th>A group number that should be associated with a specific set of ports. Specified as an integer.</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>indicates that these ports can be considered members of any MAC group.</td>
</tr>
<tr>
<td>portlist</td>
<td>A list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
At least one port must be enabled to use the MAC-based VLAN algorithm before any MAC addresses can be added.

Enabling ports for MAC-based VLAN usage automatically adds them to the VLAN called MacVlanDiscover as untagged ports.

In order to enable ports as part of a MAC group, they cannot be untagged members of any other VLAN. Before you can enable them, you must ensure that they have been removed from the default VLAN (named Default).

The group number is an integer in the range from 0 – 65535. A group number of 0 (zero) is equivalent to specifying the mac-group as any.

Examples
The following set of commands removes ports 16 and 17 from the default VLAN, and then enables them for use with the MAC-based VLAN associated with any MAC group:

```bash
configure default delete port 16, 17
enable mac-vlan mac-group any port 16,17
```

The following commands enable ports 11 and 12 for use with a MAC-based VLAN associated with MAC group 10:

```bash
configure default delete port 11, 12
enable mac-vlan mac-group 10 port 11,12
```

History
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
show gvrp

show gvrp

**Description**
Displays the current configuration and status of GVRP.

**NOTE**
This command is available only on the “i” series switches running ExtremeWare 6.0 or earlier.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A

**Usage Guidelines**
GVRP is not supported in ExtremeWare version 6.1 or later.

**Example**
The following shows results of this command:

GVRP running (866422): JoinTime 20  LeaveTime 200  LeaveAllTime 1000 cs
GVRP transmit 0 receive 0 tx errors 0 rx errors 0 int errors 0
Enabled for Tx/Rx on ports: 123456789
10111213141516171819
20212223242526272829
303132
VLAN/Ports (t=static tagged, u=static untag, G=GVRP tagged, g=GVRP untag)
Default (Tag 1)
................................
Mgmt (Tag 4094)
................................
nat (Tag 4093)
................................

**History**
This command was first available in ExtremeWare 2.0.

This command exists but is not supported in ExtremeWare version 6.1 or later.

**Platform Availability**
This command is available only on the “i” series platforms running ExtremeWare version 6.0 or earlier.
show mac-vlan

    show mac-vlan {configuration | database}

Description
Displays the MAC-based VLAN configuration and MAC address database content.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>configuration</td>
<td>Specifies display of the MAC-based VLAN configuration only.</td>
</tr>
<tr>
<td>database</td>
<td>Specifies display of the MAC address database content only.</td>
</tr>
</tbody>
</table>

Default
Shows both configuration and database information.

Usage Guidelines
Use the keyword configuration to display only the top section of this information. Use the database keyword to display only the lower section.

Example
The following is an example of the show mac-vlan command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Vlan</th>
<th>Group</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>11</td>
<td>MacVlanDiscover</td>
<td>10</td>
<td>Discover</td>
</tr>
<tr>
<td>12</td>
<td>MacVlanDiscover</td>
<td>10</td>
<td>Discover</td>
</tr>
<tr>
<td>16</td>
<td>MacVlanDiscover</td>
<td>any</td>
<td>Discover</td>
</tr>
<tr>
<td>17</td>
<td>MacVlanDiscover</td>
<td>any</td>
<td>Discover</td>
</tr>
</tbody>
</table>

Total Entries in Database: 2

<table>
<thead>
<tr>
<th>Mac</th>
<th>Vlan</th>
<th>Group</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:00:00:00:AA</td>
<td>anntest1</td>
<td>any</td>
</tr>
<tr>
<td>any</td>
<td>anntest1</td>
<td>10</td>
</tr>
</tbody>
</table>

2 matching entries

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show protocol

    show protocol {<protocol>}

Description
Displays protocol filter definitions.

Syntax Description

| protocol | Specifies a protocol filter name. |

Default
Displays all protocol filters.

Usage Guidelines
Displays the defined protocol filter(s) with the types and values of its component protocols.

Example
The following is an example of the show protocol command:

<table>
<thead>
<tr>
<th>Protocol Name</th>
<th>Type</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP</td>
<td>etype</td>
<td>0x0800</td>
</tr>
<tr>
<td></td>
<td>etype</td>
<td>0x0806</td>
</tr>
<tr>
<td>ipx</td>
<td>etype</td>
<td>0x8137</td>
</tr>
<tr>
<td>netbios</td>
<td>llc</td>
<td>0xf0f0</td>
</tr>
<tr>
<td></td>
<td>llc</td>
<td>0xf0f1</td>
</tr>
<tr>
<td>decnet</td>
<td>etype</td>
<td>0x6003</td>
</tr>
<tr>
<td></td>
<td>etype</td>
<td>0x6004</td>
</tr>
<tr>
<td>appletalk</td>
<td>snap</td>
<td>0x809b</td>
</tr>
<tr>
<td></td>
<td>snap</td>
<td>0x80f3</td>
</tr>
<tr>
<td>ipx_8022</td>
<td>llc</td>
<td>0xe0e0</td>
</tr>
<tr>
<td>ipx_snap</td>
<td>snap</td>
<td>0x8137</td>
</tr>
</tbody>
</table>

NOTE
Output referring to IPX is displayed only on the "i" series platforms.

History
This command was first available in ExtremeWare 1.0.

This command was added to the Summit "e" series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show vlan

For the "i" series platforms:

    show vlan {
        <vlan name> | detail | stats <vlan-name>
    }

For the "e" series platforms:

    show vlan {
        <vlan name> | detail
    }

**Description**

Displays configuration information about specified VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN whose configuration is to be displayed.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that detailed information should be displayed for each VLAN.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the &quot;i&quot; series switches.</td>
</tr>
<tr>
<td>stats</td>
<td>Specifies a real-time display of utilization statistics (packets transmitted and received) for a specific VLAN.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the &quot;i&quot; series switches.</td>
</tr>
</tbody>
</table>

**Default**

Summary information for all VLANs on the device.

**Usage Guidelines**

Unlike many other VLAN-related commands, the keyword vlan is required in all forms of this command except when requesting information for a specific vlan.

Use the command show vlan to display summary information for all VLANs. It shows various configuration options as a series of "flags" (see the example below). VLAN and protocol names may be abbreviated in this display.

**For the "i" Series Switches.** Use the command show vlan detail on "i" series switches to display detailed information for all VLANs. This displays the same information as for an individual VLAN, but shows every VLAN, one by one. After each VLAN information display you can elect to continue or quit.

Protocol None in the output indicates that this VLAN was configured with a user-defined protocol that has subsequently been deleted.

Use the command show vlan stats <vlan name> on "i" series switches to show real-time statistics for the number of packets transmitted and received for the named VLAN. This command continues to run until you cancel it using the [Esc] key.

Using the detail option of this command displays secondary IP addresses, which are displayed in the line following the primary IP address output.
### Examples

The following is an example of the `show vlan` command:

```
MSM64:1 # show vlan
Name           VID Protocol Addr       Flags     Proto  Ports
Default        1   0.0.0.0          /BP -----T-------- ANY     0/7
MacVlanDiscover 4095 ------------------ ANY 0/0
Mgmt           4094 10.5.4.80        /24 ------------- ANY     1/1
pv1            4093 192.168.11.1    /24 -------f------- ANY     0/1
pv2            4092 192.168.12.1    /24 -------f------- ANY     0/1
pv3            4091 ------------------ ------- ANY 0/0
pv4            4090 ------------------ ------- ANY 0/0
```

**Flags:**  
- (C) Domain-masterVlan,  
- (c) Domain-memberVlan,  
- (d) DVMRP Enabled  
- (E) ESRP Slave,  
- (f) IP Forwarding Enabled,  
- (G) GVRP Enabled  
- (i) ISIS Enabled,  
- (L) Loopback Enabled,  
- (m) IPmc Forwarding Enabled  
- (N) GNS Reply Enabled,  
- (o) OSPF Enabled,  
- (P) IPX SAP Enabled  
- (p) PIM Enabled,  
- (R) SubVLAN IP Range Configured,  
- (r) RIP Enabled  
- (S) SuperVlan,  
- (s) SubVlan,  
- (T) Member of STP Domain  
- (v) VRRP Enabled,  
- (X) IPX RIP Enabled  
- (2) IPX Type 20 Forwarding Enabled

Total number of Vlan(s) : 7

The following is an example of the `show vlan Default` command:

```
show vlan Default
VLAN Interface[0-200] with name "Default" created by user
  Tagging: 802.1Q Tag 1
  Priority: 802.1P Priority 7
  IP: 51.0.0.1/255.255.255.0
  Sec.IP 53.0.0.1/255.255.255.0
  STPD: s0(Disabled,Auto-bind)
  Protocol: Match all unfiltered protocols.
  Loopback: Disable
  RateShape: Disable
  QosProfile:QP1
  QosIngress:None
  Ports: 72. (Number of active ports=1)
  Flags: (*) Active, (!) Disabled
           (B) BcastDisabled, (R) RateLimited, (L) Loopback
           (g) Load Share Group
          4:1 4:2 4:3 4:4 4:5 4:6 4:7 4:8
```
The following example shows the detail information for VLAN, called “v2,” which contains a port for a load-sharing group that spans multiple modules:

```
show vlan detail
...
VLAN Interface[3-201] with name "v2" created by user
  Tagging:  802.1Q Tag 2
  Priority: 802.1P Priority 7
  IP:      10.222.0.2/255.255.255.0
  STPD:   s0(Disabled,Auto-bind)
  Protocol: Match all unfiltered protocols.
  Loopback: Disable
  RateShape: Disable
  QosProfile:QP1
  QosIngress:IQP1
  Ports:   5.  (Number of active ports=4)
   Flags:  * - Active, ! - Disabled
         B - BcastDisabled, R - RateLimited, L - Loopback
         (g) Load Share Group, (c) Cross Module Trunk
  Untag:  *1:25  5:10  5:25  7:25
  Tagged:  *5:4c
...
```

**History**

This command was first available in ExtremeWare 1.0.

This command was modified to support longer VLAN names in ExtremeWare 6.2.2.

This command was modified to include the Member of STP Domain flag in ExtremeWare 7.0.

This command was modified to support the “3” series modules in ExtremeWare 7.0.1.

This command was modified to include the cross-module trunk flag in ExtremeWare 7.1.1.

The output of this command was changed to accommodate the multinetting feature by including secondary IP addresses. This modified command was made available in ExtremeWare 7.3.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
unconfigure ports monitor vlan

unconfigure ports <portlist> monitor vlan <vlan name>

Description
Removes port-based VLAN monitoring.

NOTE
This command is available only on the “i” series switches.

Syntax Description
| portlist  | Specifies one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |
| vlan name  | Specifies a VLAN name. |

Default
N/A

Usage Guidelines
None

Example
The following command removes monitoring for ports on VLAN accounting:
unconfigure ports 8:1-8:6 monitor vlan accounting

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available only on the “i” series platforms.
unconfigure vlan ipaddress

unconfigure vlan <vlan name> ipaddress

Description
Removes the primary IP address of a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN for which the primary IP address is to be unconfigured.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to remove the primary IP address on a VLAN. The primary IP address will be cleared only if there are no secondary IP address(es) configured for the VLAN.

Example
The following command removes the primary IP address for the VLAN named vlantest4:
unconfig vlan vlantest4 ip-address

History
This command was first available in ExtremeWare 1.0.
This command was modified to enhance the multinetting implementation. It was made available in ExtremeWare 7.3.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
This chapter describes commands for:

- Configuring FDB entries
- Displaying FDB entries
- Configuring and enabling FDB scanning

The switch maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered.

Each FDB entry consists of the MAC address of the device, an identifier for the port on which it was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not in the FDB are flooded to all members of the VLAN.

The FDB has four types of entries:

- **Dynamic entries**—Initially, all entries in the database are dynamic. Entries in the database are removed (aged-out) if, after a period of time (aging time), the device has not transmitted. This prevents the database from becoming full of obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Dynamic entries are deleted from the database if the switch is reset or a power off/on cycle occurs.

- **Nonaging entries**—If the aging time is set to zero, all aging entries in the database are defined as static, nonaging entries. This means that they do not age, but they are still deleted if the switch is reset.

- **Permanent entries**—Permanent entries are retained in the database if the switch is reset or a power off/on cycle occurs. The system administrator must create permanent entries. A permanent entry can be either a unicast or multicast MAC address. All entries entered through the command line interface (CLI) are stored as permanent.

- **Blackhole entries**—A blackhole entry configures the switch to discard packets with a specified MAC destination address. Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged out of the database.

Entries are added into the FDB in the following two ways:

- The switch can learn entries. The system updates its FDB with the source MAC address from a packet, the VLAN, and the port identifier on which the source packet is received.

- You can enter and update entries using a MIB browser, an SNMP network manager, or the CLI. A QoS profile can be associated with a MAC address (and VLAN) of a device that will be dynamically learned. The FDB treats the entry like a dynamic entry (it is learned, it can be aged out of the database, and so on). The switch applies the QoS profile as soon as the FDB entry is learned.
clear fdb

On the “i” series of switches:

    clear fdb {<mac_address> | blackhole | ports <portlist> | remap | vlan <vlan name>}

On the “e” series of switches:

    clear fdb {<mac_address> | blackhole | ports <portlist> | vlan <vlan name>}

Description

Clears dynamic FDB entries that match the filter.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address, using colon-separated bytes.</td>
</tr>
<tr>
<td>blackhole</td>
<td>Specifies the blackhole entries.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports. May be in the form 1, 2, 3-5, 2:* 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>remap</td>
<td>Clears the remapped and questionable FDB entries.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default

Clears all dynamic FDB entries.

Usage Guidelines

This command clears FDB entries based on the specified criteria. When no options are specified, the command clears all dynamic FDB entries.

On the “i” Series of Switches. The system health checker also checks the integrity of the FDB. If you enable the system health checker, a section of the FDB memory on each module’s switching fabric is non-intrusively compared to the software copy of the FDB. The switch takes one of the following actions if it detects a bad entry:

- If the entry is not in use—remaps around the entry location
- If the entry is in use, but is safely removable (most MAC and IP-DA entries)—removes the questionable entry, allows the table to be rebuilt naturally, and remaps around the entry location
- If the entry is in use and is not safely removable (MAC_NH, IPSA, IPMCD, IPDP, IPSP, IPXSN)—sends a warning message to the log

If the switch detects more than eight questionable entries, it executes the configured failure action and stops remapping on the switch fabric. To see the questionable and remapped entries, use the show fdb command. The following information is displayed:

- Questionable entries are marked with a “Q” flag
- Remapped entries are marked with an “R” flag
- Total FDB count
You can also display FDB scan statistics using the following command:
show diagnostics sys-health-check

**Example**

The following command clears any FDB entries associated with ports 3-5:
clear fdb ports 3-5

The following command clears any FDB entries associated with VLAN corporate:
clear fdb vlan corporate

**On the “i” series of switches.** The following command clears all questionable and remapped entries from the FDB:
clear fdb remap

**History**

This command was available in ExtremeWare 2.0.

The command was modified in ExtremeWare 6.2.1 to support the broadcast-mac keyword and to support clearing locked-static entries.

This command was modified in ExtremeWare 6.2.2b108 to support the remap keyword, and questionable entries (known as suspect entries) are marked with an “S” flag.

The remap keyword was not supported in ExtremeWare 7.0.

The remap keyword is supported in ExtremeWare 7.1.0, and questionable entries are marked with a “Q” flag.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

The command was modified in ExtremeWare 7.2e to support the blackhole keyword.

**Platform Availability**

This command is available on all platforms.
configure fdb agingtime

    configure fdb agingtime <seconds>

Description
Configures the FDB aging time for dynamic entries.

Syntax Description

| seconds | Specifies the aging time in seconds. Range is 15 through 1,000,000. A value of 0 indicates that the entry should never be aged out. |

Default
300 seconds

Usage Guidelines
The range is 15 through 1,000,000 seconds.

If the aging time is set to zero, all aging entries in the database are defined as static, nonaging entries. This means that they do not age out, but non-permanent static entries can be deleted if the switch is reset.

Example
The following command sets the FDB aging time to 3,000 seconds:

```
configure fdb agingtime 3000
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure fdb-scan failure-action

configure fdb-scan failure-action [log | sys-health-check]

Description
Configures the action the switch takes if too many failures are detected within the specified FDB scan period.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Specifies that messages are sent to the syslog.</td>
</tr>
<tr>
<td>sys-health-check</td>
<td>Specifies the configured system health check action is taken.</td>
</tr>
</tbody>
</table>

Default
log

Usage Guidelines
If you use the default log, only one instance of an error message is logged at this level.

If you select sys-health-check, and the switch detects too many failures, the switch takes the configured system health check action. To configure the system health check, use the configure sys-health-check [alarm-level [card-down | default | log | system-down | traps] | auto-recovery <number of tries>] command.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the show switch command. The following is sample FDB scanning output:

Fdb-Scan Diag: Enabled. Failure action: log only

For ExtremeWare 6.2.2b108:

The default is sys-health-check, and the switch takes the configured system health check action.

Example
The following command configures the switch to perform the configured system health check action if too many failures are detected:

configure fdb-scan failure-action sys-health-check

History
This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to log in ExtremeWare 6.2.2b134.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available on the “i” series platform only.
configure fdb-scan period

    configure fdb-scan period <period <1-60>>

Description
Configures the amount of time between FDB scans.

Syntax Description

| period <1-60> | Specifies the timer interval, in seconds, between FDB scans. The range is 1 to 60 seconds. |

Default
30 seconds

Usage Guidelines
If you configure a timer interval of less than 15 seconds, the following warning message is displayed and you are asked to confirm the change:

Setting period below (15) may starve other tasks.
Do you wish to do this? (yes, no, cancel) 06/19/2003 10:29.28 <INFO:SYST> serial admin: configure fdb-scan period 1

Extreme Networks recommends an interval period of at least 15 seconds.
This setting is independent of and does not affect the system health check configurations.

Example
The following command configures a timer interval of 20 seconds between FDB scans:
configure fdb-scan period 20

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available on the “i” series platform only.
create fdbentry secure-mac

    create fdbentry secure-mac <mac_address> vlan <vlan name> ports <port-list>

Description
Specifies an authorized set of ports on which the specified MAC address will be permitted.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a device MAC address, using colon-separated bytes.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name associated with a MAC address.</td>
</tr>
<tr>
<td>port-list</td>
<td>Specifies one or more ports. May be in the form 1, 2, 3-5, 2*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
When secure MAC addresses are learned, they are aged out like other dynamically learned entries.

When a secure MAC address appears on a port/VLAN combination other than the one for which it is configured, it is blackholed.

Configuring a secure MAC address for a port does not prevent the port from learning other MAC addresses.

Example
The following command specifies that MAC address 00:0a:01:02:03:04 is permitted only on ports 1 and 2 in VLAN test:

create fdbentry secure-mac 00:0a:01:02:03:04 vlan test ports 1,2

History
This command was first available in ExtremeWare release 7.0 SR1.

Platform Availability
This command is available on all platforms.
create fdbentry vlan blackhole

create fdbentry <mac_address> vlan <vlan name> blackhole {source-mac | dest-mac | both}

**Description**
Creates a blackhole FDB entry.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a device MAC address, using colon-separated bytes.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name associated with a MAC address.</td>
</tr>
<tr>
<td>blackhole</td>
<td>Configures the MAC address as a blackhole entry.</td>
</tr>
<tr>
<td>source-mac</td>
<td>Specifies that the blackhole MAC address matches the ingress source MAC address. Support for this parameter was added in ExtremeWare 6.2.</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Specifies that the blackhole MAC address matches the egress destination MAC address. Support for this parameter was added in ExtremeWare 6.2.</td>
</tr>
<tr>
<td>both</td>
<td>Specifies that the blackhole MAC address matches the ingress source MAC address or the egress destination MAC address. Support for this parameter was added in ExtremeWare 6.2.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**

Blackhole entries are useful as a security measure or in special circumstances where packets with a specific source or destination address must be discarded.

A blackhole entry configures the switch to discard packets with the specified MAC address. You can specify whether the MAC address should match the source (ingress) MAC address, or the destination (egress) MAC address, or both.

Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged-out of the database. In the output from a `show fdb` command, entries will have “p” flag (permanent) set, as well as the “b” (for ingress blackhole) and/or “B” (for egress blackhole) flags set.

**Example**
The following example adds a blackhole entry to the FDB for MAC address is 00 E0 2B 12 34 56, in VLAN marketing on port 4:

create fdbentry 00:E0:2B:12:34:56 vlan marketing both

**History**
This command was available in ExtremeWare 2.0.

Support for specifying source or destination MAC address was added in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
create fdbentry vlan dynamic

For “i” series switches:

create fdbentry [<mac_address> | broadcast-mac | any-mac] vlan <vlan name> dynamic [qosprofile <qosprofile> {ingress-qosprofile <inqosprofile>} | ingress-qosprofile <inqosprofile> {qosprofile <qosprofile>}]}

For “e” series switches:

create fdbentry [<mac_address> | any-mac] vlan <vlan name> dynamic [ingress-qosprofile <qosprofile> {ingress-qosprofile <inqosprofile>}]}

Description

Creates a permanent dynamic FDB entry, and associates it with an ingress and/or egress QoS profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a device MAC address, using colon separated bytes.</td>
</tr>
<tr>
<td>broadcast-mac</td>
<td>Specifies the broadcast MAC address. May be used as an alternate to the colon-separated byte form of the address ff:ff:ff:ff:ff. NOTE: This option is only available on the “i” series of switches.</td>
</tr>
<tr>
<td>any-mac</td>
<td>Specifies the wildcard, permanent FDB entry used to give higher priority to an 802.1p packet.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name associated with a MAC address.</td>
</tr>
<tr>
<td>dynamic</td>
<td>Specifies that the entry will be learned dynamically.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>QoS profile associated with the destination MAC address of the egress port.</td>
</tr>
<tr>
<td>inqosprofile</td>
<td>QoS profile associated with the source MAC address of the ingress port.</td>
</tr>
</tbody>
</table>

NOTE: This option is only available on the “i” series of switches.

Default

N/A

Usage Guidelines

This command is used to associate QoS profiles with packets received from or destined for the specified MAC address, while still allowing the FDB entry to be dynamically learned.

The FDB entry is not actually created until the MAC address is encountered as the source MAC address in a packet. Thus, initially the entry may not appear in the show fdb output. Once the entry has been learned, it is created as a permanent dynamic entry, designated by “dpm” in the flags field of the show fdb output.

A dynamic entry is flushed and relearned (updated) when any of the following take place:

- A VLAN is deleted.
- A VLAN identifier (VLANid) is changed.
- A port mode is changed (tagged/untagged).
- A port is deleted from a VLAN.
• A port is disabled.
• A port enters blocking state.
• A port QoS setting is changed.
• A port goes down (link down).

Using the any-mac keyword, you can enable traffic from a QoS VLAN to have higher priority than 802.1p traffic. Normally, an 802.1p packet has a higher priority over the VLAN classification. To use this feature, you must create a wildcard permanent FDB entry named any-mac and apply the QoS profile to the individual MAC entry.

You can use the show fdb permanent command to display permanent FDB entries, including their QoS profile associations.

**On the “i” Series of Switches.** If you specify only the ingress QoS profile, the egress QoS profile defaults to none, and vice-versa. If both profiles are specified, the source MAC address of an ingress packet and the destination MAC address of an egress packet are examined for QoS profile assignment.

**Example**

The following example associates the QoS profile qp2 with a dynamic entry for MAC address 00:A0:23:12:34:56 on VLAN net34 that will be learned by the FDB:

```markdown
create fdbentry 00:A0:23:12:34:56 vlan net34 dynamic qosprofile qp2
```

QoS profile qp2 will be applied when the entry is learned.

The following example associates the QoS profile qp5 with the wildcard permanent FDB entry any-mac on VLAN v110:

```markdown
create fdbentry any-mac vlan v110 dynamic ingress-qosprofile qp5
```

**History**

This command was available in ExtremeWare 2.0.

Support for associating separate QoS profiles with ingress and egress ports was added in ExtremeWare 6.2.

This command was modified in ExtremeWare 6.2.1 to support the broadcast-mac option.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the any-mac option.

**Platform Availability**

This command is available on all platforms.
create fdbentry vlan ports

create fdbentry <mac_address> vlan <vlan name> ports [portlist | all] {qosprofile <qosprofile>} {ingress-qosprofile <inqosprofile>}

Description
Creates a permanent static FDB entry, and optionally associates it with an ingress and/or egress QoS profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a device MAC address, using colon-separated bytes.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name associated with a MAC address.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports associated with the MAC address. May be in the</td>
</tr>
<tr>
<td></td>
<td>form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>QoS profile associated with the destination MAC address of the egress port</td>
</tr>
<tr>
<td>inqosprofile</td>
<td>QoS profile associated with the source MAC address of the ingress port.</td>
</tr>
</tbody>
</table>

The parameter was added in ExtremeWare 6.2.

Default
N/A

Usage Guidelines

If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.

Permanent entries are retained in the database if the switch is reset or a power off/on cycle occurs. A permanent static entry can either be a unicast or multicast MAC address. The stand-alone switches can support a maximum of 64 permanent entries, and the modular switches support a maximum of 254 permanent entries.

After they have been created, permanent static entries stay the same as when they were created. If the same MAC address is encountered on another virtual port that is not included in the permanent MAC entry, it is handled as a blackhole entry. The static entry is not updated when any of the following take place:

- A VLAN is deleted.
- A VLAN identifier (VLANid) is changed.
- A port mode is changed (tagged/untagged).
- A port is deleted from a VLAN.
- A port is disabled.
- A port enters blocking state.
- A port QoS setting is changed.
- A port goes down (link down).
Permanent static entries are designated by “spm” in the flags field of the show fdb output. You can use the show fdb permanent command to display permanent FDB entries, including their QoS profile associations.

**Example**

The following example adds a permanent, static entry to the FDB for MAC address is 00 E0 2B 12 34 56, in VLAN *marketing* on port 4:

create fdbentry 00:E0:2B:12:34:56 vlan marketing port 4

**History**

This command was available in ExtremeWare 2.0.

Support for associating separate QoS profiles with ingress and egress ports was added in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
delete fdbentry

delete fdbentry [[<mac_address> | broadcast-mac] vlan <vlan name> | all]

Description
Deletes one or all permanent FDB entries.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a device MAC address, using colon-separated bytes.</td>
</tr>
<tr>
<td>broadcast-mac</td>
<td>Specifies the broadcast MAC address. May be used as an alternate to the colon-separated byte form of the address ff:ff:ff:ff:ff:ff.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all FDB entries should be deleted.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following example deletes a permanent entry from the FDB:
delete fdbentry 00:E0:2B:12:34:56 vlan marketing

The following example deletes all permanent entry from the FDB:
delete fdbentry all

History
This command was available in ExtremeWare 2.0.
This command was modified in ExtremeWare 6.2.0 to support the all option.
This command was modified in ExtremeWare 6.2.1 to support the broadcast-mac option.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2.e to support the broadcast-mac option.

Platform Availability
This command is available on all platforms.
disable fdb-scan

    disable fdb-scan [all | slot {{backplane} | <slot number> | msm-a | msm-b}]

Description
Disables FDB scanning on a stand-alone switch or on a per slot or backplane basis on a modular switch.

Syntax Description

- **all**: Specifies all of the slots in the chassis.
  - NOTE: This is available on modular switches only.
- **backplane**: Specifies the backplane of the chassis.
  - NOTE: This is available on Alpine switches only.
- **slot number**: Specifies the slot number of the module to scan.
  - NOTE: This is available on BlackDiamond switches only.
- **msm-a**: Specifies the MSM in slot A.
  - NOTE: This is available on BlackDiamond switches only
- **msm-b**: Specifies the MSM in slot B
  - NOTE: This is available on BlackDiamond switches only

Default
Disabled

Usage Guidelines
This setting is independent of and does not affect the system health check configurations. (Health check is only available on “i” series of switches.)

To determine if you have FDB scanning enabled and the failure action the switch takes, use the `show switch` command. The following is sample FDB scanning output:

Fdb-Scan Diag: Enabled. Failure action: log only

For ExtremeWare 6.2.2b108:

The default for the FDB scan is enabled.

**For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:** The default for the FDB scan is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, FDB scanning is enabled. You must manually disable FDB scanning if you want the feature disabled.

Example
The following command disables FDB scanning on a stand-alone switch:

disable fdb-scan
The following command disables FDB scanning on all of the slots of a modular switch:

```
disable fdb-scan all
```

**History**

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available on the “i” series platform and the BlackDiamond modules.
enable fdb-scan

enable fdb-scan [all | slot {{backplane} | <slot number> | msm-a | msm-b}]

**Description**
Enables FDB scanning on a stand-alone switch or on a per slot or backplane basis on a modular switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all of the slots in the chassis.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available on modular switches only.</td>
</tr>
<tr>
<td>backplane</td>
<td>Specifies the backplane of the chassis.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available on Alpine switches only.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot number of the module to scan.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available on BlackDiamond switches only.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies the MSM in slot A.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available on BlackDiamond switches only</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies the MSM in slot B.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available on BlackDiamond switches only</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Guidelines**
In addition to the system health checker, you can scan the FDB on a stand-alone switch, or on a per slot or backplane basis on a modular switch. This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the `show switch` command. The following is sample FDB scanning output:

```
Fdb-Scan Diag: Enabled. Failure action: log only
```

For ExtremeWare 6.2.2b108:

The default for the FDB scan is enabled.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the FDB scan is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, FDB scanning is enabled. You must manually disable FDB scanning if you want the feature disabled.

**Example**
The following command enables FDB scanning on a stand-alone switch:

```
enable fdb-scan
```
The following command enables FDB scanning on all of the slots of a modular switch:

```
enable fdb-scan all
```

**History**

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available on the “i” series platform and the BlackDiamond modules.
run fdb-check

    run fdb-check [index <bucket> <entry> | [<mac_address> | broadcast-mac] <vlan name>]} {extended} {detail}

Description
Checks MAC FDB entries for consistency.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket</td>
<td>Specifies the bucket portion of the FDB hash index.</td>
</tr>
<tr>
<td>entry</td>
<td>Specifies the entry portion of the FDB hash index.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies a MAC address (hex octet). FDB entries with this MAC address will be checked.</td>
</tr>
<tr>
<td>broadcast-mac</td>
<td>Specifies the broadcast MAC address. May be used as an alternate to the hex octet form, ff:ff:ff:ff:ff. (6.2.1 and higher)</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name. FDB entries for this VLAN with the specified MAC address will be checked.</td>
</tr>
<tr>
<td>extended</td>
<td>Enables OTP index checking in the MAC entry and VPST of the egress port.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that more detailed debug information should be logged.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The FDB error checking function logs the error count into the system log. Use the detail option to log more detailed debug information.

If you do not enter a VLAN name, ExtremeWare check all FDB entries with the specified MAC address.

Example

Given the following FDB entry on an MSM 64:

<table>
<thead>
<tr>
<th>Index</th>
<th>Mac</th>
<th>Vlan</th>
<th>Age</th>
<th>Use</th>
<th>Flags</th>
<th>Port</th>
<th>List</th>
</tr>
</thead>
<tbody>
<tr>
<td>cf3c0-006</td>
<td>00:00:00:00:00:01</td>
<td>v1(4093)</td>
<td>0540</td>
<td>0000</td>
<td>d m</td>
<td>3:4</td>
<td></td>
</tr>
</tbody>
</table>

All the following commands will do consistency checking on this entry:

- run fdb-check 00:00:00:00:00:01
- run fdb-check 00:00:00:00:00:01 detail
- run fdb-check 00:00:00:00:00:01 extended detail
- run fdb-check 00:00:00:00:00:01 vlan v1
- run fdb-check index cf3c 0 extended detail

History
This command was first available in ExtremeWare 6.1.9
This command was modified in ExtremeWare 6.2.1 to support the \texttt{broadcast-mac} keyword.

\textbf{Platform Availability}

This command is available on the \textquote{“i”} series platform.

The \textit{extended} option is available on the Black Diamond 6800 chassis-based system only.
show fdb

On “i” series of switches:

    show fdb {<mac_address> | broadcast-mac | permanent | ports <portlist> | remap | vlan <vlan name>}

On “e” series of switches:

    show fdb {<mac_address> | permanent | ports <portlist> | vlan <vlan name>}

Description
Displays FDB entries.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address, using colon-separated bytes, for which FDB entries should be displayed.</td>
</tr>
<tr>
<td>broadcast-mac</td>
<td>Specifies the broadcast MAC address. May be used as an alternate to the colon-separated byte form of the address ff:ff:ff:ff:ff:ff.</td>
</tr>
<tr>
<td>permanent</td>
<td>Displays all permanent entries, including the ingress and egress QoS profiles and secure MAC addresses.</td>
</tr>
<tr>
<td>portlist</td>
<td>Displays the entries for one or more ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>remap</td>
<td>Displays the remapped FDB entries.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Displays the entries for a specific VLAN.</td>
</tr>
</tbody>
</table>

Default
All

Usage Guidelines
Displays FDB entries as specified, or displays all FDB entries.

The show output displays the following information:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EQP</td>
<td>The Ingress QoS profile assigned to the entry (appears only if the keyword permanent is specified).</td>
</tr>
<tr>
<td>IQP</td>
<td>The Egress QoS profile assigned to the entry (appears only if the keyword permanent is specified).</td>
</tr>
<tr>
<td>Index</td>
<td>The FDB hash index, in the format &lt;bucket&gt;-&lt;entry&gt;.</td>
</tr>
<tr>
<td>Mac</td>
<td>The MAC address that defines the entry.</td>
</tr>
<tr>
<td>Vlan</td>
<td>The VLAN for the entry.</td>
</tr>
<tr>
<td>Age</td>
<td>The age of the entry, in seconds (does not appear if the keyword permanent is specified).</td>
</tr>
<tr>
<td>Use</td>
<td>The number of IP FDB entries that use this MAC address as a next hop or last hop (does not appear if the keyword permanent is specified).</td>
</tr>
</tbody>
</table>
Example

The following command displays information about all the entries in the FDB:

```
show fdb
```

It produces output similar to the following:

<table>
<thead>
<tr>
<th>Index</th>
<th>Mac</th>
<th>Vlan</th>
<th>Age</th>
<th>Use</th>
<th>Flags</th>
<th>Port List</th>
</tr>
</thead>
<tbody>
<tr>
<td>0a0e0-100</td>
<td>00:01:30:EC:D3:00</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0001</td>
<td>d i</td>
<td>1</td>
</tr>
<tr>
<td>2b560-ff0</td>
<td>01:00:0C:CC:CC:CD</td>
<td>(0000)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>30040-ff0</td>
<td>00:E0:2B:00:00:00</td>
<td>zzz(0652)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>332890-ff0</td>
<td>00:E0:2B:00:00:00</td>
<td>Default(0001)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>3d760-ff0</td>
<td>00:E0:2B:00:00:00</td>
<td>Mgmt(4094)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>3d770-ff0</td>
<td>00:E0:2B:00:00:00</td>
<td>MacVlanDis(4095)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>42560-ff0</td>
<td>00:01:30:6C:0D:00</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>46460-100</td>
<td>00:10:E3:1D:00:1E</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0001</td>
<td>d i</td>
<td>1</td>
</tr>
<tr>
<td>4d060-100</td>
<td>00:10:E3:1D:00:05</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0001</td>
<td>d i</td>
<td>1</td>
</tr>
<tr>
<td>4df0-ff0</td>
<td>00:01:30:6C:0D:00</td>
<td>Default(0001)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>4f7a0-ff0</td>
<td>00:01:30:6C:0D:00</td>
<td>zzz(0652)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>51f50-100</td>
<td>00:01:30:CA:F6:00</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0001</td>
<td>d i</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>67b20-100</td>
<td>00:30:D3:01:5A:E0</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0001</td>
<td>d i</td>
<td>1</td>
</tr>
<tr>
<td>80a10-204</td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU, 2, 1</td>
</tr>
<tr>
<td>80f0-208</td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>MacVlanDis(4095)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>80ff-202</td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Mgmt(4094)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>8d8d-20a</td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>zzz(0652)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>8f000-200</td>
<td>FF:FF:FF:FF:FF:FF</td>
<td>Default(0001)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
<tr>
<td>98670-100</td>
<td>00:01:30:1E:1E:00</td>
<td>lab(4000)</td>
<td>0000</td>
<td>0001</td>
<td>d i</td>
<td>1</td>
</tr>
<tr>
<td>fcf70-202</td>
<td>00:E0:2B:00:00:02</td>
<td>Mgmt(4094)</td>
<td>0000</td>
<td>0000</td>
<td>s m</td>
<td>CPU</td>
</tr>
</tbody>
</table>

Flags: (B) Egress Blackhole, (b) Ingress Blackhole, (d) Dynamic, (s) Static (p) Permanent, (m) MAC, (S) secure MAC, (l) lockdown MAC, (M) Mirror (i) IP, (x) IPX, (z) translation MAC, (Q) Questionable, (R) Remapped
FDB Commands

Total: 33 Static: 16 Perm: 0 Locked: 0 Secure: 0 Dynamic: 17 Dropped: 0
Questionable: 0 Remapped: 0
FDB Aging time: 300 seconds

**NOTE**

IPX information only shows in "i" series switch output.

The following command displays information about the permanent entries in the FDB:

```
show fdb permanent
```

It produces output similar to the following:

```
QP IQP Index   Mac               Vlan   Flags Port List
--------------------------------------------------------------------------------
QP3 QP2 ----- --- 00:10:E3:1D:00:05   anntest1(4094) pm     ---
QP3 QP2 4e610-206 00:01:03:2F:38:EE   anntest1(4094) spm     ---
QP3 QP2 ----- --- 00:60:B0:F9:58:9D    Default(0001) pm     ---
```

Flags: (B) Egress Blackhole, (b) Ingress Blackhole, (d) Dynamic, (s) Static
(p) Permanent, (m) MAC, (S) secure MAC, (l) lockdown MAC, (M) Mirror
(i) IP, (x) IPX, (z) translation MAC, (Q) Questionable, (R) Remapped
[ ] : authorize port list

Total: 3 Secure: 0

**NOTE**

IPX information only shows in "i" series switch output.

**History**

This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.1 to support the `broadcast-mac` option.

This command was modified in ExtremeWare 6.2.2b108 to support the `remap` option.

The `remap` option was not supported in ExtremeWare 7.0.

This `remap` option is supported in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
unconfigure fdb-scan failure-action

Description
Returns the switch to its default of sending FDB scan messages to the syslog if too many failures are detected within the specified scan period.

Syntax Description
The command has no arguments or variables.

Default
N/A

Usage Guidelines
This setting is independent of and does not affect the system health check configurations.

To determine if you have FDB scanning enabled and the failure action the switch takes, use the show switch command.

For ExtremeWare 6.2.2b108:

The failure action default is sys-health-check. If you use the unconfigure fdb-scan failure-action command, the switch returns to its default of performing the configured system health check action.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The failure action default is log. If you use the unconfigure fdb-scan failure-action command, the switch sends one instance of an error message to the syslog.

Example
The following command returns the switch to its default of sending one instance of an error message to the syslog:

unconfigure fdb-scan failure-action

History
This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available on the “i” series platform only.
unconfigure fdb-scan period

unconfigure fdb-scan period

Description
Returns the FDB scan interval to the factory default of 30 seconds.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This setting is independent of and does not affect the system health check configurations.

Example
The following command returns the FDB scan interval to 30 seconds:
unconfigure fdb-scan period

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available on the “i” series platform only.
This chapter describes the following commands:

- Commands for configuring Quality of Service (QoS) profiles
- Commands creating traffic groupings and assigning the groups to QoS profiles
- Commands for configuring, enabling and disabling explicit class-of-service traffic groupings (802.1p and DiffServ)
- Commands for configuring, enabling and disabling Random Early Detection (RED) (supported only on “i” series switches)
- Commands for configuring traffic grouping priorities
- Commands for verifying configuration and performance
- Commands for enabling and disabling the Dynamic Link Context System (DLCS) (supported only on “i” series switches)

This chapter does not describe the additional ingress and egress QoS capabilities available on the High Density Gigabit Ethernet “3” series I/O modules for “i” series switches. For more information and a full description of the “3” series I/O module command set, see Chapter 30.

QoS is a feature of ExtremeWare that allows you to specify different service levels for outbound and inbound traffic. QoS is an effective control mechanism for networks that have heterogeneous traffic patterns. Using QoS, you can specify the service that a traffic type receives.

Policy-based QoS allows you to protect bandwidth for important categories of applications or specifically limit the bandwidth associated with less critical traffic. The switch contains separate hardware queues on every physical port. Each hardware queue is programmed by ExtremeWare with bandwidth management and priority parameters, defined as a QoS profile. The bandwidth management and priority parameters that modify the forwarding behavior of the switch affect how the switch transmits traffic for a given hardware queue on a physical port. Up to eight physical queues per port are available.

Policy-based QoS can be configured on the “i” series switches to perform per-port Random Early Detection (RED). Using this capability, the switch detects when traffic is filling up in any of the eight hardware queues, and performs a random discard on subsequent packets, based on the configured RED drop-probability. Instead of dropping sessions during times when the queue depth is exceeded, RED causes the switch to lower session throughput.
To configure QoS, you define how your switch responds to different categories of traffic by creating and configuring QoS profiles. The service that a particular type of traffic receives is determined by assigning a QoS profile to a traffic grouping or classification. The building blocks are defined as follows:

- **QoS profile**—Defines bandwidth and priority parameters.
- **Traffic grouping**—A method of classifying or grouping traffic that has one or more attributes in common.
- **QoS policy**—The combination that results from assigning a QoS profile to a traffic grouping.

QoS profiles are assigned to traffic groupings to modify switch forwarding behavior. The combination of the traffic grouping and the assigned QoS profile makes an example of a single policy that is part of policy-based QoS.

Extreme switch products support explicit Class of Service traffic groupings. This category of traffic groupings describes what is sometimes called *explicit packet marking*, and includes:

- IP DiffServ code points, formerly known as IP TOS bits
- Priority bits used in IEEE 802.1p packets

All Extreme switches support the standard 802.1p priority bits that are part of a tagged Ethernet packet.

**DLCS—“i” Series Switches Only**

The Dynamic Link Context System (DLCS) is a feature of ExtremeWare and Extreme “i” series switches that snoops Windows Internet Naming Service (WINS) NetBIOS packets and creates a mapping between a user name, the IP address or MAC address of the workstation, and a port on the switch. Based on the information in the packet, DLCS can detect when an workstation boots up or a user logs in or out, and dynamically maps the user or workstation name to the current IP address and switch port. For DLCS to operate within ExtremeWare, the user or workstation must allow automatic DLCS updates.

Information obtained through DLCS is used by the EPICenter Policy Manager software, and enables the configuration of policies that apply to named users or workstations. Enabling the DLCS feature is useful only if you plan to use the EPICenter software. Currently, there are no other features that can make use of the information that the DLCS feature provides.

The DLCS feature is supported only on the “i” series switches.
clear dlcs

Description
Clears all learned DLCS data.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
If the IP address of an end-station changes, and the end-station is not immediately rebooted, the old host-to-IP mapping is not deleted. You must delete the mapping through the ExtremeWare Enterprise Manager Policy System.

Example
The following command clears all learned DLCS data from the switch:
clear dlcs

History
This command was available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
configure diffserv examination code-point qosprofile ports

configure diffserv examination code-point <code_point> qosprofile
<qosprofile> ports [<portlist> | all] {low-drop-probability | high-drop-probability}

Description
Configures the default mapping of ingress DiffServ code points (DSCP) to QoS profiles.

NOTE
This command is available only on the “i” series switches.

Syntax Description

code_point
  Specifies a DiffServ code point (a 6-bit value in the IP-TOS byte in the IP header).

qosprofile
  Specifies the QoS profile to which the DiffServ code point is mapped.

portlist
  Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.

all
  Specifies that this applies to all ports on the device.

low-drop-probability
  Specifies that the DSCP has a low drop-probability level.
  NOTE: This option is supported only for SONET ports on a PoS module.

high-drop-probability
  Specifies that the DSCP has a high drop-probability level.
  NOTE: This option is supported only for SONET ports on a PoS module.

Default
See Table 10.

Usage Guidelines
You can specify up to 64 different code points for each port. Code point values are grouped and
assigned to the default QoS profiles as listed in Table 10. The mapping is applied in the ingress
direction.

Table 10: Default Code Point-to-QoS Profile Mapping

<table>
<thead>
<tr>
<th>Code Point</th>
<th>QoS Profile for “i” Series and Summit 400</th>
<th>QoS Profile for Summit 200 and Summit 300</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>Qp1</td>
<td>Qp1</td>
</tr>
<tr>
<td>8-15</td>
<td>Qp2</td>
<td></td>
</tr>
<tr>
<td>16-23</td>
<td>Qp3</td>
<td>Qp2</td>
</tr>
<tr>
<td>24-31</td>
<td>Qp4</td>
<td></td>
</tr>
<tr>
<td>32-39</td>
<td>Qp5</td>
<td>Qp3</td>
</tr>
<tr>
<td>40-47</td>
<td>Qp6</td>
<td></td>
</tr>
<tr>
<td>48-55</td>
<td>Qp7</td>
<td>Qp4</td>
</tr>
<tr>
<td>56-63</td>
<td>Qp8</td>
<td></td>
</tr>
</tbody>
</table>
For the BlackDiamond Switches. The low-drop-probability and high-drop-probability keywords are applicable only to SONET ports. The low-drop-probability and high-drop-probability keywords are useful in conjunction with the weighted RED (WRED) implementation provided by SONET ports. This implementation supports two different drop probabilities; one for DSCPs designated as having low drop-probability and another for DSCPs designated as having high drop-probability. These keywords enable complete flexibility in assigning DSCPs to the two different drop-probability levels.

Examples

The following command specifies that packets arriving on ports 5-8 that use code point 25 be assigned to qp2:

```
configure diffserv examination code-point 25 qosprofile qp2 ports 5-8
```

The following command sets up the mapping for the EF PHB (PoS module only):

```
configure diffserv examination code-point 46 qosprofile qp8 ports 2:1-2:2
```

History

This command was first available in ExtremeWare 6.0.

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

Platform Availability

This command is available on “i” series platforms. The PoS module extensions are supported on the BlackDiamond switch only.
configure diffserv replacement priority code-point ports

configure diffserv replacement priority <value> code-point <code_point>
ports [<portlist> | all]

Description
Configures the default egress DiffServ replacement mapping.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Specifies the 802.1p priority value.</td>
</tr>
<tr>
<td>code_point</td>
<td>Specifies a 6-bit value to be used as the replacement code point in the IP-TOS byte in the IP header.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of egress ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
To replace DiffServ code points you must enable both 802.1p replacement and DiffServ replacement using the enable dot1p replacement ports and enable diffserv replacement ports commands.

The default 802.1p priority value to code point mappings are described in Table 11.

Table 11: Default 802.1p Priority Value-to-Code Point Mapping

<table>
<thead>
<tr>
<th>Hardware Queue</th>
<th>802.1p Priority value</th>
<th>Code Point</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Q1</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>Q2</td>
<td>2</td>
<td>16</td>
</tr>
<tr>
<td>Q3</td>
<td>3</td>
<td>24</td>
</tr>
<tr>
<td>Q4</td>
<td>4</td>
<td>32</td>
</tr>
<tr>
<td>Q5</td>
<td>5</td>
<td>40</td>
</tr>
<tr>
<td>Q6</td>
<td>6</td>
<td>48</td>
</tr>
<tr>
<td>Q7</td>
<td>7</td>
<td>56</td>
</tr>
</tbody>
</table>
Example
The following command specifies that a code point value of 25 should be used to replace the TOS bits in packets with an 802.1p priority of 2 for ports 5-9:

configure diffserv replacement priority 2 code-point 25 ports 5-9

History
This command was first available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
configure dot1p type

    configure dot1p type <dot1p_priority> qosprofile <qosprofile>

Description
Configures the default QoS profile to 802.1p priority mapping.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1p_priority</td>
<td>Specifies the 802.1p priority value. The value is an integer between 0 and 7.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies a QoS profile.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
An 802.1p priority value seen on ingress can be mapped to a particular QoS profile and with specific bandwidth management and priority behavior.

The default mapping of each 802.1p priority value to QoS profile is described in Table 12.

Table 12: 802.1p Priority Value-to-QoS Profile Default Mapping

<table>
<thead>
<tr>
<th>Priority Value</th>
<th>QoS Profile Summit Chipset</th>
<th>QoS Profile “i” Chipset</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Qp1</td>
<td>Qp1</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>Qp2</td>
</tr>
<tr>
<td>2</td>
<td>Qp2</td>
<td>Qp3</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Qp4</td>
</tr>
<tr>
<td>4</td>
<td>Qp3</td>
<td>Qp5</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Qp6</td>
</tr>
<tr>
<td>6</td>
<td>Qp4</td>
<td>Qp7</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>Qp8</td>
</tr>
</tbody>
</table>

Example
The following commands swap the QoS profiles associated with 802.1p priority values 1 and 2 on an “i” series device:

configure dot1p type 2 qosprofile qp2
configure dot1p type 1 qosprofile qp3

History
This command was available in ExtremeWare 6.0.
Platform Availability

This command is available on the “i” series platforms only.
configure ports qosprofile

configure ports <portlist> qosprofile <qosprofile>

Description
Configures one or more ports to use a particular QoS profile.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>qosprofile</td>
<td>Specifies a QoS profile.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Extreme switches support eight QoS profiles (QP1 - QP8).

Example
The following command configures port 5 to use QoS profile QP3:
configure ports 5 qosprofile QP3

History
This command was first available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
configure qosprofile

configure qosprofile <qosprofile> minbw <min_percent> maxbw <max_percent>
priority <level> {[minbuf <percent> maxbuf <number> [K | M] | maxbuff
<number> [K | M] | <portlist>]}

Description
Modifies the default QoS profile parameters.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>qosprofile</th>
<th>Specifies a QoS profile name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>min_percent</td>
<td>Specifies a minimum bandwidth percentage for this queue. The default setting is 0.</td>
</tr>
<tr>
<td>max_percent</td>
<td>Specifies the maximum bandwidth percentage this queue is permitted to use. The default setting is 100.</td>
</tr>
<tr>
<td>level</td>
<td>Specifies a service priority setting. Settings include low, lowHi, normal, normalHi, medium, mediumHi, high, and highHi. The default setting is low. Available in egress mode only.</td>
</tr>
<tr>
<td>percent</td>
<td>Specifies the minimum percentage of the buffer set aside for the queue. Cumulative percentage of the queues should not exceed 100.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the maximum buffer size in either M or K bytes. The range is 0 to 16384. The default is 256 K. You must reboot for changes to take effect.</td>
</tr>
</tbody>
</table>
  * K indicates the value is in K bytes. |
  * M indicates the value is in M bytes. |
| portlist | Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default

- Minimum bandwidth—0%
- Maximum bandwidth—100%
- Priority—low
- Minimum buffer percent—0%
- Maximum buffer size—256K

Usage Guidelines

In ingress mode, any changes to parameters of the four predefined QoS profiles have the corresponding effect on the ports to which they are mapped.

The minbuf parameter reserves buffer memory for use exclusively by a QoS profile across all affected ports. The default value for buffer settings is 0%. The sum of all QoS profile buffer parameters should not exceed 100%. The maxbuf parameter allows you to set a maximum buffer for each queue, so that a single queue will not consume all of the unallocated buffer space. You should not modify the buffer...
parameter unless specific situations and application behavior indicate. You must reboot the switch for changes to this parameter to take effect.

For ExtremeWare 4.0:
- Only four priority levels are available (low, normal, medium, and high).

**Examples**

The following command configures the QoS profile parameters of QoS profile qp5 for specific ports on an “i” series switch:

```
configure qosprofile qp5 minbw 10% maxbw 80% priority highHi ports 5-7
```

The following command configures the buffer size for QoS profile qp5 on an “i” series switch:

```
configure qosprofile qp5 minbw 10% maxbw 80% priority highHi minbuf 3% maxbuf 1024K
```

**History**

This command was available in ExtremeWare 2.0.

The minbuff, maxbuff, and ports arguments were available in ExtremeWare 6.0.

**Platform Availability**

This command is available on the “i” series platforms only.
configure qostype priority

configure qostype priority [source-mac | dest-mac | access-list | vlan | diffserv | dot1p] <priority>

Description

Configures the priority of the specified QoS traffic grouping.

NOTE

This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source-mac</td>
<td>Specifies the priority of traffic groupings based on FDB source MAC addresses. Default is 7.</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Specifies the priority of traffic groupings based on FDB destination MAC addresses. Default is 8.</td>
</tr>
<tr>
<td>access-list</td>
<td>Specifies the priority of access-list based traffic groupings. Default is 11.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies the priority of VLAN-based traffic groupings. Default is 1.</td>
</tr>
<tr>
<td>diffserv</td>
<td>Specifies the priority of traffic groupings based on DiffServ information. Default is 3.</td>
</tr>
<tr>
<td>dot1p</td>
<td>Specifies the priority of traffic groupings based on dot1p information. Default is 2.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a priority value in the range of 0-15.</td>
</tr>
</tbody>
</table>

Default

access-list = 11
dest-mac = 8
source-mac = 7
ddiffserv = 3
dot1p = 2
vlan = 1

Usage Guidelines

QoS types with a greater value take higher precedence.

Port-based QoS traffic groupings are always the lowest priority. The priority of port-based traffic cannot be changed.

Example

The following command forces FDB source-mac QoS to take a higher precedence over FDB dest-mac QoS (with a default priority of 8):

configure qostype priority source-mac 9

History

This command was first available in ExtremeWare 6.2.
Platform Availability

This command is available on the “i” series platforms only.
configure red drop-probability

    configure red drop-probability <percent>

Description
Configures the random early detect (RED) drop probability.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>percent</td>
<td>Specifies the RED drop probability as a percentage. Range is 0 - 100.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
When the switch detects that traffic is filling up any of the eight hardware queues, it performs a random discard on subsequent packets, based on the configured RED drop probability. The destination node detects the dropped packet and, using standard TCP windowing mechanisms, slows the transmission from the source node. RED drop probability is configured on a system-wide basis. The percentage range is 0 - 100%.

Example
The following command configures the RED drop-probability as 80%:

    configure red drop-probability 80

History
This command was first available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
configure vlan priority

    configure vlan <vlan name> priority <priority>

Description
Configures the 802.1p priority value for traffic generated on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the 802.1p priority value. The value is an integer between 0 and 7.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The 802.1p priority field is placed in the 802.1Q tag when a packet is generated by the switch. The switch CPU generates traffic, for example, when ping packets are sent out by a user on the switch console.

To configure which queue to use for traffic traveling across a VLAN, use the following command:

custom configure vlan <vlan name> qosprofile <qosprofile>

Example
The following command configures VLAN accounting to use priority 6 in its generated traffic:

configure vlan accounting priority 6

History
This command was available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure vlan qosprofile

    configure vlan <vlan name> qosprofile <qosprofile>

Description
Configures a VLAN to use a particular QoS profile.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies a QoS profile.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Extreme switches support eight QoS profiles (QP1 - QP8).

Example
The following command configures the VLAN called accounting to use QoS profile QP3:

    configure vlan accounting qosprofile QP3

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on the “i” series platforms only.
disable diffserv examination ports

disable diffserv examination ports [<portlist> | all]

Description
Disables the examination of the DiffServ field in an IP packet.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that DiffServ examination should be disabled for all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command disables DiffServ examination on selected ports:

disable diffserv examination ports 3,5,6

History
This command was available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable diffserv replacement ports

disable diffserv replacement ports [<portlist> | all]

Description
Disables the replacement of diffserv code points in packets transmitted by the switch.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that DiffServ replacement should be disabled for all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command disables DiffServ replacement on selected ports:

disable diffserv replacement ports 3,5,6

History
This command was available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
disable dlcs

disable dlcs {fast-ethernet-ports | ports [all | <port_number>]}

Description
This command disables Windows internet Naming Service (WINS) snooping for ports on this switch.

**NOTE**
*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast-ethernet-ports</td>
<td>Specifies that WINS packet snooping should be disabled on all Fast Ethernet ports.</td>
</tr>
<tr>
<td>all</td>
<td>All specifies that WINS packet snooping should be disabled on all ports.</td>
</tr>
<tr>
<td>port_number</td>
<td>Specifies a port on which WINS packet snooping should be disabled.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Guidelines**
Disabling DLCS means that DLCS information for this switch will no longer be available to the ExtremeWare Enterprise Manager Policy System.

Used with no parameters, this command disables WINS packet snooping on all ports on which it was enabled.

If the command is executed with no parameters the DLCS is disabled only on the system, but not on all ports. The ports are still dlcs enabled until they are specifically disabled by the `disable dlcs ports all` or `disable dlcs ports <port_number>` command.

Using the `ports` parameter disables WINS packet snooping only on the specified port.

**Example**
The following command disables all WINS packet snooping on the switch:

disable dlcs

**History**
This command was available in ExtremeWare 6.0.

The command was modified in ExtremeWare 6.1 to support the `fast-ethernet-ports` parameter.

**Platform Availability**
This command is available on the “i” series platforms only.
**disable dot1p replacement ports**

disable dot1p replacement ports [<portlist> | all]

**Description**

Disables the ability to overwrite 802.1p priority values for a given set of ports.

**NOTE**

This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that 892.1p replacement should be disabled for all ports.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

None

**Example**

The following command disables DiffServ replacement on all ports:

disable dot1p replacement ports all

**History**

This command was available in ExtremeWare 6.0.

**Platform Availability**

This command is available on the “i” series platforms only.
**disable qosmonitor**

    disable qosmonitor

**Description**
Disables the QoS monitoring capability.

**NOTE**
This command is available only on the “i” series switches.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled

**Usage Guidelines**
The QoS monitor is a utility on “i” series switches that monitors the eight hardware queues (QP1-QP8) associated with any port(s). The QoS monitor keeps track of the number of frames and the frames per second that a specific queue is responsible for transmitting on a physical port. By default, QoS monitor is disabled on the switch.

**Example**
The following command disables QoS monitoring:

disable qosmonitor

**History**
This command was available in ExtremeWare 4.0.

**Platform Availability**
This command is available on the “i” series platforms only.
disable red ports

    disable red ports <portlist>

Description
Disables random early detection (RED) on the specified ports.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the port number(s). May be in the form 1, 2, 3-5, 2:5, 2:6:2:8.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
None

Example
The following command disables RED on ports 5-7:

disable red ports 5-7

History
This command was first available in ExtremeWare 6.0.10.

Platform Availability
This command is available on the “i” series platforms only.
enable diffserv examination ports

```
enable diffserv examination ports [<portlist> | all]
```

**Description**
Enables examination of the DiffServ field of an ingress IP packet in order to select a QoS profile.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that DiffServ examination should be enabled for all ports.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Guidelines**
None

**Example**
The following command enables DiffServ examination on selected ports:
```
enable diffserv examination ports 3,5,6
```

**History**
This command was available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable diffserv replacement ports

   enable diffserv replacement ports [<portlist> | all]

Description
Enables the DiffServ code point to be overwritten in packets transmitted by the switch.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that DiffServ replacement should be enabled for all ports.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Eight user-defined code points can be configured on each port. The 802.1P priority bits (3-bits) are used to select one of the eight code points.

Example
The following command enables DiffServ replacement on selected ports:

   enable diffserv replacement ports 3,5,6

History
This command was available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
enable dlcs

   enable dlcs (fast-etherenable dlcs net-ports | ports [all | <port_number>])

Description
This command enables Windows Internet Naming Service (WINS) snooping for ports on the switch.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>fast-ethernet-ports</td>
<td>Specifies that WINS packets should be snooped on all Fast Ethernet ports.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that WINS packets should be snooped on all ports.</td>
</tr>
<tr>
<td>port_number</td>
<td>Specifies a port on which WINS packets are to be snooped.</td>
</tr>
</tbody>
</table>

Default
Enables snooping on all ports.

Usage Guidelines
DLCS must be enabled to allow usage of DLCS information by the ExtremeWare Enterprise Manager Policy System.

enable dlcs is used to enable DLCS on the system, and enable dlcs ports all is used to enable DLCS on all ports. For DLCS to work properly both commands need to be executed. See PD3-26670001 for more details.

The fast-ethernet-ports parameter is a shortcut to enable DLCS on all Fast Ethernet ports, rather than having to enter each port individually.

Example
The following command enables DLCS snooping on port 4:

   enable dlcs ports 4

Use the following commands to enable DLCS snooping on the system and on all ports:

   enable dlcs
   enable dlcs ports all

History
This command was available in ExtremeWare 6.0.

The command was modified in ExtremeWare 6.1 to support the fast-ethernet-ports parameter.
Platform Availability

This command is available on the “i” series platforms only.
enable dot1p replacement ports

    enable dot1p replacement ports [<portlist> | all]

**Description**

Allows the 802.1p priority field to be overwritten on egress according to the QoS profile-to-802.1p priority mapping for a given set of ports.

**NOTE**

*This command is available only on the “i” series switches.*

**Syntax Description**

| portlist   | Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |
| all        | Specifies that dot1p replacement should be enabled for all ports. |

**Default**

Disabled

**Usage Guidelines**

By default, 802.1p priority information is not replaced or manipulated, and the information observed on ingress is preserved when transmitting the packet.

If 802.1p replacement is enabled, the 802.1p priority information that is transmitted is determined by the hardware queue that is used when transmitting the packet. The mapping is described in Table 13. This mapping cannot be changed.

**Table 13: Queue to 802.1p Priority Replacement Value**

<table>
<thead>
<tr>
<th>Hardware Queue</th>
<th>802.1p Priority Replacement Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q0</td>
<td>0</td>
</tr>
<tr>
<td>Q1</td>
<td>1</td>
</tr>
<tr>
<td>Q2</td>
<td>2</td>
</tr>
<tr>
<td>Q3</td>
<td>3</td>
</tr>
<tr>
<td>Q4</td>
<td>4</td>
</tr>
<tr>
<td>Q5</td>
<td>5</td>
</tr>
<tr>
<td>Q6</td>
<td>6</td>
</tr>
<tr>
<td>Q7</td>
<td>7</td>
</tr>
</tbody>
</table>

**Example**

The following command enables dot1p replacement on all ports:

    enable dot1p replacement ports all
**History**

This command was available in ExtremeWare 6.0.

**Platform Availability**

This command is available on the “i” series platforms only.
enable qosmonitor

   enable qosmonitor {port <port>}

Description
Enables the QoS monitoring capability on the switch.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| port    | Specifies a port. |

Default
Disabled

Usage Guidelines
When no port is specified, the QoS monitor automatically samples all the ports and records the sampled results. Error messages are logged to the syslog if the traffic exceeds the parameters of the QoS profile(s).

The QoS monitor is a utility that monitors the eight hardware queues (QP1-QP8) associated with any port(s). The QoS monitor keeps track of the number of frames and the frames per second that a specific queue is responsible for transmitting on a physical port. Two options are available: a real-time display and a separate option for retrieving information in the background and writing it to the log.

The real-time display scrolls through the given portlist to provide statistics. The particular port being monitored at that time is indicated by an asterisk (*) appearing after the port number in the display.

Monitoring QoS in the background places transmit counter and any “overflow” information into the switch log. The log notification appears if one of the queues experiences an overflow condition since the last time it was sampled. An overflow entry indicates that a queue was over-subscribed at least temporarily, and is useful for determining correct QoS settings and potential over-subscription issues.

Example
The following command enables the QoS monitoring capability on port 4:

   enable qosmonitor port 4

History
This command was available in ExtremeWare 4.0.

Platform Availability
This command is available on the “i” series platforms only.
enable red ports

    enable red ports <portlist>

Description
Enables random early detection (RED) on a port.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| portlist | Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default
Disabled

Usage Guidelines
Policy-based QoS can be configured to perform per-port Random Early Detection (RED) and drop-probability. Using this capability, the switch detects when traffic is filling up in any of the eight hardware queues, and performs a random discard on subsequent packets, based on the configured RED drop-probability.

Instead of dropping sessions during times when the queue depth is exceeded, RED causes the switch to lower session throughput. The destination node detects the dropped packet, and, using standard TCP windowing mechanisms, slows the transmission from the source node. RED drop-probability is configured on a system-wide basis, and has a valid range from 0% to 100%.

Example
The following command enables RED on ports 5-7:

    enable red ports 5-7

History
This command was first available in ExtremeWare 6.0.10.

Platform Availability
This command is available on the “i” series platforms only.
show dlcs

Description
Displays the status of DLCS (enabled or disabled) and the status of ports that are snooping WINS packets.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays DLCS status and data from the switch:
show dlcs
It produces output such as the following:
DLCS: Enabled
Ports: 4

History
This command was available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
show dot1p

Description
Displays the 802.1p-to-QoS profile mappings.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays the current 802.1p-to-QoS mappings on the switch:
show dot1p

Following is the output from this command:

<table>
<thead>
<tr>
<th>802.1p Priority Value</th>
<th>QOS Profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>QP1</td>
</tr>
<tr>
<td>1</td>
<td>QP2</td>
</tr>
<tr>
<td>2</td>
<td>QP3</td>
</tr>
<tr>
<td>3</td>
<td>QP4</td>
</tr>
<tr>
<td>4</td>
<td>QP5</td>
</tr>
<tr>
<td>5</td>
<td>QP6</td>
</tr>
<tr>
<td>6</td>
<td>QP7</td>
</tr>
<tr>
<td>7</td>
<td>QP8</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on the “i” series platforms only.
**show ports qosmonitor**

For the “i” series switches:

```
show ports {mgmt | <portlist>} qosmonitor {egress | ingress} {discards}
```

For the “e” series switches:

```
show ports {mgmt | <portlist>} qosmonitor
```

**Description**

Displays real-time QoS statistics for egress packets on one or more ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>egress</td>
<td>Specifies to display statistics in egress. Default.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>ingress</td>
<td>Specifies to display statistics in ingress.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>discards</td>
<td>Specifies to display packets discarded.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
</tbody>
</table>

**Default**

Shows QoS statistics for all ports in egress.

**Usage Guidelines**

The real-time display scrolls through the given portlist to provide statistics. You can choose screens for packet count and packets per second. The specific port being monitored is indicated by an asterisk (*) appearing after the port number in the display.

QoS monitor sampling is configured as follows:

- The port is monitored for 20 seconds before the switch moves on to the next port in the list.
- A port is sampled for five seconds before the packets per second (pps) value is displayed on the screen.

**Example**

The following command shows the real-time QoS statistics related to the specified ports:

```
show ports 1-2, 49 qosmonitor
```
Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Q0 Xmts</th>
<th>Q1 Xmts</th>
<th>Q2 Xmts</th>
<th>Q3 Xmts</th>
<th>Q4 Xmts</th>
<th>Q5 Xmts</th>
<th>Q6 Xmts</th>
<th>Q7 Xmts</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>7</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>4</td>
</tr>
<tr>
<td>2*</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>49</td>
<td>5</td>
<td>134</td>
<td>133</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>7</td>
</tr>
</tbody>
</table>

History

This command was available in ExtremeWare 2.0.

This command was updated to support PoS in Extreme 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
show qosprofile

     show qosprofile (<qosprofile>) (port <portlist>)

Description
Displays QoS information for the switch.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;qosprofile&gt;</td>
<td>Specifies a QoS profile name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Displays QoS information for all profiles.

Usage Guidelines
Information displayed includes:

- QoS profile name
- Minimum bandwidth
- Maximum bandwidth
- Priority
- A list of all traffic groups to which the QoS profile is applied

Example
The following command shows the QoS information for the specified port:

show qosprofile 2:1

Following is sample output from this command:

2:1:
    Queue:  Q0 using QP1  MinBw=0%  MaxBw=100%  Pri=2.
    Q1 using QP2  MinBw=0%  MaxBw=100%  Pri=1.
    Q2 using QP3  MinBw=0%  MaxBw=100%  Pri=4.
    Q3 using QP4  MinBw=0%  MaxBw=100%  Pri=3.
    Q4 using QP5  MinBw=0%  MaxBw=100%  Pri=4.
    Q5 using QP6  MinBw=0%  MaxBw=100%  Pri=5.
    Q6 using QP7  MinBw=0%  MaxBw=100%  Pri=6.
    Q7 using QP8  MinBw=0%  MaxBw=100%  Pri=7.

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e
This command was modified in ExtremeWare 7.2e to support a port list.
**Platform Availability**

This command is available on all platforms.
show qostype priority

Description
Displays priority settings for QoS traffic groupings.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays the QoS traffic grouping priority settings for this switch:
show qostype priority

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on the “i” series platforms only.
unconfigure diffserv examination ports

unconfigure diffserv examination ports [<portlist> | all]

Description
Removes the DiffServ examination code point from a port.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that DiffServ examination code points should be removed from all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes DiffServ code-point examination from ports 5-8:

unconfigure diffserv examination ports 5-8

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
unconfigure diffserv replacement ports

unconfigure diffserv replacement ports [<portlist> | all]

Description
Removes the DiffServ replacement mapping from a port.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that DiffServ replacement mapping should be removed from all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes DiffServ replacement from ports 5-8:
unconfigure diffserv replacement ports 5-8

History
This command was first available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
unconfigure qos-type priority

Description
Resets all traffic grouping priority values to their defaults.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Resets the traffic grouping priorities to the following:

access-list = 11
dest-mac = 8
source-mac = 7
diffserv = 3
dot1p = 2
vlan = 1

Example
The following command resets the QoS traffic grouping priorities:

unconfigure qos-type priority

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on the “i” series platforms only.
8 NAT Commands

This chapter describes commands for:

- Configuring VLANs for Network Address Translation (NAT)
- Configuring NAT translation rules
- Displaying NAT settings

Network address translation (NAT) is a feature that allows one set of IP addresses, typically private IP addresses, to be converted to another set of IP addresses, typically public Internet IP addresses. This conversion is done transparently by having a NAT device (for example, any Extreme Networks switch) rewrite the source IP address and layer 4 port of the packets.

You can configure NAT to conserve IP address space by mapping a large number of inside (private) addresses to a much smaller number of outside (public) addresses.

In implementing NAT, you must configure at least two separate VLANs involved. One VLAN is configured as inside, and corresponds to the private IP addresses you would like to translate into other IP addresses. The other type of VLAN is configured as outside, which corresponds to the public (probably Internet) IP addresses you want the inside addresses translated to. The mappings between inside and outside IP addresses are done using rules that specify the IP subnets involved and the algorithms used to translate the addresses.

**NOTE**

*The NAT modes in ExtremeWare only support translating only traffic that initiates from inside addresses.*

NAT rules are associated with a single outside VLAN. Multiple rules per outside VLAN are allowed. The rules take effect in the order they are displayed using the `show` command. Any number of inside VLANs can use a single outside VLAN, assuming that you have created proper rules. Similarly, a single inside VLAN can use any number of different outside VLANs, assuming that the rules and routing are set up properly.

TCP and UDP layer 4 ports, in combination with the IP addresses, form a unique identifier which allows hosts (as well as the NAT switch) to distinguish between separate conversations. NAT operates by replacing the inside IP packet’s source IP address and layer 4 port with an outside IP address and layer 4 port. The NAT switch maintains a connection table to map the return packets on the outside VLAN back into their corresponding inside sessions.
clear nat

    clear nat [connections | stats]

**Description**

Clears NAT connections or statistics.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>connections</td>
<td>Specifies the current NAT connections table.</td>
</tr>
<tr>
<td>stats</td>
<td>Specifies the statistics counter.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

None

**Example**

The following command clears NAT connections:

```
clear nat connections
```

**History**

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure nat add vlan map

configure nat add vlan <vlan name> map source [any | <source_ipaddress>/<mask>] {l4-port [any | <port> {(- <port>)}] {destination [any | <dest_ipaddress>/<mask>] {l4-port [any | <port> {(- <port>)}] to <nat_ip address> [/<mask> | - <ip address>] [{tcp | udp | both} [portmap {<min> - <max>} | auto-constrain]]

Description

Adds a NAT translation rule that translates private IP addresses to public IP addresses on the outside VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of the outside VLAN to which this rule applies.</td>
</tr>
<tr>
<td>source_ipaddress/mask</td>
<td>Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) that defines the source of the traffic to be mapped.</td>
</tr>
<tr>
<td>l4-port</td>
<td>Specifies a layer 4 port or port range. When used with a source IP address, indicates that the rule applies only to traffic from the specified layer 4 port(s). When used with a destination IP address, indicates that the rule applies only to packets with the specified layer 4 port(s) as their destination.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a port number in the range 1 to 65535. any indicates that the rule should be applied to traffic to/from any layer 4 port.</td>
</tr>
<tr>
<td>dest_ipaddress/mask</td>
<td>Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) used to determine the packets to which this rule applies.</td>
</tr>
<tr>
<td>nat_ipaddress</td>
<td>Specifies an IP address for the outside VLAN to which the source IP addresses will be mapped. This can be specified as a subnet (IP address and mask) or as an address range.</td>
</tr>
<tr>
<td>tcp</td>
<td>Specifies only TCP traffic should be translated.</td>
</tr>
<tr>
<td>udp</td>
<td>Specifies only UDP traffic should be translated.</td>
</tr>
<tr>
<td>both</td>
<td>Specifies that both TCP and UDP traffic should be translated.</td>
</tr>
<tr>
<td>portmap</td>
<td>Specifies that port-mapping mode should be used.</td>
</tr>
<tr>
<td>min</td>
<td>Specifies a port number in the range 1 to 65535. The default setting is 1024.</td>
</tr>
<tr>
<td>max</td>
<td>Specifies a port number in the range 1 to 65535. The default setting is 65535.</td>
</tr>
<tr>
<td>auto-constrain</td>
<td>Specifies that each inside IP address should be restricted in the number of simultaneous connections.</td>
</tr>
</tbody>
</table>

Default

N/A
Usage Guidelines

Four different modes are used to determine how the outside IP addresses and layer 4 ports are assigned:

- **Static mapping**
- **Dynamic mapping**
- **Port mapping**
- **Auto-constraining**

**Static and Dynamic Mapping.** When static mapping is used, each inside IP address uses a single outside IP address. The layer 4 ports are not changed, and only the IP address is rewritten.

With dynamic mapping, the number of inside hosts can be greater than the number of outside hosts. The outside IP addresses are allocated on a first-come, first-serve basis to the inside IP addresses. The layer 4 ports are not changed. When the last session for a specific inside IP address closes, that outside IP address can be used by other hosts.

The source IP address specifies private side IP addresses and the to IP address (the NAT address) specifies the public side IP address. The addition of the destination optional keyword after the source IP address and mask species that the NAT rule to be applied to only packets with a specific destination IP address.

If the netmask for both the source and NAT addresses is /32, the switch uses static NAT translation. If the netmasks for the source and NAT addresses are not both /32, the switch uses dynamic NAT translation.

With static or dynamic translation rules, which do not rely on layer 4 ports, ICMP traffic is translated and allowed to pass.

**Port Mapping.** The addition of a layer 4 protocol name and the portmap keyword tells the switch to use port mapping mode. As each new connection is initiated from the inside, the NAT device picks the next available source layer 4 port on the first available outside IP address. When all ports on a given IP address are in use, the NAT device uses ports from the next outside IP address.

Optionally, you may specify the range of layer 4 ports the switch chooses on the translated IP addresses. The default setting for min is 1024. The default setting for max is 65535. There is a performance penalty associated with specifying a specific port range other than the default.

ICMP traffic is not translated in port mapping mode. You must add a dynamic NAT rule for the same IP address range to allow for ICMP traffic.

**Auto-constraining.** The auto-constraining algorithm for port-mapping limits the number of outside layer 4 ports a single inside host can use simultaneously. The limitation is based on the ratio of inside to outside IP addresses. The outside IP address and layer 4 port space is evenly distributed to all possible inside hosts. This guarantees that no single inside host can prevent other traffic from flowing through the NAT device. Because of the large number of simultaneous requests that can be made from a web browser, it is not recommended that this mode be used when a large number of inside hosts are being translated to a small number of outside IP addresses.

ICMP traffic is not translated in auto-constrain mode. You must add a dynamic NAT rule for the same IP address range to allow for ICMP traffic.
Using Layer 4 Port Numbers. The addition of the `l4-port` optional keyword allows the NAT rule to be applied to only packets with a specific layer 4 source or destination port. If you use the layer 4-port command after the source IP/mask, the rule matches only if the port(s) specified are the source layer 4-ports. If you use the `l4-port` command after the destination IP/mask, the rule matches only if the port(s) specified are the destination layer 4 ports. Both options can be used together to further limit the rule. If you specify layer 4 ports, ICMP traffic will not be translated and allowed to pass.

Rule Processing. Rules are processed in order, usually in the order in which they were added. When a single rule is matched, no other rules are processed. You can view the rule order using the `show nat rules` command.

Examples

Static Mapping. The following command defines a static translation rule that specifies that traffic coming from 192.168.1.12 will be mapped to 216.52.8.32 on the outside VLAN called `out_vlan_1`:

```
configure nat add out_vlan_1 map source 192.168.1.12/32 to 216.52.8.32/32
```

Using `/32` as the netmask for both the `source` and `to` netmasks specifies static translation.

Dynamic Mapping. The following command defines a dynamic translation rule that specifies that traffic coming from subnet 192.168.1.0 will be mapped to IP addresses in the range of 216.52.8.1 to 216.52.8.31 on outside VLAN `out_vlan_1`:

```
configure nat add out_vlan_1 map source 192.168.1.0/24 to 216.52.8.1 - 216.52.8.31
```

Port Mapping. The following command defines a translation rule that specifies that TCP/UDP packets coming from 192.168.1.12 and destined for 192.168.5.20 will be mapped to 216.52.8.32 on outside VLAN `out_vlan_1`:

```
configure nat add out_vlan_1 map source 192.168.1.12/32 destination 192.168.5.20 to 216.52.8.32/32
```

The following command defines a portmap translation rule that specifies that both TCP and UDP traffic from subnet 102.168.2.0/25 will be mapped to available layer 4 ports on the IP addresses in the subnet `216.52.8.32/28`:

```
configure nat add out_vlan_2 map source 192.168.2.0/25 to 216.52.8.32 /28 both portmap
```

The following command defines a portmap translation rule that specifies that only TCP traffic from subnet 102.168.2.0/25 be mapped to layer 4 ports in the range of 1024-8192 on the IP addresses in the subnet `216.52.8.64/28`:

```
configure nat add out_vlan_2 map source 192.168.2.128/25 to 216.52.8.64/28 tcp portmap 1024 - 8192
```

Auto-constraining. The following command specifies an auto-constrain NAT translation rule that applies to both TCP and UDP traffic:

```
configure nat add out_vlan_3 map source 192.168.3.0/24 to 216.52.8.64/32 both auto-constrain
```

History

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
configure nat delete

configure nat delete [all | 
 vlan <vlan name> map source [any | <source_ip address>/<mask>] 
  {l4-port [any | <port> {- <port>}]}
  {destination <dest_ip address>/<mask> {l4-port [any | <port> {- <port>}]}}
  to <nat_ip address> [/<mask> | - <ip address>] 
  [tcp | udp | both] [portmap {<min> - <max>} | auto-constrain]

Description
Deletes a NAT translation rule.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that all NAT rules should be deleted.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the name of the outside VLAN to which this rule applies.</td>
</tr>
<tr>
<td>source_ipaddress/mask</td>
<td>Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) that defines the source of the traffic to be mapped.</td>
</tr>
<tr>
<td>l4-port</td>
<td>Specifies a layer 4 port or port range. When used with a source IP address, indicates that the rule applies only to traffic from the specified layer 4 port(s). When used with a destination IP address, indicates that the rule applies only to packets with the specified layer 4 port(s) as their destination.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a port number in the range 1 to 65535. any indicates that the rule should be applied to traffic to or from any layer 4 port.</td>
</tr>
<tr>
<td>dest_ipaddress/mask</td>
<td>Specifies a subnet IP address (in the format x.x.x.x/mask where mask is the number of bits in the subnet mask) used to determine the packets to which this rule applies.</td>
</tr>
<tr>
<td>nat_ipaddress</td>
<td>Specifies an IP address for the outside VLAN to which the source IP addresses will be mapped. This can be specified as a subnet (IP address and mask) or as an address range.</td>
</tr>
<tr>
<td>tcp</td>
<td>Specifies only TCP traffic should be translated.</td>
</tr>
<tr>
<td>udp</td>
<td>Specifies only UDP traffic should be translated.</td>
</tr>
<tr>
<td>both</td>
<td>Specifies that both TCP and UDP traffic should be translated.</td>
</tr>
<tr>
<td>min</td>
<td>Specifies a port number in the range 1 to 65535. The default setting is 1024.</td>
</tr>
<tr>
<td>max</td>
<td>Specifies a port number in the range 1 to 65535. The default setting is 65535.</td>
</tr>
<tr>
<td>autoconstrain</td>
<td>Specifies that each inside IP address should be restricted in the number of simultaneous connections.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
To delete all NAT rules, use the all keyword. To delete a specific NAT rule, you must use exactly the same parameters that were used to create the rule.
**Example**
The following command deletes a portmap translation rule:

```
configure nat delete out_vlan_2 map source 192.168.2.128/25 to 216.52.8.64/28 tcp portmap 1024 - 8192
```

**History**
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure nat finrst-timeout

configure nat finrst-timeout <seconds>

Description
Configures the timeout for a TCP session that has been torn down or reset.

Syntax Description

| seconds | Specifies the number of seconds to wait before the session table entry times out. |

Default
Default timeout is 60 seconds.

Usage Guidelines
Setting the timeout to zero specifies that session table entries should not be timed out. This setting is not normally recommended, because NAT resources will be used up.

Example
The following command configures the timeout for a reset or torn down TCP session to 120 seconds:

```
configure nat finrst-timeout 120
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure nat icmp-timeout

configure nat icmp-timeout <seconds>

Description
Configures the timeout for an ICMP packet.

Syntax Description

| seconds | Specifies the number of seconds to wait before the session table entry times out. |

Default
Default timeout is 3 seconds.

Usage Guidelines
Setting the timeout to zero specifies that session table entries should not be timed out. This setting is not normally recommended, because NAT resources will be used up.

Example
The following command configures the timeout for an ICMP packet to 5 seconds:

```
configure nat icmp-timeout 5
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure nat syn-timeout

configure nat syn-timeout <seconds>

Description
Configures the timeout for an entry with an unacknowledged TCP SYN state.

Syntax Description

| seconds | Specifies the number of seconds to wait before the session table entry times out. |

Default
Default timeout is 60 seconds.

Usage Guidelines
Setting the timeout to zero specifies that session table entries should not be timed out. This setting is not normally recommended, because NAT resources will be used up.

Example
The following command configures the timeout for a session with an unacknowledged SYN packet to 120 seconds:

configure nat syn-timeout 120

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure nat tcp-timeout

configure nat tcp-timeout <seconds>

Description
Configures the timeout for a fully set up TCP SYN session.

Syntax Description

| seconds | Specifies the number of seconds to wait before the session table entry times out. |

Default
Default timeout is 120 seconds.

Usage Guidelines
Setting the timeout to zero specifies that session table entries should not be timed out. This setting is not normally recommended, because NAT resources will be used up.

Example
The following command configures the timeout for a TCP session to 90 seconds:
configure nat tcp-timeout 90

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure nat timeout

configure nat timeout <seconds>

Description
Configures the timeout for any IP packet that is not TCP, UDP, or ICMP.

Syntax Description

| seconds | Specifies the number of seconds to wait before the session table entry times out. |

Default
Default timeout is 600 seconds.

Usage Guidelines
Setting the timeout to zero specifies that session table entries should not be timed out. This setting is not normally recommended, because NAT resources will be used up.

Example
The following command configures the timeout for packets other than TCP, UDP, or ICMP to 240 seconds:

```
configure nat timeout 240
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure nat udp-timeout

    configure nat udp-timeout <seconds>

**Description**
Configures the timeout for a UDP session.

**Syntax Description**

| seconds         | Specifies the number of seconds to wait before the session table entry times out. |

**Default**
Default timeout is 120 seconds.

**Usage Guidelines**
Setting the timeout to zero specifies that session table entries should not be timed out. This setting is not normally recommended, because NAT resources will be used up.

**Example**
The following command configures the timeout for a UDP session to 90 seconds:

```
configure nat udp-timeout 90
```

**History**
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure nat vlan

    configure nat vlan <vlan name> [inside | outside | none]

Description
Configures a VLAN to participate in NAT.

Syntax Description

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>inside</td>
<td>Specifies that the VLAN is an inside VLAN.</td>
</tr>
<tr>
<td>outside</td>
<td>Specifies that the VLAN is an outside VLAN.</td>
</tr>
<tr>
<td>none</td>
<td>Disables NAT functions on this VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
When a VLAN is configured to be inside, traffic from that VLAN is translated only if it has a matching NAT rule. Any unmatched traffic will be routed normally and not be translated. When a VLAN is configured to be outside, it routes all traffic.

Because all traffic runs through the central processing unit (CPU), it cannot run at line rate.

Normally, outside traffic will be able to initiate connections to the internal private IP addresses. If you want to prevent this, you can create IP and ICMP access lists on the outside VLAN ports to deny traffic destined for the inside IP addresses. There is a NAT performance penalty when you do this.

When a VLAN is configured to be none, all NAT functions are disabled and the VLAN operates normally.

Example
The following command configures the VLAN out_vlan_1 as an outside VLAN for use with NAT:

    configure nat vlan out_vlan_1 outside

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable nat

disable nat

Description
Disables network address translation on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
None

Example
The following command disables NAT functionality on the switch:
disable nat

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable nat

Description
Enables network address translation on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
None

Example
The following command enables NAT functionality on the switch:
```bash
enable nat
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show nat

    show nat {timeout | stats | connections | rules {vlan <outside_vlan>}}

Description
Displays NAT settings.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeout</td>
<td>Specifies the display of NAT timeout settings.</td>
</tr>
<tr>
<td>stats</td>
<td>Specifies the display of statistics for NAT traffic.</td>
</tr>
<tr>
<td>connections</td>
<td>Specifies the display of the current NAT connection table.</td>
</tr>
<tr>
<td>rules</td>
<td>Specifies the display of NAT rules, optionally for a specific VLAN.</td>
</tr>
<tr>
<td>outside_vlan</td>
<td>Specifies the outside VLAN for which NAT rules should be displayed.</td>
</tr>
</tbody>
</table>

Default
Displays all NAT settings.

Usage Guidelines
Use the keyword stats to display statistics for the NAT traffic, including:
- Number of rules
- Number of current connections
- Number of translated packets on the inside and outside VLANs
- Information about missed translations

Use the keyword connections to display the current NAT connection table, including source IP/layer 4 port mappings from inside to outside.

Use the keyword rules to display the NAT translation rules for the outside VLANs configured on the switch. Rules are displayed in the order they are processed, starting with the first one. To display the NAT rules for a specific VLAN, add the VLAN name.

Use the keyword timeout to display the NAT timeout settings configured on the switch.

Example
The following command shows the NAT translation rules configured for VLAN out_vlan_1:

    show nat rules vlan out_vlan_1

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
This chapter discusses server load balancing (SLB) and flow redirection commands.

SLB distributes client requests transparently among several servers. The main use for SLB is for web hosting (using redundant servers to increase the performance and reliability of busy websites).

You can use SLB to manage and balance traffic for client equipment such as web servers, cache servers, routers, and proxy servers. SLB is especially useful for e-commerce sites, Internet service providers, and managers of large intranets.

SLB also provides health checking. Health checking allows you to actively poll nodes to determine their health. The switch makes new connections only if the virtual server and node are both enabled and passing health checks. The switch considers a virtual server or node active unless a health check fails. If a health check fails, the switch considers the virtual server or node inactive. A virtual server or node is also considered inactive if it is disabled and has zero active connections.

Flow redirection overrides routing decisions to transparently redirect client requests to a target device (or group of devices). Unlike SLB, you do not duplicate content on the target device(s).

The switch can only redirect traffic that crosses a VLAN boundary, because flow redirection operates at layer 3. Flow redirection examines traffic and redirects it based on the following criteria, in order of priority:

1. Destination IP address and mask
2. Layer 4 port
3. Source IP address and mask

You can use flow redirection for the following:

- Web cache redirection
- Policy-based routing
clear slb connections

    clear slb connections {ipaddress <ip address> : <port> | vip <vip name>}

Description
Cleans all existing SLB connections.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a port.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify an IP address or a virtual server, all connections are cleared.

This command interrupts all current connections, but does not prevent new connections from being established. To prevent new connections from being established, disable SLB to each virtual server using the following command:

    disable slb vip <vip name> all

To prevent new connections from being established to a specific virtual server and simultaneously close all current connections, use the following command:

    disable slb vip <vip name> all close-connections-now

Example
The following command cleans the connections to the virtual server “content”:

    clear slb connections content

History
This command was available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
clear slb persistence vip

clear slb persistence vip <vip name>

Description
Clears the connection information in the persistence table.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command only during testing. Clearing persistence disables applications, such as shopping carts, that require persistence.

Example
The following command clears all information in the persistence table:

clear slb vip all persistence

History
This command was available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect add next-hop

configure flow-redirect <flow redirect> add next-hop <ip address>

Description
Adds the next hop host (gateway) that is to receive the packets that match the flow redirection policy.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command also automatically enables ping-based health checking.

Example
The following command adds the next hop of 10.2.1.20 to the flow redirection policy named “http_flow”:

```
configure flow-redirect http_flow add next-hop 10.2.1.20
```

History
This command was available in ExtremeWare 6.1.4.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect delete next-hop

configure flow-redirect <flow redirect> delete next-hop <ip address>

Description
Deletes the next hop host (gateway).

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command deletes the next hop of 10.2.1.20 from the flow redirection policy named “http_flow”:
configure flow-redirect http_flow delete next-hop 10.2.1.20

History
This command was available in ExtremeWare 6.1.4.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect service-check ftp

configure flow-redirect <flow redirect> service-check ftp user <user name> <password>

**Description**

Configures the flow redirection FTP check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name for logging in to the FTP service.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for logging in to the FTP service.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command automatically enables FTP check. The FTP check logs in to each next hop specified in the flow redirection policy with the user name and password specified.

For ExtremeWare 6.2.0 and prior, the frequency of the FTP check is 60 seconds, the timeout of the FTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

`configure flow-redirect timer service-check`

**Example**

The following command configures (and enables) FTP check for the flow redirection policy named “ftp_flow” and logs in with the user name “test” and password “extreme”:

`configure flow-redirect ftp_flow service-check ftp user test extreme`

**History**

This command was first available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on all “i” series platforms.
configure flow-redirect service-check http

configure flow-redirect <flow redirect> service-check http url <url>
match-string <alphanumeric string>

Description
Configures the flow redirection HTTP check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>url</td>
<td>Specifies the URL to be checked.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies the text to search for.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables HTTP check. The HTTP requests the designated URL from each next hop specified in the flow redirection policy and checks for the specified alphanumeric string in the first 5000 bytes. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include “http://” in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

For ExtremeWare 6.2.0 and prior, the frequency of the HTTP check is 60 seconds, the timeout of the HTTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example
The following command configures (and enables) HTTP check for the flow redirection policy named “http_flow” and checks http://www.checktest.com for the string “test”:

```
configure flow-redirect http_flow service-check http url www.checktest.com
match-string test
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect service-check L4-port

configure flow-redirect <flow redirect> service-check L4-port

Description
Configures the flow redirection layer 4 port check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables layer 4 port check. The layer 4 port check opens and closes the layer 4 port specified in the flow redirection policy.
For ExtremeWare 6.2.0 and prior, the frequency of the layer 4 port check is 10 seconds, the timeout of the layer 4 port check is 30 seconds, and you cannot configure these times.
For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer tcp-port-check
```

Example
The following command configures (and enables) layer 4 port check for the flow redirection policy named “http_flow”:

```
configure flow-redirect http_flow service-check L4-port
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect service-check nntp

configure flow-redirect <flow redirect> service-check nntp <newsgroup>

Description
Configures the flow redirection NNTP check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>newsgroup</td>
<td>Specifies the news group to be checked.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables NNTP check. The NNTP check checks the news server specified in the flow redirection policy.

For ExtremeWare 6.2.0 and prior, the frequency of the NNTP check is 60 seconds, the timeout of the NNTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example
The following command configures (and enables) NNTP check for the flow redirection policy named “nttp_flow” and checks the newsgroup “testgroup”:

```
configure flow-redirect nttp_flow service-check nntp testgroup
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect service-check ping

   configure flow-redirect <flow redirect> service-check ping

Description
Configures the flow redirection ping check.

Syntax Description

| flow redirect | Specifies a flow redirection policy. |

Default
N/A

Usage Guidelines
This command automatically enables ping check.

Ping check is also automatically enabled when you add a next hop using the following command:

configure flow-redirect add next-hop

In ExtremeWare 6.2.0 and prior, the frequency of the ping check is 10 seconds, the timeout of the ping check is 30 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

configure flow-redirect timer ping-check

Example
The following command configures (and enables) ping check for the flow redirection policy named “http_flow”:

configure flow-redirect http_flow service-check ping

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect service-check pop3

configure flow-redirect <flow redirect> service-check pop3 user <user name> <password>

Description
Configures the flow redirection POP3 check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>flow redirect</code></td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td><code>user name</code></td>
<td>Specifies the user name for logging in to the POP3 service.</td>
</tr>
<tr>
<td><code>password</code></td>
<td>Specifies the password for logging in to the POP3 service.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables POP3 check. The POP3 check logs in to each next hop specified in the flow redirection policy with the user name and password specified.

For ExtremeWare 6.2.0 and prior, the frequency of the POP3 check is 60 seconds, the timeout of the POP3 check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example
The following command configures (and enables) POP3 check for the flow redirection policy named “pop3_flow” and logs in with the user name “test” and the password “extreme”:

```
configure flow-redirect pop3_flow service-check pop3 user test extreme
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect service-check smtp

configure flow-redirect <flow redirect> service-check smtp <dns domain>

**Description**

Configures the flow redirection SMTP check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>dns domain</td>
<td>Specifies the DNS domain of the mail server.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command automatically enables SMTP check. The SMTP ensures that the mail server specified in the flow redirection policy is able to send and receive mail.

For ExtremeWare 6.2.0 and prior, the frequency of the SMTP check is 60 seconds, the timeout of the SMTP check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

configure flow-redirect timer service-check

**Example**

The following command configures (and enables) SMTP check for the flow redirection policy named “smtp_flow”:

configure flow-redirect smtp_flow service-check smtp 10.4.1.40

**History**

This command was first available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on all “i” series platforms.
configure flow-redirect service-check telnet

configure flow-redirect <flow redirect> service-check telnet user <username> <password>

Description
Configures the flow redirection telnet check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>user name</td>
<td>Specifies the user name for logging in to the telnet service.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for logging in to the telnet service.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables telnet check. The telnet check logs in to each next hop specified in the flow redirection policy with the user name and password specified.

For ExtremeWare 6.2.0 and prior, the frequency of the telnet check is 60 seconds, the timeout of the telnet check is 180 seconds, and you cannot configure these times.

For ExtremeWare 6.2.1 and later, configure the frequency and timeout using the following command:

```
configure flow-redirect timer service-check
```

Example
The following command configures (and enables) telnet check for the flow redirection policy named “telnet_flow” and logs in with the user name “test” and the password “extreme”:

```
configure flow-redirect telnet_flow service-check telnet user test extreme
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect timer ping-check

configure flow-redirect timer ping-check frequency <seconds> timeout <seconds>

**Description**
Configures the frequency and timeout for the flow redirection ping check.

**Syntax Description**

<table>
<thead>
<tr>
<th>option</th>
<th>description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>Specifies the ping check frequency. The range is 1 to 60.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the ping check timeout. The range is 1 to 60.</td>
</tr>
</tbody>
</table>

**Default**
The default frequency is 10 seconds.
The default timeout is 30 seconds.

**Usage Guidelines**
The frequency must be less than the timeout.

**Example**
The following command configures a flow redirection ping check frequency of 5 seconds and a timeout of 15 seconds:

```
configure flow-redirect timer ping-check frequency 5 timeout 15
```

**History**
This command was first available in ExtremeWare 6.2.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure flow-redirect timer service-check

   configure flow-redirect timer service-check frequency <seconds> timeout <seconds>

Description
Configures the frequency and timeout for the flow redirection service check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>Specifies the service-check frequency. The range is 15 to 300.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the service-check timeout. The range is 15 to 300.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 60 seconds.
The default timeout is 180 seconds.

Usage Guidelines
The frequency must be less than the timeout.
This frequency and timeout apply to all layer 7 service checks.

Example
The following command configures a flow redirection service-check frequency of 100 seconds and a timeout of 300 seconds:

configure flow-redirect timer service-check frequency 100 timeout 300

History
This command was first available in ExtremeWare 6.2.1.

Platform Availability
This command is available on all “i” series platforms.
configure flow-redirect timer tcp-port-check

configure flow-redirect timer tcp-port-check frequency <seconds> timeout <seconds>

Description
Configures the frequency and timeout for the flow redirection TCP port check.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>Specifies the tcp-port-check frequency. The range is 5 to 120.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the tcp-port-check timeout. The range is 5 to 300.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 10 seconds.
The default timeout is 30 seconds.

Usage Guidelines
The frequency must be less than the timeout.

Example
The following command configures a flow redirection tcp-port-check frequency of 15 seconds and a timeout of 45 seconds:

configure flow-redirect timer tcp-port-check frequency 15 timeout 45

History
This command was first available in ExtremeWare 6.2.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb esrp vlan

configure slb esrp vlan <vlan name> [add | delete] unit [number]

Description
Configures all virtual servers with the specified unit number to match the state of the specified ESRP VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan name&gt;</td>
<td>Specifies an ESRP VLAN.</td>
</tr>
<tr>
<td>unit</td>
<td>Specifies a unit identifier on a virtual server. The range is 1 to 16.</td>
</tr>
</tbody>
</table>

Default
The default is unit 1.

Usage Guidelines
You must configure ESRP for the VLAN that you specify.

Virtual servers added with a unit number that is already configured for ESRP failover automatically match the ESRP state configured for that unit number.

Use the unit number to associate a group of virtual servers with an ESRP VLAN so that ESRP controls the failover state of the virtual servers. To set the unit number of a virtual server, use the following command:

configure slb vip

For simplicity, Extreme Networks recommends that you put client, server, and virtual server VLANs in the same ESRP group.

Example
The following command configures ESRP VLAN “servers” to control the failover state of all virtual servers configured with unit 3:

call 

configure slb esrp vlan servers add unit 3

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
**configure slb failover alive-frequency**

`configure slb failover alive-frequency <seconds> timeout <seconds>`

**Description**

Configures the frequency at which the local SLB device polls the remote SLB device.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>alive-frequency</td>
<td>The frequency at which the local SLB device polls the remote SLB device. The range is 1 to 60.</td>
</tr>
<tr>
<td>timeout</td>
<td>The amount of time within which the local switch must receive a response from the remote switch. The range is 1 to 60.</td>
</tr>
</tbody>
</table>

**Default**

The default alive frequency is 1 second.

The default timeout is 3 seconds.

**Usage Guidelines**

The frequency must be less than the timeout. Extreme Networks recommends that you set the timeout greater than an even multiple of the frequency.

To enable active-active operation, use the following command:

```
enable slb failover
```

**Example**

The following command sets the alive frequency to 5 seconds and the timeout to 10 seconds:

```
configure slb alive-frequency 5 timeout 10
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb failover dead-frequency

configure slb failover dead-frequency <seconds>

**Description**
Configures the frequency at which the local switch attempts to re-establish communication with an unresponsive remote switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dead-frequency</td>
<td>The frequency at which the local switch attempts to re-establish communication with an unresponsive remote switch. The range is 1 to 60.</td>
</tr>
</tbody>
</table>

**Default**
The default dead frequency is 2 seconds.

**Usage Guidelines**
To enable active-active operation, use the following command:

`enable slb failover`

**Example**
The following command sets the dead frequency to 5 seconds:

`configure slb dead-frequency 5`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb failover failback-now

configure slb failover failback-now

Description
Configures the local SLB device to release the remote SLB resources if the remote SLB is alive.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
When an active SLB unit fails and recovers, and manual failback is enabled, use this command to force the recovered SLB unit to become the active unit. Executing this command does not affect the SLB configuration.

To enable manual failback, use the following command:

   enable slb failover manual-failback

To disable manual failback, use the following command:

   disable slb failover manual-failback

Example
The following command forces SLB to immediately fail back to the backup unit:
configure slb failover failback-now

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb failover ping-check

configure slb failover ping-check <ip address> {frequency <seconds> timeout <seconds>}

Description
Configures the SLB device to actively determine if a remote gateway is reachable by performing a ping.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the remote gateway.</td>
</tr>
<tr>
<td>frequency</td>
<td>Specifies the frequency of pings sent to the remote gateway. The range is 1 to 60.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the time before the local device declares the remote gateway down. The range is 1 to 60.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 1 second.
The default timeout is 3 seconds.

Usage Guidelines
The frequency must be less than the timeout.

If the external gateway is not reachable, the virtual servers failover to the remote SLB device.

Do not configure ping check to the remote SLB switch. If you configure ping check to the remote SLB switch and the remote switch fails, the local switch also fails.

Example
The following command sets the IP address of the remote gateway to 10.10.10.21 with a ping frequency of 5 seconds and a timeout of 10 seconds:

```
configure slb failover ping-check 10.10.10.21 frequency 5 timeout 10
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb failover unit

configure slb failover unit <number> remote-ipaddress <ip address>
local-ipaddress <ip address> {L4-port <port number>}

**Description**
Configures the switch for active-active operation.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>unit</td>
<td>Specifies a unit identifier on a virtual server. The range is 1 to 16.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a number from 1 - 16.</td>
</tr>
<tr>
<td>remote-ipaddress</td>
<td>Specifies the remote peer IP address.</td>
</tr>
<tr>
<td>local-ipaddress</td>
<td>Specifies the local failover IP address.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>L4-port</td>
<td>Specifies the TCP port used for keep alive packets between failover peers.</td>
</tr>
<tr>
<td>port number</td>
<td>Specifies a port.</td>
</tr>
</tbody>
</table>

**Default**
The default L4-port is 1028.

**Usage Guidelines**
You must configure both active switches. You must use the actual IP address of the switches for the remote-ip and local-ip; you cannot use the IP address of a virtual server.

To enable active-active operation, use the following command:

`enable slb failover`

Extreme Networks recommends that you use a dedicated layer 2 VLAN to connect the two active-active switches.

**Example**
The following command configures the local SLB switch (with an IP address of 10.10.10.22) to direct unit 2 virtual servers to failover to the SLB switch with an IP address of 10.10.10.21:

`configure slb failover unit 2 remote-ipaddress 10.10.10.21 local-ipaddress 10.10.10.22`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb global connection-block

configure slb global connection-block <number>

Description
Configures the number of SLB connections to allocate in memory; this allocation can improve performance.

Syntax Description

<table>
<thead>
<tr>
<th>number</th>
<th>Specifies the number of connection blocks. The range is 100 to 20,000.</th>
</tr>
</thead>
</table>

Default
The default is 10,000.

Usage Guidelines
Use this command when you are sure that you will have a minimum guaranteed number of connections. Additional connection blocks are allocated when necessary.

Do not use this command unless you are absolutely sure that you will use the memory allocated.

Example
The following command allocates memory for 500 connections:
configure slb global connection-block 500

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global connection-timeout

    configure slb global connection-timeout <seconds>

Description
Configures the connection timeout for transparent and translation modes.

Syntax Description

| seconds | Specifies the number of seconds. The range is 1 to 180. |

Default
The default is one second.

Usage Guidelines
None

Example
The following command configures the connection timeout for 50 seconds:
configure slb global connection-timeout 50

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global ftp

    configure slb global ftp user <user name> {password {encrypted} <password>}

Description
Configures the default parameters for layer 7 FTP service checking.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

Default
For both user and password, the default value is anonymous.

Usage Guidelines
If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The FTP service check provides a more thorough check than ping check, because the FTP service check logs in to the service.

To enable service checking, use the following command:

    enable slb vip service-check

To configure the frequency and timeout of service checks, use the following command:

    configure slb global service-check

To configure the parameters for a specific virtual server, use the following command:

    configure slb vip service-check ftp

Example
The following command configures FTP service check to log in using the user name service and the password check:

    configure slb global ftp user service password check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global http

configure slb global http url <url> match-string [any-content | alphanumeric string]

**Description**
Configures the default parameters for layer 7 HTTP service checking.

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>Specifies a URL.</td>
</tr>
<tr>
<td>match string</td>
<td>Specifies the text to be matched at the specified URL.</td>
</tr>
<tr>
<td>any-content</td>
<td>Specifies that any content confirms check.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies the text string to match.</td>
</tr>
</tbody>
</table>

**Default**
The default value for url is `/`. The default match string is any content.

**Usage Guidelines**
The HTTP service check provides a more thorough check than ping check, because the HTTP service check connects to a specific URL and checks for a specific text string. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include “http://” in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

To enable service checking, use the following command:

```bash
enable slb vip service-check
```

To configure the frequency and timeout of service checks, use the following command:

```bash
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```bash
configure slb vip service-check ftp
```

**Example**
The following command configures service check to access http://www.checktest.com and look for the text “test”:

```bash
configure slb global http url www.checktest.com match-string test
```

**History**
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
configure slb global nntp

    configure slb global nntp <newsgroup>

**Description**

Configures the default parameters for layer 7 NNTP service checking.

**Syntax Description**

<table>
<thead>
<tr>
<th>newsgroup</th>
<th>Specifies a newsgroup.</th>
</tr>
</thead>
</table>

**Default**

The default newsgroup is ebusiness.

**Usage Guidelines**

The NNTP service check provides a more thorough check than ping check, because the NNTP service check logs in to the service.

To enable service checking, use the following command:

```
enable slb vip service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip service-check ftp
```

**Example**

The following command configures the service check to log into the newsgroup “comp.dcom.lans.ethernet”:

```
configure slb global nntp comp.dcom.lans.ethernet
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb global persistence-level

    configure slb global persistence-level [any-vip | same-vip-any-port | same-vip-same-port]

Description
Configures the persistence level globally.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>any-vip</td>
<td>Specifies that an entry can match any port on any virtual server.</td>
</tr>
<tr>
<td>same-vip-any-port</td>
<td>Specifies that an entry must match the virtual server and can be any port.</td>
</tr>
<tr>
<td>same-vip-same-port</td>
<td>Specifies that an entry must match both virtual server and port for persistence.</td>
</tr>
</tbody>
</table>

Default
The default level is same-vip-same-port.

Usage Guidelines
Use this command when different virtual servers do not require different persistence settings.

If you configure any-vip persistence, ensure that all virtual servers in all pools have the same services.

Example
The following command sets the global persistence level to any-vip:

    configure slb global persistence-level any-vip

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global persistence-method

configure slb global persistence-method [per-packet | per-session]

Description

Configures the behavior of the persistence timer.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>per-packet</td>
<td>Resets the persistence timer at the receipt of each packet.</td>
</tr>
<tr>
<td>per-session</td>
<td>Resets the persistence timer at the beginning of the session. When the timer expires, persistence for the session ends.</td>
</tr>
</tbody>
</table>

Default

The default method is per-session.

Usage Guidelines

Using per-packet persistence requires more CPU processing.

To set the persistence timer, use the following command:

```
configure slb vip <vip name> client-persistence-timeout
```

Example

The following command sets the global persistence method to expire at the end of the session:

```
configure slb global persistence-method per-session
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all “i” series platforms.
configure slb global ping-check

`configure slb global ping-check frequency <seconds> timeout <seconds>`

**Description**
Configures the default health checking frequency and timeout period using layer 3-based pinging of the physical node.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the ping check. The range is 1 to 60 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the ping check. The range is 1 to 60 seconds.</td>
</tr>
</tbody>
</table>

**Default**
The default frequency is 10 seconds.
The default timeout is 30 seconds.

**Usage Guidelines**
This command sets the global values for ping check. Use the global values if your servers are all equally reliable. You can configure a node to override the global values using the following command:
`configure slb node <ip address> ping-check`
The frequency must be less than the timeout.
If the pinged node does not respond within the specified timeout period (three ping intervals by default), the node is considered down.
Shorter ping intervals require more CPU processing.

**Example**
The following command sets the global ping check frequency to 5 seconds and the timeout to 15 seconds:
`configure slb global ping-check frequency 5 timeout 15`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb global pop3

configure slb global pop3 user <user name> {password {encrypted} <password>}

Description
Configures the default parameters for layer 7 POP3 service checking.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

Default
For both user and password, the default value is anonymous.

Usage Guidelines
If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The POP3 service check provides a more thorough check than ping check, because the POP3 service check logs in to the service.

To enable service checking, use the following command:

enable slb vip service-check

To configure the frequency and timeout of service checks, use the following command:

configure slb global service-check

To configure the parameters for a specific virtual server, use the following command:

configure slb vip service-check ftp

Example
The following command configures the service check to log in using the user name “service” and the password “check”:

configure slb global pop3 user service password check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global service-check

    configure slb global service-check frequency <seconds> timeout <seconds>

Description
Configures the default health checking frequency and timeout period using layer 7-based application-dependent checking.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the service check. The range is 15 to 300 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the service check. The range is 5 to 300 seconds.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 60 seconds.
The default timeout is 180 seconds.

Usage Guidelines
The frequency must be less than the timeout.

If the health check frequency and timeout are not specified for a specific virtual server, the global values are used. To set specific frequency and timeout values for a virtual server, use the following command:

    configure slb vip <vip name> service-check

Shorter intervals require more CPU processing.

Example
The following command sets the service check frequency to 90 seconds and the timeout to 270 seconds:

    configure slb global service-check frequency 90 timeout 270

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global smtp

configure slb global smtp <dns domain>

Description
Configures the default parameters for layer 7 SMTP service checking.

Syntax Description

<table>
<thead>
<tr>
<th>dns domain</th>
<th>Specifies the domain to check.</th>
</tr>
</thead>
</table>

Default
The default value for dns domain is the switch domain. If the switch does not have a DNS domain configured, the value is “mydomain.com”.

Usage Guidelines
The SMTP service check provides a more thorough check than ping check, because the SMTP service check accesses the service.

To enable service checking, use the following command:

`enable slb vip service-check`

To configure the frequency and timeout of service checks, use the following command:

`configure slb global service-check`

To configure the parameters for a specific virtual server, use the following command:

`configure slb vip service-check ftp`

Example
The following command configures the service check to access the DNS domain servicecheck.domain.com:

`configure slb global smtp servicecheck.domain.com`

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global synguard

    configure slb global synguard max-unacknowledged-SYNs <number>

**Description**
Configures the SYN-guard feature.

**Syntax Description**

| max-unacknowledged-SYNs | Specifies the number of half-open connections that the switch allows. The range is 10 to 4000. |

**Default**
The default value is 50.

**Usage Guidelines**
If the number of half-open connections exceeds the number specified, the switch immediately ages out the half-open connections. This applies only to connections from the same source IP address.

SYN-guard is disabled by default. To enable SYN-guard, use the following command:

    enable slb global synguard

SYN-guard is automatically enabled if you configure a max-unacknowledged-SYNs value greater than 0. A max-unacknowledged-SYNs value of 0 automatically disables SYN-guard.

**Example**
The following command configures the SYN-guard feature to age out half-open connections from the same source IP address when the number of connections exceeds 30:

    configure slb global synguard max-unacknowledged-SYNs 30

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb global tcp-port-check

configure slb global tcp-port-check frequency <seconds> timeout <seconds>

Description
Configures the default health checking frequency and timeout period using layer 4-based TCP port testing.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the TCP port check. The range is 5 to 120 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the TCP port check. The range is 5 to 300 seconds.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 30 seconds.
The default timeout is 90 seconds.

Usage Guidelines
The frequency must be less than the timeout.
The TCP port check is the least intrusive health check, because it does not log in to or access the server.

If the frequency and timeout are not specified for a specific node, the global values are used. You can configure a node to override the global values using the following command:
configure slb node <ip address> : <L4 port> tcp-port-check

To enable TCP port checking, use the following command:

enable slb node tcp-port-check

Example
The following command sets the global TCP port check frequency to 15 seconds and timeout to 45 seconds:

configure slb global tcp-port-check frequency 15 timeout 45

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb global telnet

configure slb global telnet userid <userid> password {encrypted} {<password>}

**Description**

Configures the default parameters for layer 7 telnet service checking.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

**Default**

For both user and password, the default value is anonymous.

**Usage Guidelines**

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The telnet service check provides a more thorough check than ping check, because the telnet service check logs in to the service.

To enable service checking, use the following command:

```
enable slb vip service-check
```

To configure the frequency and timeout of service checks, use the following command:

```
configure slb global service-check
```

To configure the parameters for a specific virtual server, use the following command:

```
configure slb vip service-check ftp
```

**Example**

The following command configures the service check to log in using the user name “service” and the password “check”:

```
configure slb global telnet user service password check
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb gogo-mode health-check

configure slb gogo-mode <port number> health-check <ip address>

Description
Configures the health checker with the common IP addresses of the GoGo mode servers in this group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to configure the IP address before configuring individual health checks.

Example
The following command configures the GoGo mode health check for the group with port 29 as the master port and an IP address of 192.168.200.2:

```
configure slb gogo-mode 29 health-check 192.168.200.2
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure slb gogo-mode ping-check

configure slb gogo-mode <port number> ping-check frequency <seconds>
timeout <seconds>

Description
Overrrides the global default ping check frequency and timeout values for this GoGo mode group.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the ping check. The range is 1 to 60 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the ping check. The range is 1 to 60 seconds.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 10 seconds.
The default timeout is 30 seconds.

Usage Guidelines
The frequency must be less than the timeout.

To restore a configured frequency and timeout back to the global default, specify 0 for the frequency and timeout.

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

configure slb gogo-mode health-check

To enable ping check for a GoGo mode group, use the following command:

enable slb gogo-mode ping-check

To disable ping check for a GoGo mode group, use the following command:

disable slb gogo-mode ping-check

Example
The following command configures a GoGo mode ping check frequency of 15 seconds and a timeout of 45 seconds for the group with port 29 as the master port:

configure slb gogo-mode 29 ping-check frequency 15 timeout 45

History
This command was first available in ExtremeWare 6.1.5.
Platform Availability

This command is available on all “i” series platforms.
configure slb gogo-mode service-check ftp

configure slb gogo-mode <port number> service-check ftp {L4-port <L4-port>} {user <user> | password {encrypted} <password>}

Description
Configures the FTP service check parameters for a GoGo mode group.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>L4-port</td>
<td>Specifies a layer 4 port.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

Default
For both user and password, the default value is anonymous.

Usage Guidelines
Before you use this command, configure the IP address on the GoGo mode servers using the following command:

configure slb gogo-mode health-check

To enable service check for a GoGo mode group, use the following command:

enable slb gogo-mode service-check

To disable service check for a GoGo mode group, use the following command:

disable slb gogo-mode service-check

Example
The following command configures GoGo mode service check for the group with port 29 as the master port to log in using the user name service and the password check:

configure slb gogo-mode 29 service-check ftp user service password check

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure slb gogo-mode service-check http

configure slb gogo-mode <port number> service-check http {L4-port <L4-port>} {url <url> match-string [any-content | <alphanumeric string>]}*

**Description**

Configures the HTTP service check parameters for a GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>L4-port</td>
<td>Specifies a layer 4 port.</td>
</tr>
<tr>
<td>url</td>
<td>Specifies a URL.</td>
</tr>
<tr>
<td>any-content</td>
<td>Specifies that any content confirms check.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies the text string to match.</td>
</tr>
</tbody>
</table>

**Default**

The default value for url is `/.

The default match string is any content.

**Usage Guidelines**

This command accesses the specified URL and checks for the specified alphanumeric string in the first 1000 bytes. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include “http://” in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```
configure slb gogo-mode health-check
```

To enable service check for a GoGo mode group, use the following command:

```
enable slb gogo-mode service-check
```

To disable service check for a GoGo mode group, use the following command:

```
disable slb gogo-mode service-check
```

**Example**

The following command configures GoGo mode service check for the group with port 29 as the master port to access http://www.checktest.com and look for the text “test”:

```
configure slb gogo-mode 29 service-check http url www.checktest.com match-string test
```

**History**

This command was first available in ExtremeWare 6.1.5.
Platform Availability
This command is available on all “i” series platforms.
configure slb gogo-mode service-check pop3
configure slb gogo-mode <port number> service-check pop3 {L4-port <L4-port>} {userid <userid> | password {encrypted} <password>}

Description
Configures the service check parameters for a GoGo mode group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>L4-port</td>
<td>Specifies a layer 4 port.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

Default
For both user and password, the default value is anonymous.

Usage Guidelines
Before you use this command, configure the IP address on the GoGo mode servers using the following command:

configure slb gogo-mode health-check

To enable service check for a GoGo mode group, use the following command:

enable slb gogo-mode <port number> service-check

To disable service check for a GoGo mode group, use the following command:

disable slb gogo-mode <port number> service-check

Example
The following command configures GoGo mode service check for the group with port 29 as the master port to log in using the user name “service” and the password “check”:

configure slb gogo-mode 29 service-check pop3 user service password check

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure slb gogo-mode service-check smtp

configure slb gogo-mode <port number> service-check smtp {L4-port <L4-port>} {<dns domain>}

Description
Configures the service check parameters for a GoGo mode group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>L4-port</td>
<td>Specifies a layer 4 port.</td>
</tr>
<tr>
<td>dns domain</td>
<td>Specifies the domain to check.</td>
</tr>
</tbody>
</table>

Default
The default value for dns domain is the switch domain. If the switch does not have a DNS domain configured, the value is “mydomain.com”.

Usage Guidelines
Before you use this command, configure the IP address on the GoGo mode servers using the following command:

configure slb gogo-mode health-check

To enable service check for a GoGo mode group, use the following command:

enable slb gogo-mode service-check

To disable service check for a GoGo mode group, use the following command:

disable slb gogo-mode service-check

Example
The following command configures the GoGo mode service check for the group with port 29 as the master port to access the DNS domain servicecheck.domain.com:

configure slb gogo-mode 29 service-check smtp servicecheck.domain.com

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
configure slb gogo-mode service-check telnet

configure slb gogo-mode <port number> service-check telnet {L4-port <L4-port>} {user <user name> | password {encrypted} <password>}

**Description**

Configures the service check parameters for a GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>L4-port</td>
<td>Specifies a layer 4 port.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

**Default**

For both user and password, the default value is anonymous.

**Usage Guidelines**

Before you use this command, configure the IP address on the GoGo mode servers using the following command:

```bash
configure slb gogo-mode health-check
```

To enable service check for a GoGo mode group, use the following command:

```bash
enable slb gogo-mode service-check
```

To disable service check for a GoGo mode group, use the following command:

```bash
disable slb gogo-mode service-check
```

**Example**

The following command configures GoGo mode service check for the group with port 29 as the master port to log in using the user name “service” and the password “check”:

```bash
configure slb gogo-mode 29 service-check telnet user service password check
```

**History**

This command was first available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb gogo-mode service-check timer

configure slb gogo-mode <port number> service-check timer [all | ftp | http | telnet | smtp | nntp | pop3 | <TCP port number>] frequency <seconds> timeout <seconds>

**Description**
Overrides the global frequency and timeout values for the service check.

**Syntax Description**

<table>
<thead>
<tr>
<th>port number</th>
<th>Specifies the GoGo mode master port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all service checks.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP service check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP service check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet service check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP service check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP service check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 service check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies a TCP port, instead of a service, for the service check.</td>
</tr>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the service check. The range is 15 to 300 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the service check. The range is 15 to 300 seconds.</td>
</tr>
</tbody>
</table>

**Default**
The default frequency is 60 seconds.

The default timeout is 180 seconds.

**Usage Guidelines**
You can use this command at any time. This command affects the frequency and timeout for the specified service check in the specified GoGo mode group.

The frequency must be less than the timeout.

**Example**
The following command configures GoGo mode FTP service check for the group with port 29 as the master port with a frequency of 15 seconds and a timeout of 45 seconds:

```
configure slb gogo-mode 29 service-check timer ftp frequency 15 timeout 45
```

**History**
This command was first available in ExtremeWare 6.1.5.
Platform Availability

This command is available on all “i” series platforms.
configure slb gogo-mode tcp-port-check add

    configure slb gogo-mode <port number> tcp-port-check add [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www | <TCP port number>]

**Description**

Adds the specified layer 4 port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP TCP port check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP TCP port check.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies the HTTPS TCP port check.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies the IMAP4 TCP port check.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies the LDAP TCP port check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP TCP port check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 TCP port check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP TCP port check.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies the SOCKS TCP port check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet TCP port check.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies the TFTP TCP port check.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies the Web TCP port check.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies the www TCP port check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies a TCP port for the TCP port check.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command adds the port to the specified TCP port check in the specified GoGo mode group. You can only add a single port with each command; to add multiple ports, you must enter multiple commands.

**Example**

The following command adds FTP as a GoGo mode TCP port check for the group with port 29 as the master port:

    configure slb gogo-mode 29 tcp-port-check add ftp

**History**

This command was first available in ExtremeWare 6.1.5.
Platform Availability

This command is available on all “i” series platforms.
configure slb gogo-mode tcp-port-check delete

configure slb gogo-mode <port number> tcp-port-check delete [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www | <TCP port number>]

**Description**
Deletes the specified layer 4 port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP TCP port check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP TCP port check.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies the HTTPS TCP port check.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies the IMAP4 TCP port check.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies the LDAP TCP port check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP TCP port check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 TCP port check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP TCP port check.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies the SOCKS TCP port check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet TCP port check.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies the TFTP TCP port check.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies the Web TCP port check.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies the www TCP port check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies a TCP port for the TCP port check.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command deletes the port from the specified TCP port check in the specified GoGo mode group. You can only delete a single port with each command; to delete multiple ports, you must enter multiple commands.

**Example**
The following command deletes FTP from the GoGo mode TCP port check for the group with port 29 as the master port:

configure slb gogo-mode 29 tcp-port-check delete ftp

**History**
This command was first available in ExtremeWare 6.1.5.
Platform Availability

This command is available on all “i” series platforms.
configure slb gogo-mode tcp-port-check timer

configure slb gogo-mode <port number> tcp-port-check timer [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www | <TCP port number>] frequency <seconds> timeout <seconds>

Description
Overwrites the global frequency and timeout values for the TCP port check.

Syntax Description

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
</tr>
<tr>
<td>ftp</td>
</tr>
<tr>
<td>http</td>
</tr>
<tr>
<td>https</td>
</tr>
<tr>
<td>imap4</td>
</tr>
<tr>
<td>ldap</td>
</tr>
<tr>
<td>nntp</td>
</tr>
<tr>
<td>pop3</td>
</tr>
<tr>
<td>smtp</td>
</tr>
<tr>
<td>socks</td>
</tr>
<tr>
<td>telnet</td>
</tr>
<tr>
<td>tftp</td>
</tr>
<tr>
<td>web</td>
</tr>
<tr>
<td>www</td>
</tr>
<tr>
<td>TCP port number</td>
</tr>
<tr>
<td>frequency</td>
</tr>
<tr>
<td>timeout</td>
</tr>
</tbody>
</table>

Default
The default frequency is 30 seconds.
The default timeout is 90 seconds.

Usage Guidelines
This command affects only the specified GoGo mode group.

To set the global TCP port check frequency and timeout, use the following command:

```
configure slb global tcp-port-check
```

The frequency must be less than the timeout.
Example

The following command configures GoGo mode FTP TCP port check for the group with port 29 as the master port with a frequency of 15 seconds and a timeout of 45 seconds:

```
configure slb gogo-mode 29 tcp-port-check timer ftp frequency 15 timeout 45
```

History

This command was first available in ExtremeWare 6.1.5.

Platform Availability

This command is available on all “i” series platforms.
configure slb L4-port

configure slb L4-port [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>] [treaper-timeout <seconds> ] udp-idle-timeout <seconds>]

Description
Configures the inactive period for TCP or UDP before the connection is aged out.

Syntax Description

<table>
<thead>
<tr>
<th>Service</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>Specifies the FTP service.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP service.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies the HTTPS service.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies the IMAP4 service.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies the LDAP service.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP service.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 service.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP service.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies the SOCKS service.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet service.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies the TFTP service.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies the Web service.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies the WWW service.</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the service.</td>
</tr>
<tr>
<td>treaper-timeout</td>
<td>Specifies the timeout for TCP.</td>
</tr>
<tr>
<td>udp-idle-timeout</td>
<td>Specifies the timeout for UDP.</td>
</tr>
</tbody>
</table>

Default
The default treaper-timeout is 600 seconds.
The default udp-idle-timeout is 600 seconds.

Usage Guidelines
You must configure the port and add it to a pool before you use this command. The timeout value affects all connections to the specified service on all virtual servers.

To set the timeout values for a wildcard virtual server, use a TCP or UDP port number of 0.

Example
The following command configures the ftp nodes with a TCP idle period of 30 seconds:
configure slb 14-port ftp treaper-timeout 30
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb node max-connections

configure slb node <ip address>:[ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>] max-connections <number>

Description
Configures the maximum number of simultaneous connections that can be established to a node.

Syntax Description

| ip address | Specifies the IP address of the node. |
| ftp        | Specifies the FTP TCP port check.    |
| http       | Specifies the HTTP TCP port check.   |
| https      | Specifies the HTTPS TCP port check.  |
| imap4      | Specifies the IMAP4 TCP port check.  |
| ldap       | Specifies the LDAP TCP port check.   |
| nntp       | Specifies the NNTP TCP port check.   |
| pop3       | Specifies the POP3 TCP port check.   |
| smtp       | Specifies the SMTP TCP port check.   |
| socks      | Specifies the SOCKS TCP port check.  |
| telnet     | Specifies the telnet TCP port check. |
| tftp        | Specifies the TFTP TCP port check.   |
| web        | Specifies the Web TCP port check.    |
| wildcard   | Specifies any port associated with a wildcard server. |
| www        | Specifies the www TCP port check.    |
| TCP or UDP port number | Specifies a TCP or UDP port for the TCP port check. |
| max-connections | Specifies the maximum number of simultaneous connections. The range is 0 to 999999999. |

Default
The default is 0.

Usage Guidelines
Use this command to limit the number of connections possible to a server with limited capabilities. Use max-connections of 0 to specify no limit.

Example
The following command configures the server with an IP address of 10.1.1.2:80 to accept a maximum of 10 connections:

configure slb node 10.1.1.2 : 80 max-connections 10
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb node ping-check

configure slb node <ip address> ping-check frequency <seconds> timeout <seconds>

Description
Overrides the global default frequency and timeout values for this node.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the ping check. The range is 1 to 60 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the ping check. The range is 1 to 60 seconds.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 10 seconds.
The default timeout is 30 seconds.

Usage Guidelines
The frequency must be less than the timeout.

To set the global ping-check frequency and timeout, use the following command:

configure slb global ping-check

Example
The following command sets the ping-check for the node with an IP address of 10.2.1.2 to a frequency of 30 seconds and a timeout of 90 seconds:

configure slb node 10.2.1.2 ping-check frequency 30 timeout 90

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb node tcp-port-check

configure slb node <ip address>: [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>] tcp-port-check frequency <seconds> timeout <seconds>

**Description**

Overwrites the global default frequency and timeout values for this node.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP TCP port check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP TCP port check.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies the HTTPS TCP port check.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies the IMAP4 TCP port check.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies the LDAP TCP port check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP TCP port check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 TCP port check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP TCP port check.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies the SOCKS TCP port check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet TCP port check.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies the TFTP TCP port check.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies the Web TCP port check.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies the www TCP port check.</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the TCP port check.</td>
</tr>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the TCP port check. The range is 5 to 120 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the TCP port check. The range is 5 to 300 seconds.</td>
</tr>
</tbody>
</table>

**Default**

The default frequency is 30 seconds.

The default timeout is 90 seconds.

**Usage Guidelines**

To set the global TCP port check frequency and timeout, use the following command:

```plaintext
configure slb global tcp-port-check
```

The frequency must be less than the timeout.
**Example**

The following command sets the FTP TCP port check for the node with an IP address of 10.2.1.2 to a frequency of 30 seconds and a timeout of 90 seconds:

```
configure slb node 10.2.1.2 : ftp tcp-port-check frequency 30 timeout 90
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb pool add

configure slb pool <pool name> add <ip address>: [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>] {ratio <number> | priority <number>}

**Description**

Adds a node to a pool.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool name</td>
<td>Specifies a pool.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
<tr>
<td>ratio</td>
<td>Specifies the ratio for the ratio load balancing method. The range is 0 to 65,535.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the priority for the priority load balancing method. The range is 1 to 65535.</td>
</tr>
</tbody>
</table>

**Default**

The default ratio is 1.

The default priority is 1.

**Usage Guidelines**

This command also configures the ratio or priority for the ratio and priority load balancing methods.

You must create the pool before you add nodes. When you add a new node, ping check is automatically enabled.

A ratio of 2 results in twice as much traffic as a ratio of 1. If all nodes use the same ratio, connections are distributed equally among the nodes. A ratio of 0 results in no traffic to the node. When you
configure the ratio, use the smallest common denominator. For example, to configure a ratio of 25% and 75%, use ratios of 1 and 3, instead of 25 and 75.

To configure a pool to use the ratio load balancing method, use the following command:

```
configure slb pool <pool name> lb-method ratio
```

Higher priority numbers indicate higher priority. To configure a pool to use the priority load balancing method, use the following command:

```
configure slb pool <pool name> lb-method priority
```

To change the ratio or priority of a node that is already in a pool, use the following command:

```
configure slb pool <pool name> member
```

**Example**

The following command adds the FTP node with an IP address of 10.2.1.2 to the pool “ftp” and configures the node with a priority of 2:

```
configure slb pool ftp add 10.2.1.2 : ftp priority 2
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb pool delete

configure slb pool <pool name> delete <ip address>: [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]

Description
Deletes a node from a pool.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool name</td>
<td>Specifies a pool.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node.</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Deleting a node from a pool does not delete the node from other pools. You can delete all nodes in a pool by deleting the pool. To delete a pool, use the following command:

dele te slb pool

Example
The following command deletes the FTP node with an IP address of 10.2.1.2 from the pool “ftp”:

configure slb pool ftp delete 10.2.1.2 : ftp
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb pool lb-method

    configure slb pool <pool name> lb-method [least-connections | priority | ratio | round-robin]

**Description**
Configures the SLB load balancing method.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool name</td>
<td>Specifies a pool.</td>
</tr>
<tr>
<td>least-connections</td>
<td>Specifies the least connections load balancing method.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the priority load balancing method.</td>
</tr>
<tr>
<td>ratio</td>
<td>Specifies the ratio load balancing method.</td>
</tr>
<tr>
<td>round-robin</td>
<td>Specifies the round-robin load balancing method.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to change the load balancing method after you have already created a pool.

To set the ratio or priority of a node, use the following command:

```
configure slb pool member
```

**Example**
The following command changes the load balancing method for the pool “ftp” to ratio:

```
configure slb pool ftp lb-method ratio
```

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb pool member

configure slb pool <pool name> member <ip address>: [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www | <TCP or UDP port number>] [ratio <number> | priority <number>]

Description
Configures the ratio or priority of an existing pool member.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>pool name</td>
<td>Specifies a pool.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
<tr>
<td>ratio</td>
<td>Specifies the ratio for the ratio load balancing method. The range is 0 to 65535.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the priority for the priority load balancing method. The range is 1 to 65535.</td>
</tr>
</tbody>
</table>

Default
The default ratio is 1.
The default priority is 1.

Usage Guidelines
Use this command to change the ratio or priority of an existing node. To add a node to a pool (and set the ratio or priority), use the following command:

configure slb pool add
Example
The following command changes the priority of the FTP node with an IP address of 10.2.1.2 in the pool “ftp” to 2:

```
configure slb pool ftp member 10.2.1.2 : ftp priority 2
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb proxy-client-persistence

configure slb proxy-client-persistence [add | delete] <ip address>/<netmask>

Description
Configures a client subnet that should be treated as one persistent entity.

Syntax Description

<table>
<thead>
<tr>
<th>ip address/netmask</th>
<th>Specifies an IP address and netmask.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
Use this command to force all clients from the specified proxy array to connect to the same physical server.

Example
The following command specifies that the subnet 10.10.10.20/24 should be treated as a single, persistent entity:

configure slb proxy-client-persistence add 10.10.10.20/24

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb vip

configure slb vip <vip name> unit [number]

Description
Configures the unit number for active-active failover.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>unit</td>
<td>Specifies a unit identifier on a virtual server. The range is 1 to 16.</td>
</tr>
</tbody>
</table>

Default
The default unit is 1.

Usage Guidelines
You must first create the virtual server before you use this command. To create a virtual server, use the following command:
create slb vip

Example
The following command configures the virtual server “test” with a unit number of 3:
configure slb vip test unit 3

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb vip client-persistence-timeout

configure slb vip [<vip name> | all] client-persistence-timeout <seconds>

Description
Configures the client persistence timeout value.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>client-persistence-timeout</td>
<td>Specifies the persistence timeout. The range is 1 to 999,999,999.</td>
</tr>
</tbody>
</table>

Default
The default client-persistence-timeout is 3600.

Usage Guidelines
Extreme Networks recommends that you specify a short client persistence timeout, because longer timeout values consume more memory.

Example
The following command configures the virtual server “ftp” with a client persistence timeout of 3000 seconds:

configure slb vip ftp client-persistence-timeout 3000

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb vip max-connections

configure slb vip <vip name> max-connections <number>

Description
Configures the maximum connections allowed to a particular virtual server.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>max-connections</td>
<td>Specifies the maximum number of connections allowed to a virtual server. The range is 0 to 999,999,999.</td>
</tr>
</tbody>
</table>

Default
The default value is 0.

Usage Guidelines
A value of 0 indicates that no maximum is enforced. When the maximum number of connections is reached, the server stops responding to new requests; existing connections are maintained.

Example
The following command sets the maximum connections to the virtual server “ftp” to 10:

configure slb vip ftp max-connections 10

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb vip service-check frequency

configure slb vip <vip name> service-check frequency <seconds> timeout <seconds>

Description
Configures the layer 7 service check frequency and timeout for a particular virtual server.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>frequency</td>
<td>Specifies the frequency of the service check. The range is 15 to 300 seconds.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the timeout of the service check. The range is 5 to 300 seconds.</td>
</tr>
</tbody>
</table>

Default
The default frequency is 60 seconds.
The default timeout is 180 seconds.

Usage Guidelines
The frequency must be less than the timeout.
To return to the global values, specify 0 for frequency and timeout. To set the global service check frequency and timeout, use the following command:

```
configure slb global service-check
```

Example
The following command sets the service check frequency to 15 and timeout to 45 for the virtual server named ftp:

```
configure slb vip ftp service-check frequency 15 timeout 45
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure slb vip service-check ftp

    configure slb vip <vip name> service-check ftp {user <user name> password (encrypted) <password>}

**Description**
Configures layer 7 FTP service checking for a specific virtual server.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command automatically enables service checking.

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The FTP service check provides a more thorough check than ping check, because the FTP service check logs in to the service.

To configure the frequency and timeout of service checks, use the following command:
configure slb global service-check

To configure the global parameters, use the following command:
configure slb global ftp

**Example**
The following command configures service check to login using the user name “service” and the password “check” on the virtual server “ftpvip”:
configure slb vip ftvpip service-check ftp user service password check

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb vip service-check http

    configure slb vip <vip name> service-check http {url <url> match-string [any-content | <alphanumeric string>]}

**Description**

Configures layer 7 HTTP service checking for a specific virtual server.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>url</td>
<td>Specifies a URL.</td>
</tr>
<tr>
<td>match string</td>
<td>Specifies the text to be matched at the specified URL.</td>
</tr>
<tr>
<td>any-content</td>
<td>Specifies that any content confirms the check.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies the text string to match.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command automatically enables service checking.

The HTTP service check provides a more thorough check than ping check, because the HTTP service check connects to a specific URL and checks for a specific text string. Extreme Networks recommends that you create a specific URL dedicated to this check.

Do not include “http://” in the URL. To check a URL beyond the root directory, include the path in the specified URL. The maximum length of a URL is 255 characters.

To configure the frequency and timeout of service checks, use the following command:

    configure slb global service-check

To configure the global parameters, use the following command:

    configure slb global http

**Example**

The following command configures service check to access http://www.checktest.com and look for the text “test” on the virtual server called httpvip:

    configure slb vip httpvip service-check http url www.checktest.com match-string test

**History**

This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
configure slb vip service-check nntp

    configure slb vip <vip name> service-check nntp <newsgroup>

**Description**

Configures layer 7 NNTP service checking for a specific virtual server.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>newsgroup</td>
<td>Specifies a newsgroup.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command automatically enables service checking.

The NNTP service check provides a more thorough check than ping check, because the NNTP service check logs in to the service.

To configure the frequency and timeout of service checks, use the following command:

`configure slb global service-check`

To configure the global parameters, use the following command:

`configure slb global nntp`

**Example**

The following command configures the service check to log into the newsgroup “comp.dcom.lans.ethernet” on the virtual server called nntpvip:

`configure slb vip nntpvip service-check nntp comp.dcom.lans.ethernet`

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
configure slb vip service-check pop3

configure slb vip <vip name> service-check pop3 user <user name> password {encrypted} {password}

Description
Configures layer 7 POP3 service checking for a specific virtual server.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables service checking.

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The POP3 service check provides a more thorough check than ping check, because the POP3 service check logs in to the service.

To configure the frequency and timeout of service checks, use the following command:
configure slb global service-check

To configure the global parameters, use the following command:
configure slb global pop3

Example

The following command configures the service check to login using the user name “service” and the password “check” to the virtual server named pop3vip:

configure slb vip pop3vip service-check pop3 user service password check

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on all “i” series platforms.
configure slb vip service-check smtp

configure slb vip <vip name> service-check smtp {<dns domain>}

**Description**
Configures layer 7 SMTP service checking for a specific virtual server.

**Syntax Description**

<table>
<thead>
<tr>
<th>vip name</th>
<th>Specifies a virtual server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dns domain</td>
<td>Specifies the domain to check.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command automatically enables service checking.

The SMTP service check provides a more thorough check than ping check, because the SMTP service check accesses the service.

To configure the frequency and timeout of service checks, use the following command:

`configure slb global service-check`

To configure the global parameters, use the following command:

`configure slb global smtp`

**Example**
The following command configures the service check to access the DNS domain servicecheck.domain.com on the virtual server named smtpvip:

`configure slb vip smtpvip service-check smtp servicecheck.domain.com`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
configure slb vip service-check telnet

configure slb vip <vip name> service-check telnet {user <user name> password {encrypted} <password>}

Description
Configures layer 7 telnet service checking for a specific virtual server.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies the user name that is checked.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for the user name.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Encrypts the password stored in the configuration file.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command automatically enables service checking.

If you do not enter a password, you are prompted for the password twice. Extreme Networks recommends that you use a password.

The telnet service check provides a more thorough check than ping check, because the telnet service check logs in to the service.

To configure the frequency and timeout of service checks, use the following command:
configure slb global service-check

To configure the global parameters, use the following command:
configure slb global telnet

Example
The following command configures the service check to login using the user name service and the password check on the virtual server named telnetvip:
configure slb vip telnetvip service-check telnet user service password check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
configure vlan slb-type

    configure vlan <vlan name> slb-type [both | client | none | server]

Description
Marks a VLAN as either a server VLAN or a client VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>both</td>
<td>Configures the VLAN as both a server and a client VLAN.</td>
</tr>
<tr>
<td>client</td>
<td>Configures the VLAN as a client VLAN.</td>
</tr>
<tr>
<td>none</td>
<td>Disables SLB on the VLAN.</td>
</tr>
<tr>
<td>server</td>
<td>Configures the VLAN as a server VLAN.</td>
</tr>
</tbody>
</table>

Default
The default is none.

Usage Guidelines
Use the both option if a server originates or could possibly originate connections to other servers.

Example
The following command configures the VLAN “client_vlan” as a client VLAN:

    configure vlan client_vlan slb-type client

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
create flow-redirect

create flow-redirect <flow redirect> [any | tcp | tup | udp] destination 
[<ip address> / <mask> [ip-port <number> | src-ip-port <number>]] | any] 
source [<ip address> / <mask> | any]

Description
Creates a flow redirection policy.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
<tr>
<td>any</td>
<td>Forwards traffic using either TCP or UDP on any IP port.</td>
</tr>
<tr>
<td>tcp</td>
<td>Forwards TCP traffic on a single IP port.</td>
</tr>
<tr>
<td>tup</td>
<td>Forwards traffic using either TCP or UDP on a single IP port.</td>
</tr>
<tr>
<td>udp</td>
<td>Forwards traffic using only UDP on a single IP port.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ip-port</td>
<td>Specifies the destination TCP or UDP layer 4 port for traffic going to a destination range.</td>
</tr>
<tr>
<td>src-ip-port</td>
<td>Specifies the TCP or UDP layer 4 port for traffic coming from the source IP ranges to the destination IP ranges.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the port.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Creating a flow redirection policy automatically enables flow redirection.

To delete a flow redirection policy, use the following command:

disable flow-redirect

To rename or modify a flow redirection policy, you must delete and recreate the flow redirection policy.

Example
The following command creates a flow redirection policy named “http” that forwards TCP traffic to 10.1.1.10 port 80 from any source IP address:

create flow-redirect http tcp destination 10.1.1.10/29 ip-port 80 source any

History
This command was available in ExtremeWare 6.1.4. This command was modified in 6.2 to add the tup parameter.
Platform Availability
This command is available on all “i” series platforms.
create slb pool

create slb pool <pool name> {lb-method [least-connections | priority | ratio | round-robin]}

Description
Creates a server pool and optionally assigns a load-balancing method to the pool.

Syntax Description

| pool name | Specifies a pool. |
| lb-method | Specifies the load-balancing method. |

Default
The default load-balancing method is round-robin.

Usage Guidelines
To change the load-balancing method of an existing pool, use the following command:
configure slb pool lb-method

To add a node to the pool (and set the ratio or priority), use the following command:
configure slb pool add

Example
The following command creates the pool named ftp_pool and assigns the priority load-balancing method:
configure slb pool ftp_pool lb-method priority

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
create slb vip

create slb vip <vip name> pool <pool name> mode [transparent | translation | port-translation] <ip address> {- <upper range>} : <L4 port> {unit <number>}

Description
Creates one or more new virtual servers.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>pool name</td>
<td>Specifies a pool.</td>
</tr>
<tr>
<td>mode</td>
<td>Specifies the forwarding mode.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the virtual server.</td>
</tr>
<tr>
<td>upper range</td>
<td>Specifies the upper IP address for a range of IP addresses.</td>
</tr>
<tr>
<td>L4 port</td>
<td>Specifies a port.</td>
</tr>
<tr>
<td>unit</td>
<td>Specifies a unit identifier on a virtual server. The range is 1 to 16.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You must create the pool before assigning a virtual server to the pool. To create a pool, use the following command:

```
create slb pool
```

Example
The following command creates the virtual server named ftp_vip, with an IP address of 10.10.10.2 in the pool named ftp_pool, and assigns the port-translation forwarding mode:

```
configure slb vip ftp_vip pool ftp_pool mode port-translation 10.10.10.2 : ftp
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
delete flow-redirect

    delete flow-redirect <flow redirect>

Description
Deletes a flow redirection policy.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
To rename or modify a flow redirection policy, you must delete and recreate the flow redirection policy.

Example
The following command deletes a flow redirection policy named http:

delete flow-redirect http

History
This command was available in ExtremeWare 6.1.4.

Platform Availability
This command is available on all “i” series platforms.
delete slb pool

dele te slb pool [<pool name> | all]

Description
Deletes a server pool.

Syntax Description

<table>
<thead>
<tr>
<th>pool name</th>
<th>Specifies a pool.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all pools.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You must first delete all virtual servers before deleting the pool. To delete a virtual server, use the following command:
delete slb vip

Example
The following command deletes the pool named http_pool:
delete slb pool http_pool

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
delete slb vip

delete slb vip [<vip name> | all]

**Description**
Deletes one or all virtual servers.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
You must use this command to delete all virtual servers from a pool before deleting the pool.

**Example**
The following command deletes the virtual server named http_vip:

delete slb vip http_vip

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
disable flow-redirect

disable flow-redirect [all | <flow redirect>]

Description
Disables flow redirection.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all flow policies.</td>
</tr>
<tr>
<td>flow redirect</td>
<td>Specifies a single flow redirection policy.</td>
</tr>
</tbody>
</table>

Default
The default parameter is all.

Flow redirection is disabled by default.

Usage Guidelines
When you create a new flow redirection policy, flow redirection is automatically enabled.

To enable flow redirection, use the following command:

```
enable flow-redirect
```

Example
The following command disables flow redirection for all flow policies:

```
disable flow-redirect all
```

History
This command was available in ExtremeWare 6.1.4.

Platform Availability
This command is available on all “i” series platforms.
disable slb

disable slb

Description
Disables SLB processing.

Syntax Description
This command has no arguments or variables.

Default
SLB is disabled by default.

Usage Guidelines
Disabling SLB causes the following to occur:
- Closes all connections.
- Withdraws virtual server routes or routes that do not respond with proxy ARP responses of virtual server addresses.
- Disconnects the switch from redundant SLB switches.

To enable SLB, use the following command:

enable slb

Example
The following command disables SLB:

disable slb

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb 3dns

disable slb 3dns iquery-client

Description
Disables 3DNS support.

Syntax Description
This command has no arguments or variables.

Default
3DNS is disabled by default.

Usage Guidelines
To enable 3DNS, use the following command:

   enable slb 3dns

Example
The following command disables 3DNS:

disable slb 3dns iquery-client

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb failover

disable slb failover

Description
Disables the SLB failover mechanism.

Syntax Description
This command has no arguments or variables.

Default
SLB failover is disabled by default.

Usage Guidelines
To enable SLB failover, use the following command:

enable slb failover

Example
The following command disables SLB failover:

disable slb failover

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb failover manual-failback

disable slb failover manual-failback

Description
Disables manual failback.

Syntax Description
This command has no arguments or variables.

Default
Manual failback is disabled by default.

Usage Guidelines
To enable manual failback, use the following command:

```text
enable slb failover manual-failback
```

Example
The following command disables manual failback:

```text
disable slb failover manual-failback
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb failover ping-check

    disable slb failover ping-check

Description
Disables ping check to an external gateway.

Syntax Description
This command has no arguments or variables.

Default
Ping check is disabled by default.

Usage Guidelines
To enable ping check, use the following command:

    enable slb failover ping-check

Example
The following command disables ping check:

    disable slb failover ping-check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb global synguard

Description
Disables the TCP SYN-guard feature.

Syntax Description
This command has no arguments or variables.

Default
SYN-guard is disabled by default.

Usage Guidelines
To enable SYN-guard, use the following command:

```
enable slb global synguard
```

Example
The following command disables SYN-guard:

```
disable slb global synguard
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb gogo-mode

disable slb gogo-mode <port number> {all}

Description
Disables GoGo mode processing.

Syntax Description

<table>
<thead>
<tr>
<th>port number</th>
<th>Specifies the GoGo mode master port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Disables all health checking.</td>
</tr>
</tbody>
</table>

Default
GoGo mode is disabled by default.

Usage Guidelines
Before you disable GoGo mode, disconnect the servers; they all have identical MAC and IP addresses, which can cause VLAN conflicts.

To enable GoGo mode, use the following command:

```
enable slb gogo-mode
```

Example
The following command disables GoGo mode for the group with port 29 as the master port:

disable slb gogo-mode 29

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb gogo-mode ping-check

disable slb gogo-mode <port number> ping-check

Description
Disables layer 3 ping check for this GoGo mode group.

Syntax Description

<table>
<thead>
<tr>
<th>port number</th>
<th>Specifies the GoGo mode master port.</th>
</tr>
</thead>
</table>

Default
GoGo mode ping check is disabled by default.

Usage Guidelines
To enable ping check for a GoGo mode group, use the following command:

```
enable slb gogo-mode ping-check
```

Example
The following command disables GoGo mode ping check for the group with port 29 as the master port:

```
disable slb gogo-mode 29 ping-check
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
**disable slb gogo-mode service-check**

disable slb gogo-mode <port number> service-check [all | ftp | http | nntp | pop3 | smtp | telnet | <TCP port number>]

**Description**
Disables layer 7 service check for this GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all service checks.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP service check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP service check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP service check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 service check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP service check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet service check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies the TCP port, instead of the service.</td>
</tr>
</tbody>
</table>

**Default**
GoGo mode service check is disabled by default.

**Usage Guidelines**
To enable service-check for a GoGo mode group, use the following command:

`enable slb gogo-mode service-check`

**Example**
The following command disables GoGo mode FTP service-check for the group with port 29 as the master port:

`disable slb gogo-mode 29 service-check ftp`

**History**
This command was first available in ExtremeWare 6.1.5.

**Platform Availability**
This command is available on all “i” series platforms.
disable slb gogo-mode tcp-port-check

disable slb gogo-mode <port number> tcp-port-check [all | ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www | <TCP port number>]

Description
Disables layer 4 TCP port check for this GoGo mode group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all TCP port checks.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP TCP port check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP TCP port check.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies the HTTPS TCP port check.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies the IMAP4 TCP port check.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies the LDAP TCP port check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP TCP port check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 TCP port check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP TCP port check.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies the SOCKS TCP port check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet TCP port check.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies the TFTP TCP port check.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies the Web TCP port check.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies the www TCP port check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies the TCP port of the TCP port check.</td>
</tr>
</tbody>
</table>

Default
GoGo mode TCP port check is disabled by default.

Usage Guidelines
To enable TCP port check for a GoGo mode group, use the following command:

```
enable slb gogo-mode <port number> tcp-port-check
```

Example
The following command disables all GoGo mode TCP port checks for the group with port 29 as the master port:

```
disable slb gogo-mode 29 tcp-port-check all
```

History
This command was first available in ExtremeWare 6.1.5.
Platform Availability

This command is available on all “i” series platforms.
disable slb L4-port

disable slb L4-port [all | ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]

**Description**
Disables one or all SLB ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
To enable an SLB port, use the following command:

`enable slb L4-port`

**Example**
The following command disables SLB for FTP ports:

`disable slb L4-port ftp`

**History**
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
disable slb node

disable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>] ] {close-connections-now}

Description
Disables one or all nodes.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
<tr>
<td>close-connections-now</td>
<td>Immediately closes all open connections.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command stops nodes from accepting new connections; existing connections are not closed unless you specify close-connections-now. SLB continues to function with other nodes.

If you disable all nodes in a pool, all virtual servers associated with that pool are effectively disabled.

To enable a node, use the following command:

enable slb node
Example
The following command disables all nodes and immediately closes all open connections:

disable slb node all close-connections-now

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb node ping-check

disable slb node [all | <ip address>] ping-check

Description
Disables layer 3 ping check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
</tbody>
</table>

Default
Ping check is disabled by default.

Usage Guidelines
Ping check is automatically enabled when a node is added to a pool.

To enable ping check on a node, use the following command:

```
enable slb node ping-check
```

Example
The following command disables all ping checks:

```
disable slb node all ping-check
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb node tcp-port-check

```
disable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]] tcp-port-check
```

**Description**
Disables layer 4 TCP port checking.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

**Default**
TCP port check is disabled by default.

**Usage Guidelines**
To enable TCP port check, use the following command:
```
enable slb node tcp-port-check
```

**Example**
The following command disables all TCP port checks:
```
disable slb node all tcp-port-check
```

**History**
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
disable slb proxy-client-persistence

disable slb proxy-client-persistence

Description
Disables proxy client persistence.

Syntax Description
This command has no arguments or variables.

Default
Proxy client persistence is disabled by default.

Usage Guidelines
To enable proxy client persistence, use the following command:

enable slb proxy-client-persistence

Example
The following command disables proxy client persistence:

disable slb proxy-client-persistence

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb vip

disable slb vip [all | <vip name> | ipaddress <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]] {close-connections-now}

Description
Disables one or all virtual servers.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP virtual server.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP virtual server.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS virtual server.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 virtual server.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP virtual server.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP virtual server.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 virtual server.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP virtual server.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS virtual server.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet virtual server.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP virtual server.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web virtual server.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www virtual server</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the virtual server.</td>
</tr>
<tr>
<td>close-connections-now</td>
<td>Immediately closes all open connections.</td>
</tr>
</tbody>
</table>

Default
SLB is disabled by default.

Usage Guidelines
When SLB is disabled, no new connections are allowed to the real servers. If close-connections-now is specified, all existing connections are immediately closed.

To enable a virtual server, use the following command:

enable slb vip
Example
The following command disables the virtual server named ftp_vip and closes all open connections:
\[ \text{disable slb vip ftp_vip close-connections-now} \]

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
disable slb vip client-persistence

disable slb vip [all | <vip name>] client-persistence

**Description**
Disables client persistence.

**Syntax Description**

<table>
<thead>
<tr>
<th>all</th>
<th>Specifies all virtual servers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

**Default**
Client persistence is disabled by default.

**Usage Guidelines**
To enable client persistence, use the following command:

`enable slb vip client-persistence`

**Example**
The following command disables client persistence for the virtual server "ftp_vip":

`disable slb vip ftp_vip client-persistence`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
disable slb vip service-check

disable slb vip [all | <vip name>] service-check

Description
Disables layer 7 service check.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
Service check is disabled by default.

Usage Guidelines
To enable service check, use the following command:

```
enable slb vip service-check
```

Example
The following command disables service check for the virtual server named ftp_vip:

```
disable slb vip ftp_vip service-check
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
Disable SLB VIP Sticky-Persistence

_disable slb vip [all | <vip name>] sticky-persistence_

**Description**
Disables sticky persistence.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

**Default**
Sticky persistence is disabled by default.

**Usage Guidelines**
Sticky persistence is available only on wildcard virtual servers; it is especially useful for cache servers. Sticky persistence tracks destination IP addresses. When a client tries to connect to a destination IP address, the switch directs the client to the same cache server previously used for that destination IP address. This helps reduce the amount of duplicated content on cache servers in your network.

To enable sticky persistence, use the following command:

`enable slb vip sticky-persistence`

**Example**
The following command disables sticky persistence for the virtual server “ftp_vip”:

`disable slb vip ftp_vip sticky-persistence`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
disable slb vip svcdown-reset

    disable slb vip [all | <vip name>] svcdown-reset

Description
Disables the svcdown-reset feature.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
The svcdown-reset feature is disabled by default.

Usage Guidelines
The svcdown-reset feature configures the switch to send TCP RST packets to both the clients and the virtual server if the virtual server fails a health-check.

To enable svcdown-reset, use the following command:

    enable slb vip svcdown-reset

Example
The following command disables svcdown-reset for the virtual server named ftp_vip:

    disable slb vip ftp_vip svcdown-reset

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable flow-redirect

enable flow-redirect [all | <flow redirect>]

Description
Enables flow redirection.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all flow redirection policies.</td>
</tr>
<tr>
<td>flow redirect</td>
<td>Specifies a single flow redirection policy.</td>
</tr>
</tbody>
</table>

Default
The default parameter is all.
Flow redirection is disabled by default.

Usage Guidelines
When you create a new flow redirection policy, flow redirection is automatically enabled.

To disable flow redirection, use the following command:
disable flow-redirect

Example
The following command enables flow redirection for all flow policies:
enable flow-redirect all

History
This command was available in ExtremeWare 6.1.4.

Platform Availability
This command is available on all “i” series platforms.
enable slb

   enable slb

Description
Enables SLB processing.

Syntax Description
This command has no arguments or variables.

Default
SLB is disabled by default.

Usage Guidelines
This command activates the following functions for transparent, translational, and port translation modes:

- Exporting of VIP routes or proxy ARP for VIP addresses.
- Processing of VIP lookup and connection setup.
- Establishing communication with redundant SLB switches.
- Positively responding to MIB, 3DNS, and SeeIT requests.

Before you enable SLB, enable IP forwarding on the associated VLANs.

NOTE
SLB cannot be enabled when MPLS or Destination-sensitive accounting is enabled or SLPM is active.

Example
The following command enables SLB:

   enable slb

History
This command was first available in ExtremeWare 6.1.

This command was updated in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was modified in ExtremeWare 7.0.0.

Platform Availability
This command is available on all “i” series platforms.
enable slb 3dns

enable slb 3dns iquery-client

Description
Enables 3DNS support.

Syntax Description
This command has no arguments or variables.

Default
3DNS is disabled by default.

Usage Guidelines
The following 3DNS global balance modes are supported:
- completion
- rate
- global_availability
- leastcon
- null
- packet_rate
- random
- ration
- rr
- return_to_dns

To disable 3DNS, use the following command:
disable slb 3dns

Example
The following command enables 3DNS:
enable slb 3dns iquery-client

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb failover

enable slb failover

**Description**
Enables SLB failover.

**Syntax Description**
This command has no arguments or variables.

**Default**
Failover is disabled by default.

**Usage Guidelines**
When SLB failover is enabled, the primary SLB switch automatically resumes primary status when it becomes active.

Before you enable SLB failover, configure your switches using the following command:
```
class enable slb failover unit
```

To disable SLB failover, use the following command:
```
disable slb failover
```

**Example**
The following command enables SLB failover:
```
enable slb failover
```

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on all “i” series platforms.
enable slb failover manual-failback

enable slb failover manual-failback

Description
Enables manual failback.

Syntax Description
This command has no arguments or variables.

Default
Manual failback is disabled by default.

Usage Guidelines
When manual failback is enabled, the primary SLB switch does not automatically resume primary status until you use the following command:

`configure slb failover failback-now`

To disable manual failback, use the following command:

`disable slb failover manual-failback`

Example
The following command enables manual failback:

`enable slb failover manual-failback`

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb failover ping-check

 enable slb failover ping-check

Description
Enables ping check.

Syntax Description
This command has no arguments or variables.

Default
Ping check is disabled by default.

Usage Guidelines
To disable ping check, use the following command:

disable slb failover ping-check

Example
The following command enables ping check:

enable slb failover ping-check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb global synguard

enable slb global synguard

Description
Enables the TCP SYN-guard feature.

Syntax Description
This command has no arguments or variables.

Default
SYN-guard is disabled by default.

Usage Guidelines
To disable SYN-guard, use the following command:
disable slb global synguard

Example
The following command enables SYN-guard:
enable slb global synguard

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb gogo-mode

   enable slb gogo-mode <port number> grouping <port list>

Description
Enables GoGo mode processing for a group of ports.

Syntax Description

<table>
<thead>
<tr>
<th>port number</th>
<th>Specifies the GoGo mode master port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>port list</td>
<td>Specifies a range or list of ports assigned to the group.</td>
</tr>
</tbody>
</table>

Default
GoGo mode is disabled by default.

Usage Guidelines
To disable GoGo mode, use the following command:

disable slb gogo-mode

Example
The following command enables GoGo mode for the group containing ports 15, 17, 19-23, and 25-30 with port 29 as the master port:

```
enable slb gogo-mode 29 grouping 15, 17, 19 - 23, 25 - 30
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb gogo-mode ping-check

```
enable slb gogo-mode <port number> ping-check <ip address>
```

**Description**

Enables layer 3 ping check for the GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th>port number</th>
<th>Specifies the GoGo mode master port.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address to be pinged.</td>
</tr>
</tbody>
</table>

**Default**

GoGo mode ping check is disabled by default.

**Usage Guidelines**

GoGo mode ping check sends a ping from each physical port in the GoGo mode grouping to the configured IP address.

If you do not specify an IP address, GoGo mode ping check uses the previously configured IP address.

You must enable GoGo mode for the group before you enable ping check. To enable GoGo mode, use the following command:

```
enable slb gogo-mode
```

To disable ping check for a GoGo mode group, use the following command:

```
disable slb gogo-mode ping-check
```

**Example**

The following command enables GoGo mode ping check for the group with port 29 as the master port to IP address 10.10.200.3:

```
enable slb gogo-mode 29 ping-check 10.10.200.3
```

**History**

This command was first available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on all “i” series platforms.
enable slb gogo-mode service-check

```
enable slb gogo-mode <port number> service-check [all | ftp | http | nntp | pop3 | smtp | telnet | <TCP port number>]
```

**Description**
Enables layer 7 service checking for the GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all service checks.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP service check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP service check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP service check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 service check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP service check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet service check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies the TCP port, instead of the service.</td>
</tr>
</tbody>
</table>

**Default**
GoGo mode service check is disabled by default.

**Usage Guidelines**
To disable service-check for a GoGo mode group, use the following command:

```
disable slb gogo-mode service-check
```

**Example**
The following command enables GoGo mode FTP service-check for the group with port 29 as the master port:

```
enable slb gogo-mode 29 service-check ftp
```

**History**
This command was first available in ExtremeWare 6.1.5.

**Platform Availability**
This command is available on all “i” series platforms.
enable slb gogo-mode tcp-port-check

enable slb gogo-mode <port number> tcp-port-check [all | ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | www | <TCP port number>]

**Description**

Enables layer 4 TCP port check for the GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Example</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all TCP port checks.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP TCP port check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP TCP port check.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies the HTTPS TCP port check.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies the IMAP4 TCP port check.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies the LDAP TCP port check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP TCP port check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 TCP port check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP TCP port check.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies the SOCKS TCP port check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet TCP port check.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies the TFTP TCP port check.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies the Web TCP port check.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies the www TCP port check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies the TCP port of the TCP port check.</td>
</tr>
</tbody>
</table>

**Default**

GoGo mode TCP port check is disabled by default.

**Usage Guidelines**

To disable TCP port check for a GoGo mode group, use the following command:

disable slb gogo-mode tcp-port-check

**Example**

The following command enables all GoGo mode TCP port checks for the group with port 29 as the master port:

enable slb gogo-mode 29 tcp-port-check all

**History**

This command was first available in ExtremeWare 6.1.5.
Platform Availability

This command is available on all “i” series platforms.
enable slb L4-port

enable slb L4-port [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]

Description
Enables an SLB port.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

Default
Layer 4 ports are enabled by default.

Usage Guidelines
To disable a layer 4 port, use the following command:

disable slb L4-port

Example
The following command enables SLB for FTP ports:
enable slb L4-port ftp

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
enable slb node

enable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]]

Description
Enables one or all nodes.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

Default
Nodes are enabled by default.

Usage Guidelines
This command allows nodes to accept new connections.

To disable a node, use the following command:

disable slb node

Example
The following command enables all nodes:

enable slb node all
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb node ping-check

    enable slb node [all | <ip address>] ping-check

**Description**

Enables layer 3 ping check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the node.</td>
</tr>
</tbody>
</table>

**Default**

Ping check is enabled by default.

**Usage Guidelines**

Ping check is automatically enabled when a node is added to a pool.

To disable ping check on a node, use the following command:

disable slb node ping-check

**Example**

The following command enables all ping checks:

enable slb node all ping-check

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
enable slb node tcp-port-check

```
enable slb node [all | <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]] tcp-port-check
```

**Description**

Enables layer 4 TCP port check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all nodes.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node.</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

**Default**

TCP port check is disabled by default.

**Usage Guidelines**

To disable TCP port check, use the following command:

```
disable slb node tcp-port-check
```

**Example**

The following command enables all TCP port checks:

```
enable slb node all tcp-port-check
```

**History**

This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
enable slb proxy-client-persistence

enable slb proxy-client-persistence

Description
Enables proxy client persistence.

Syntax Description
This command has no arguments or variables.

Default
Proxy client persistence is disabled by default.

Usage Guidelines
To disable proxy client persistence, use the following command:

disable slb proxy-client-persistence

Example
The following command enables proxy client persistence:

enable slb proxy-client-persistence

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb vip

enable slb vip [all | <vip name> | ipaddress <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]]

Description
Enables one or all virtual servers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP virtual server.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP virtual server.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS virtual server.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 virtual server.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP virtual server.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP virtual server.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 virtual server.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP virtual server.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS virtual server.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet virtual server.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP virtual server.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web virtual server.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www virtual server.</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the virtual server.</td>
</tr>
</tbody>
</table>

Default
SLB is disabled by default.

Usage Guidelines
To disable a virtual server, use the following command:

disable slb vip

Example
The following command enables the virtual server “ftp_vip”:

enable slb vip ftp_vip
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb vip client-persistence

    enable slb vip [all | <vip name>] client-persistence {netmask <netmask>}

Description
Enables client persistence.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a netmask.</td>
</tr>
</tbody>
</table>

Default
The default is disabled.

Usage Guidelines
To disable client persistence, use the following command:

disable slb vip client-persistence

Example
The following command enables client persistence for the virtual server named ftp_vip:

enable slb vip ftp_vip client-persistence

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb vip service-check

    enable slb vip [all | <vip name>] service-check

Description
Enables layer 7 service check.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
Service check is disabled by default.

Usage Guidelines
The service checks are based on the following information:

- If a service check is already configured, it will use the configured service-checking information.
- If a service check is configured for a TCP port number (instead of for a service), ExtremeWare assigns the service based on the port number (if the port number is well known) and uses the global default parameters.

To disable service check, use the following command:

disable slb vip service-check

Example
The following command enables service-check for the virtual server “ftp_vip”:

enable slb vip ftp_vip service-check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
enable slb vip sticky-persistence

```
enable slb vip [all | ipaddress <ip address> | <vip name>]
sticky-persistence {netmask <netmask>}
```

**Description**

Enables the sticky persistence feature and specifies the client address mask.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a netmask.</td>
</tr>
</tbody>
</table>

**Default**

Sticky persistence is disabled by default.

**Usage Guidelines**

To disable sticky persistence, use the following command:

```
disable slb vip sticky-persistence
```

**Example**

The following command enables sticky persistence for the virtual server “ftp_vip”:

```
enable slb vip ftp_vip sticky-persistence
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all “i” series platforms.
enable slb vip svcdown-reset

    enable slb vip [all | <vip name>] svcdown-reset

Description
Enables svcdown-reset.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
The svcdown-reset feature is disabled by default.

Usage Guidelines
The svcdown-reset feature configures the switch to send TCP RST packets to both the clients and the virtual server if the virtual server fails a health-check.

To disable svcdown-reset, use the following command:

disable slb vip svcdown-reset

Example
The following command enables svcdown-reset for the virtual server named ftp_vip:

enable slb vip ftp_vip svcdown-reset

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show flow-redirect

    show flow-redirect <flow redirect>

Description
Displays the current configuration and statistics for flow redirection.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>flow redirect</td>
<td>Specifies a flow redirection policy.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a flow redirection policy, configuration and statistics for all flow redirection policies are displayed.

The following fields are displayed:

<table>
<thead>
<tr>
<th>Service Check</th>
<th>Displays the frequency and timeout settings for the flow redirection ping check, TCP port check, and service check.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timer Settings:</td>
<td>Displays the IP source address mode:</td>
</tr>
<tr>
<td>Flow IPSA Mode</td>
<td>• Enumeration Mode—The default mode, used for network masks from /32 to /20.</td>
</tr>
<tr>
<td></td>
<td>• Subnet Mode— Used for network masks from /19 to /1.</td>
</tr>
<tr>
<td></td>
<td>The mode is selected automatically when you specify a network mask.</td>
</tr>
<tr>
<td>Proto:</td>
<td>Displays the flow type.</td>
</tr>
<tr>
<td></td>
<td>• any—Forwards any traffic over any IP port.</td>
</tr>
<tr>
<td></td>
<td>• tcp—Forwards TCP traffic over a single IP port.</td>
</tr>
<tr>
<td></td>
<td>• tup—Forwards both TCP and UDP traffic over a single IP port.</td>
</tr>
<tr>
<td></td>
<td>• udp—Forwards UDP traffic over a single IP port.</td>
</tr>
<tr>
<td>Dest:</td>
<td>Displays the destination IP address.</td>
</tr>
<tr>
<td>L4-src-port:</td>
<td>Displays the source port number.</td>
</tr>
<tr>
<td>Enabled:</td>
<td>Displays the status of flow redirection.</td>
</tr>
<tr>
<td></td>
<td>• Yes—Flow redirection is enabled.</td>
</tr>
<tr>
<td></td>
<td>• No—Flow redirection is not enabled.</td>
</tr>
<tr>
<td>Source:</td>
<td>• Displays the source IP address.</td>
</tr>
<tr>
<td># Servers Up:</td>
<td>Displays the number of next hops up over the number of next hops configured.</td>
</tr>
</tbody>
</table>
The following command displays the current flow redirection configuration and statistics for the flow policy “flow1”:

```
show flow-redirect flow1
```

Following is the output from this command:

**Service Check Timer Settings:**
- Ping-check Frequency: 10  Timeout: 30
- TCP-Port-check Frequency: 10  Timeout: 30
- Service-check Frequency: 60  Timeout: 180

**Flow IPSA Mode:** Enumeration Mode

**http1**
- Proto: tcp  Dest: 0.0.0.0/ 0  L4-Port: 80  Enabled: yes
- Source: 0.0.0.0/ 0  # Servers Up: 0/1

**Service Checking:**
- ping

**IP Address**
- State
- Flow Info
  - 24.3.89.145  Down  0000

**History**

This command was available in ExtremeWare 6.1.4.

**Platform Availability**

This command is available on all “i” series platforms.
show slb 3dns members

Description
Displays the current connection information between the switch and the 3DNS query.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command displays the current 3DNS information:
show slb 3dns members
IP Address       Port  Encrypt  Socket  LastUpdated
--------------- -----  -------  ------  --------------------------
There are no known 3DNS entries in our local iQuery table.

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb connections

show slb connections [ipaddress <ip address>: [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>] | vip <vip name>]

Description
Displays information about current connections.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP port.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP port.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS port.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 port.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP port.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP port.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 port.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP port.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS port.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet port.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP port.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web port.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www port.</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You can specify a client, virtual server, or node. If you do not specify a virtual server or IP address, information on all connections is displayed. An IP address of 0.0.0.0:0 is a wildcard.

Example
The following command displays the current connection information for all connections:

```
show slb connections
```

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
show slb esrp

    show slb esrp

Description
Displays SLB configuration for ESRP.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays the current ESRP configuration:
show slb esrp

Following is the output from this command:
VLAN Name  SLB Unit Status  SLB Unit(s)
servers    Standby       1

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb failover

Description
Displays SLB failover configuration and status.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
The show slb global command also displays SLB failover configuration and status.

Example
The following command displays the current SLB failover configuration and status:
show slb failover

Following is the output from this command:

SLB Failover Configuration:
  Failover: Enabled
  Local unit ID: 1
  Local IP address: 10.1.1.1
  Remote IP address: 10.1.1.2
  TCP port number: 1028
  Remote Alive frequency: 1
  Remote Dead frequency: 2
  Keepalive Timeout: 3
  Ping check: Disabled
  Ping check IP address: 0.0.0.0
  Ping frequency: 1
  Ping timeout: 3
  Manual failback: Disabled
#
#
SLB Failover Status: Running
  Units active in local SLB: 2
  Units active in or requested by remote SLB: None
  Send connection: Down
  Receive connection: Down
  Ping check: Not Running

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on all “i” series platforms.
show slb global

show slb global

Description
Displays the current SLB global configuration information.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Displays the following:
- Global enable/disable mode
- Global modes
- Default settings for health checker
- Failover configuration

Example
The following command displays the current SLB global configuration information:

show slb global

Following is the output from this command:

SLB: Enabled
SynGuard: Disabled
3DNS IQuery Support Status: Disabled
SLB persist-level: same-vip-same-port
SLB persistence-method: per-session
SLB pre-allocated connection-block size: 10000
SLB connection timeout: 1
SLB persistence on client proxies: Disabled
Proxy Client Persistence entries: No. of Proxy Client Persistence entries: 0
#
#
Health Check Defaults:
Ping-check Frequency: 10 Timeout: 30
Port-check Frequency: 30 Timeout: 90
Service-check Frequency: 60 Timeout: 180
HTTPURL: "/"
    Match String: (any-content)
FTPUser: anonymous
    Password: (not shown)
TelnetUser: anonymous
Password: (not shown)
SMTPDomain: "mydomain.com"
    NNTP Newsgroup: "ebusiness"
    User: anonymous
    Password: (not shown)
POP3User: anonymous
    Password: (not shown)
#
#
SLB Failover Configuration:
Failover: Enabled
Local unit ID: 1
Local IP address: 10.1.1.1
Remote IP address: 10.1.1.2
TCP port number: 1028
Remote Alive frequency: 1
Remote Dead frequency: 2
Keepalive Timeout: 3
Ping check: Disabled
Ping check IP address: 0.0.0.0
Ping frequency: 1
Ping timeout: 3
Manual failback: Disabled
#
#
SLB Failover Status: Running
Units active in local SLB: 2
Units active in or requested by remote SLB: None
Send connection: Down
Receive connection: Down
Ping check: Not Running

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb gogo-mode

show slb gogo-mode <port number> {configuration}

Description
Displays GoGo mode ping check, TCP port check, and service check status.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>configuration</td>
<td>Displays configuration instead of status.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a master port, status is displayed for all GoGo mode groups with health checks configured.

Example
The following command displays the current GoGo mode health check configuration for the group with port 29 as the master port:

test:~# show slb gogo-mode 29 configuration

The following command displays the current GoGO mode health check configuration for all groups.

test:~# show slb gogo-mode
No SLB GoGo mode Health Check configured.

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
show slb L4-port

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ftp</td>
<td>Specifies an FTP port.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP port.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS port.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 port.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP port.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP port.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 port.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies a SMTP port.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS port.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet port.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP port.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web port.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www port</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

If you do not specify a port, configuration and status for all layer 4 ports is displayed.

Example

The following command displays the current layer 4 port configuration:

```
show slb L4-port
```

Following is the output from this command:

```
Port: 80 Enabled TCP idle timeout (treaper): 600 UDP idle timeout: 600
```
Platform Availability

This command is available on all “i” series platforms.
show slb node

show slb node {<ip address> [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]]}

Description
Displays node configuration and status.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP node.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP node.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS node.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 node.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP node.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP node.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 node.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP node.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS node.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet node.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP node.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web node.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www node</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the node.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a node, status for all nodes is displayed.

Example
The following command displays the current node configuration and statistics for all nodes:

```
show slb node
```

Following is the output from this command:

```
Node IP Address | IP Flags | Freq/Timeout | TCP/UDP Port | Flags | Frequency/Max Timeout#PoolsConns
-----------------|----------|--------------|--------------|-------|-------------------|
1.111.1.1        | E--H--   | 10/30        | 80           | E---  | 30/902 (no limit) |
1.111.1.2        | E--H--   | 10/30        | 80           | E---  | 30/902 (no limit) |
1.111.1.3        | E--H--   | 10/30        | 80           | E---  | 30/902 (no limit) |
```
show slb node

Flags: E - Enable,   U - Up,   R - IP Route Up,   H - Health check enabled,
P - Health check passed,   ! - VLAN not configured with "slb-type"

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb persistence

show slb persistence

Description
Displays persistence status of existing clients.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays the current persistence status:

show slb persistence

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb pool

    show slb pool <pool name>

Description
Displays the current SLB pool configuration and status.

Syntax Description

| pool name | Specifies a pool. |

Default
N/A

Usage Guidelines
If you do not specify a pool, configuration and status for all pools is displayed.

Example
The following command displays the current pool configuration and statistics for all pools, currently “rr_pool” and “ratio_pool”:

```
show slb pool
```

Following is the output from this command:

<table>
<thead>
<tr>
<th>Name</th>
<th>IP</th>
<th>TCP/UDP</th>
<th>Ratio/</th>
<th>Flags</th>
<th>Port</th>
<th>Flags</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>IP</td>
<td>Flags</td>
<td></td>
<td></td>
<td>Port</td>
<td>Flags</td>
<td>Priority</td>
</tr>
<tr>
<td>rr_pool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.111.1.1</td>
<td>E--H--</td>
<td>80</td>
<td>E---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.111.1.2</td>
<td>E--H--</td>
<td>80</td>
<td>E---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.111.1.3</td>
<td>E--H--</td>
<td>80</td>
<td>E---</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ratio_pool</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.111.1.1</td>
<td>E--H--</td>
<td>80</td>
<td>E---</td>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.111.1.2</td>
<td>E--H--</td>
<td>80</td>
<td>E---</td>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1.111.1.1</td>
<td>E--H--</td>
<td>80</td>
<td>E---</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flags: E - Enable, U - Up, R - IP Route Up, H - Health check enabled, P - Health check passed, ! - VLAN not configured with 'slb-type'

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb stats

    show slb stats [pool <pool name> | vip <vip name>]

Description
Displays the current SLB pool connection status.

Syntax Description

<table>
<thead>
<tr>
<th>pool name</th>
<th>Specifies a pool.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you specify pool but do not specify a specific pool, status for all pools is displayed.
If you specify vip but do not specify a specific virtual server, status for all virtual servers is displayed.
If you do not specify a pool or virtual server, status for all pools and virtual servers is displayed.

Example
The following command displays the current pool connection status for all pools:
show slb stats pool

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
show slb vip

show slb vip [<vip name> | ipaddress <ip address> : [ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <TCP or UDP port number>]] {detail}

Description
Displays the current virtual server configuration and statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies an FTP virtual server.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies an HTTP virtual server.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies an HTTPS virtual server.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies an IMAP4 virtual server.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies an LDAP virtual server.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies an NNTP virtual server.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies a POP3 virtual server.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies an SMTP virtual server.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies a SOCKS virtual server.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies a telnet virtual server.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies a TFTP virtual server.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies a Web virtual server.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies any port associated with a wildcard server.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies a www virtual server</td>
</tr>
<tr>
<td>TCP or UDP port number</td>
<td>Specifies a TCP or UDP port for the virtual server.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a virtual server or IP address, information on all virtual servers is displayed.

Example
The following command displays the current virtual server configuration and statistics for all virtual servers; in this example they are named ratio_vip and rr_vip:

show slb vip

Following is the output from this command:

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Address</th>
<th>Port -- Mode --</th>
<th>Flags</th>
<th>Pool</th>
<th>Up/Defined</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
SLB Commands—“i” Series Switches Only

ratio_vip 4.1.1.100 80 1 TL SR EUA-----ratio_po0/3
rr_vip 10.1.1.10 80 1 TP PA EUA----!rr_pool0/3

Modes: TP - Transparent,  TL - Translational,  PT - Port Translational
Automatically Exported via: PA - Proxy Arp, HR - Host Route, SR - Subnet Route
Flags: E - Enable,  U - Up,  A - Active Unit,  H - Health-Check Enabled,
P - Persistence,  S - Sticky,  R - SvcDown-Reset,
! - VLAN has not been configured with "slb-type"

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
unconfigure slb all

unconfigure slb all

Description
Resets SLB global defaults and clears the SLB configuration.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command does not delete nodes, pools, or virtual servers. To delete all nodes and pools, use the following command:
delete slb pool all

To delete all virtual servers, use the following command:
delete slb vip all

Example
The following command resets SLB global defaults and clears the SLB configuration:
unconfigure slb all

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
unconfigure slb gogo-mode health-check

    unconfigure slb gogo-mode <port number> health-check

**Description**

Disables and deletes all the ping check, TCP port check, and service check configurations for this GoGo mode group.

**Syntax Description**

<table>
<thead>
<tr>
<th>port number</th>
<th>Specifies the GoGo mode master port.</th>
</tr>
</thead>
</table>

**Default**

N/A

**Usage Guidelines**

None

**Example**

The following command deletes all health-check configurations for the GoGo mode group with port 29 as the master port:

`unconfigure slb gogo-mode 29 health-check`

**History**

This command was first available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on all “i” series platforms.
unconfigure slb gogo-mode service-check

unconfigure slb gogo-mode <port number> service-check [all | ftp | http | nntp | pop3 | smtp | telnet | <TCP port number>]

Description
Disables and deletes the GoGo mode service check configuration.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies the GoGo mode master port.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all service checks.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies the FTP service check.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies the HTTP service check.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies the NNTP service check.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies the POP3 service check.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies the SMTP service check.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies the telnet service check.</td>
</tr>
<tr>
<td>TCP port number</td>
<td>Specifies the TCP port, instead of the service.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command disables and deletes all the FTP service check configuration for the GoGo mode group with port 29 as the master port:

```
unconfigure slb gogo-mode 29 service-check ftp
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on all “i” series platforms.
unconfigure slb vip service-check

unconfigure slb vip [all | <vip name>] service-check

Description
Disables and deletes the service check configuration.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all virtual servers.</td>
</tr>
<tr>
<td>vip name</td>
<td>Specifies a virtual server.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command disables and deletes the FTP service-check configurations for the virtual server named ftp_vip:

unconfigure slb vip ftp_vip service-check

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all “i” series platforms.
This chapter describes commands for:

- Configuring and managing the Event Management System and logging
- Enabling and disabling NetFlow flow statistics collection ("i" series platforms only)
- Configuring flow-collection port and filtering options ("i" series platforms only)
- Configuring the flow-collector devices to which NetFlow datagrams are exported ("i" series platforms only)
- Enabling, disabling, and configuring sFlow® statistics collection ("i" series platforms only)

When an event occurs on a switch, the Event Management System (EMS) allows you to send messages generated by these events to a specified log target. You can send messages to the memory buffer, NVRAM, the console display, the current session, or to a syslog host. The log messages contain configuration and fault information pertaining to the device. The log messages can be formatted to contain various items of information, but typically a message will consist of:

- Timestamp—The time when the event occurred.
- Severity level:
  - Critical—A desired switch function is inoperable. The switch may need to be reset.
  - Error—A problem is interfering with normal operation.
  - Warning—An abnormal condition exists that may lead to a function failure.
  - Notice—A normal but significant condition has been detected; the system is functioning as expected.
  - Info—Actions and events are occurring consistent with expected behavior.
  - Debug-Summary, Debug-Verbose, and Debug-Data—These provide information that is useful when performing detailed trouble shooting procedures.

By default, log entries that are assigned a critical, error, or warning level are considered static entries and remain in the NVRAM log target after a switch reboot.

- Component: The component refers to the specific functional area to which the error refers.
- Message: The message contains the log information with text that is specific to the problem.

The switch maintains a configurable number of messages in its internal (memory-buffer) log (1000 by default). You can display a snapshot of the log at any time. In addition to viewing a snapshot of the log, you can configure the system to maintain a running real-time display of log messages on the console.
display or telnet session. In addition to maintaining an internal log, the switch supports remote logging by way of the UNIX syslog host facility.

**NetFlow Statistics—“i” Series Platforms Only**

NetFlow flow statistics provide a way for a switch to capture and export traffic classification or precedence information as data traverses, or flows across, portions of a network. A network flow is defined as a unidirectional sequence of packets between a particular source device and destination device that share the same protocol and transport-layer information. Flows are defined by the combination of their source IP address, destination IP address, source port, destination port, and protocol type.

NetFlow records are unidirectional in nature, which means that two flow records are maintained for a typical TCP connection: one record for flow in the ingress direction, and a second for the flow in the egress direction. Records are maintained only for TCP and UDP flows. Flow records are grouped together into UDP datagrams for export to a flow-collector device. A NetFlow Version 1 export datagram can contain up to 25 flow records.

The IP addresses (or hostnames) and UDP port numbers of the available flow collectors can be configured on a per-switch basis. The ExtremeWare NetFlow implementation also enables a single port to distribute statistics across multiple groups of flow-collector devices. The NetFlow distribution feature is enabled by configuring export distribution groups that contain the addresses of multiple flow-collector devices. The feature uses a distribution algorithm that ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that the flow records of the ingress direction of a TCP or UDP connection are exported to the same collector. For Ethernet applications, only ingress traffic is monitored on Ethernet ports.

By default, each Ethernet port configured for flow switching maintains statistics for all the flows traversing the link in the ingress direction. Generalized filtering options exist that enable you to configure an Ethernet port to maintain statistics selectively for only those flows that match a specified filter. Up to eight filters are supported for each Ethernet port, with a total of 128 filters possible per each I/O module.

---

**NOTE**

Some of the NetFlow commands are implemented differently in the version of ExtremeWare that supports the PoS module, than in ExtremeWare 6.2 or later. Commands or options unique to the PoS module are indicated in the comments, or are documented separately in Chapter 22.

**sFlow® Statistics—“i” Series Platforms Only**

sFlow® is a technology for monitoring traffic in data networks containing switches and routers. It relies on statistical sampling of packets from high-speed networks, plus periodic gathering of the statistics. A UDP datagram format is defined to send the information to an external entity for analysis. sFlow consists of a MIB and a specification of the packet format for forwarding information to a remote agent. Details of sFlow specifications can be found in RFC 3176 and at the following website:

http://www.sflow.org

sFlow is primarily a mechanism that statistically samples a small portion of the traffic from a network, and extrapolate from this small sample to infer information about the network as a whole. sFlow defines a packet format, where the sFlow Agent in ExtremeWare collects information from a number of sampled packets in addition to snapshots of various counters and statistics. The UDP frame is forwarded to a central monitoring station referred to as the sFlow collector.
clear counters

Description
Clears all switch statistics and port counters, including port packet statistics, bridging statistics, IP statistics, log event counters, and MPLS statistics.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
You should view the switch statistics and port counters before you clear them. Use the show port command to view port statistics. Use the show log counters command to show event statistics.

Viewing and maintaining statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. By clearing the counters, you can see fresh statistics for the time period you are monitoring.

Example
The following command clears all switch statistics and port counters:
clear counters

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
clear log

For the “i” series switches:

```
clear log {diag-status | error-led | static | messages [memory-buffer | nvram]}
```

For the “e” series switches:

```
clear log {diag-status | static | messages [memory-buffer | nvram]}
```

Description
Cleans the log database.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diag-status</td>
<td>Clears the hardware error code.</td>
</tr>
<tr>
<td>error-led</td>
<td>Clears the ERR LED on the MSM.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies that the messages in the NVRAM target are cleared, and the ERR LED on the MSM is cleared (on platforms with the MSM).</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Clears entries from the memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Clears entries from NVRAM.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

The switch log tracks configuration and fault information pertaining to the device.

By default, log entries that are sent to the NVRAM remain in the log after a switch reboot. The `clear log` and `clear log messages memory-buffer` commands remove entries in the memory buffer target; the `clear log static` and `clear log messages nvram` commands remove messages from the NVRAM target as well as the memory buffer target.

When there is a hardware failure, a hardware error code might be saved to the FLASH or NVRAM (depending on the switch configuration). Upon reboot, the switch will not try to bring up a module with an error code, so it will be shown in a failed state. Use the `clear log diag-status` command to clear the hardware error code, so the module can be brought up after the next reboot. This command clears the state for all the modules.

For the BlackDiamond Switches. There are three ways to clear the ERR LED on the MSM for the BlackDiamond switches: Clear the log, reboot the switch, or use the `clear log error-led` command. To clear the ERR LED without rebooting the switch or clearing the log messages, use the `clear log error-led` command.
Example
The following command clears all log messages, from the NVRAM:

clear log static

History
This command was first available in ExtremeWare 2.0.
The `diag-status` option was added in ExtremeWare 7.0.0.
The `error-led` option was added in ExtremeWare 7.1.0.
The `messages` option was added in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
The `diag-status` and `messages` options were added in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
clear log counters

`clear log counters {<event condition> | [all | <event component>] {severity <severity> {only}}}`

**Description**

Clears the incident counters for events.

**Syntax Description**

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event condition</td>
<td>Specifies the event condition counter to clear.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all events counters are to be cleared.</td>
</tr>
<tr>
<td>event component</td>
<td>Specifies that all the event counters associated with a particular component should be cleared.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level of event counters to clear (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only event counters of the specified severity level are to be cleared.</td>
</tr>
</tbody>
</table>

**Default**

If severity is not specified, then the event counters of any severity are cleared in the specified component.

**Usage Guidelines**

This command sets the incident counters to zero for each event specified. To display event counters, use the following command:

```
show log counters
```

See the command `show log` on page 775 for more information about severity levels.

To get a listing of the event conditions in the system, use the following command:

```
show log events {detail}
```

To get a listing of the components present in the system, use the following command:

```
show log components
```

**Example**

The following command clears the event counters for event conditions of severity error or greater in the component BGP on an “i” series switch:

```
clear log counters "BGP" severity error
```
History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
clear log diag error

clear log diag error <slot number>

Description
Clears the Alpine diagnostics failures from the NVRAM.

NOTE
This command is supported only on the Alpine switches.

Syntax Description

| slot number | Specifies the slot where the I/O module is installed. |

Default
N/A

Usage Guidelines
Use this command only at the direction of Extreme Networks personnel. Extreme Networks support personnel can clear the Alpine diagnostics failures from the NVRAM using the following command:

```
clear log diag error <slot number>
```

Example
The following command clears the Alpine diagnostics failures from the NVRAM for the module in slot 4:

```
clear log diag remap 4
```

History
This command was first available in ExtremeWare 7.2.0b25.

Platform Availability
This command is available only on the Alpine switches.
clear log diag remap

clear log diag remap <slot number>

Description
Clears the packet memory diagnostics failures from the EEPROM.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| slot number | Specifies the slot where the I/O module is installed. |

Default
N/A

Usage Guidelines
Use this command only at the direction of Extreme Networks personnel. Extreme Networks support personnel can clear the packet memory diagnostics failures from the EEPROM using the following command:

clear log diag remap <slot number>

This command clears any error remapping.

Example
The following command clears the packet memory diagnostics failures from the EEPROM for the module in slot 5:

clear log diag remap 5

History
This command was first available in ExtremeWare 7.2.0b25.

Platform Availability
This command is available only on the “i” series platforms.
clear transceiver-test

    clear transceiver-test

Description
Clears (resets) the transceiver test statistics.

NOTE
This command is available only on the “i” series modular switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
To display the transceiver test statistics, use the show diagnostics sys-health-check command. The following is sample output:

Transceiver system health diag result
Pass/Fail Counters Are in HEX
Slot  Cardtype Cardstate   Test        Pass     Fail Time_last_fail
----    -------- ---------   ----    -------- -------- --------------
slot 1  Unknown
slot 2  Unknown
slot 3  FM8V     Operational MAC        2b81b        0
slot 4  GM4X     Operational MAC        2b81b        0
BPLNE   SMMI     Operational UART       2b81a        0
BPLNE   SMMI     Operational FLASH      2b81a        0
BPLNE   SMMI     Operational SRAM       2b81a        0
BPLNE   SMMI     Operational NVRAM      2b81a        0
BPLNE   SMMI     Operational ENET       2b81a        0
BPLNE   Basbrd   Operational QUAKE      2b81a        0
BPLNE   Basbrd   Operational TWISTER    2b81a        0

Example
The following command clears (resets) all of the transceiver test statistics:

    clear transceiver-test

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.
Platform Availability
This command is available on “i” series modular switches only.
configure flowstats export add port

configure flowstats export <group#> add [<ipaddress> | <hostname>] <udp_port>

Description
Adds a flow-collector device to an export group to which NetFlow datagrams are exported.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the export group to which the specified flow-collector device should be added. The group number is an integer in the range of 1-32.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of a flow-collector destination.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of a flow-collector destination.</td>
</tr>
<tr>
<td>udp_port</td>
<td>Specifies a UDP port for the destination flow-collector.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You can configure up to 32 export distribution groups. Each group may contain up to eight flow-collection devices. At least one flow-collector destination must be configured for NetFlow datagrams to be exported to a group.

When multiple flow collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations. This NetFlow-distribution feature enables a scalable collection architecture that is able to accommodate high volumes of exported data. The distribution algorithm ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that flow records for both the ingress and egress directions of a TCP or UDP connection are exported to the same collector (when both flows traverse the same link and both filters are configured to export to the same group).

Issuing this command also enables the collection of NetFlow statistics.

For the BlackDiamond Switches. See Chapter 22 for information about a similar command for the PoS module.

Example
The following command adds the flow-collector device with IP address 10.205.30.15 using UDP port 2025 to export group 5 for this switch:

configure flowstats export 5 add 10.205.30.15 2025
History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available only on the “i” series platforms.
configure flowstats export delete port

configure flowstats export <group#> delete [<ipaddress> | <hostname>] <udp_port>

Description
Removes a flow-collector device from an export group to which NetFlow datagrams are exported.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| group# | Specifies the export group to which the specified flow-collector device belongs. The group number is an integer in the range of 1-32. |
| ipaddress | Specifies the IP address of the flow-collector destination. |
| hostname | Specifies the host name of the flow-collector destination. |
| udp_port | Specifies a UDP port of the destination flow-collector. |

Default
N/A

Usage Guidelines

For the BlackDiamond Switches. See Chapter 22 for information about a similar command for the PoS module.

Example
The following command removes the flow-collector device with IP address 10.205.30.15 using UDP port 2025 from export group 5 on this switch:
configure flowstats export 5 delete 10.205.30.15 2025

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available only on the “i” series platforms.
configure flowstats filter ports

configure flowstats filter <filter#> {aggregation} {export <group#>} ports <portlist> [ingress | egress] <filterspec>

Description

Configures a flow record filter for the specified ports.

NOTE

This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter#</td>
<td>The filter# parameter is an integer in the range from 1 to 8 that identifies the filter being defined.</td>
</tr>
<tr>
<td>&lt;group#&gt;</td>
<td>Specifies the group number that identifies the set of flow collector devices to which records for flows matching the filter are to be exported. If Group is not specified, then group # 1 will be used as default export group.</td>
</tr>
<tr>
<td>aggregation</td>
<td>To reduce the volume of exported data, use this optional keyword to maintain a single set of statistics for all the flows that match the specified filter.</td>
</tr>
</tbody>
</table>
| filterspec | Specifies a set of five parameters (four are value/mask pairs) that define the criteria by which a flow is evaluated to determine if it should be exported. The parameters are:

- [(dest-ip <ipaddress_value/mask ipaddress_filtermask>) (source-ip <ipaddress_value/mask ipaddress_filtermask>) (dest-port <port_value/port_filtermask>) (source-port <port_value/port_filtermask>) (protocol <tcp/udp/ip/protocol_value/protocol_filtermask>) | match-all-flows | match-no-flows]

All five specifications must be included in the order specified.

The range for port/port_mask is calculated using the following formula:

\[
\text{minport} = \text{port}, \quad \text{maxport} = 2^{(32-\text{port mask})} - 1.
\]

match-all-flows specifies that the filter should match any flow.

match-no-flows specifies that the filter should discard all flow. This option is not valid for Ethernet modules.

egress | Specifies that the filter should capture only egress traffic. This option is not valid for Ethernet modules.

ingress | Specifies that the filter should capture only ingress traffic.

Default

N/A

Usage Guidelines

Configuring a filter specification enables that filter for the specified ports. To specify all ports, you can specify them as the range of all ports (such as 1-32 or 7:1-7:4) or in the form <slot>:* on a modular switch.
Each Ethernet port supports up to eight filters for ingress flows.

Conceptually, the filters work by ANDing the contents of each of the five components of a forwarded flow with the associated masks from the first defined filter (filter #1). Statistics are maintained if the results of the AND operations match the configured filter values for all fields of the sequence. If there is no match, then the operation is repeated for filter #2, and so on. If there is no match for any of the filters, then statistics are not maintained for the flow. Filters for any or all of the sequence components can be configured with a single command.

**Examples**

The following command example configures filter 2 to collect aggregate statistics for all traffic flowing through ports 1-8 from the 192.170.0.0/16 subnet to the 192.171.132.0/24 subnet:

```
configure flowstats filter 2 aggregation export 1 ports 1-8 ingress dest-ip 192.171.132.0/24 source-ip 192.170.0.0/16 dest-port 0/0 source-port 0/0 protocol ip
```

The following command configures filter 3 to collect statistics on any flows for ports 4-32 that did not match the filters defined in filters 1 and 2:

```
configure flowstats filter 3 aggregation export 1 ports 4-32 ingress match-all-flows
```

**History**

This command was first available in ExtremeWare 6.2.

**Platform Availability**

This command is available only on the “i” series platforms.
configure flowstats source

    configure flowstats source ipaddress <ipaddress>

Description
Configures the IP address that is to be used as the source IP address for NetFlow datagrams to be exported.

NOTE
This command is available only on the "i" series switches.

Syntax Description

| ipaddress | Specifies the IP address of a VLAN to be used as the source address for the NetFlow datagrams. |

Default
Uses the IP address of the VLAN that has the default route to the flow-collector device.

Usage Guidelines
The IP address must have a route to the flow-collector device.

Example
The following command specifies that IP address 198.168.100.1 is the source:
configure flowstats source ipaddress 198.168.100.1

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available only on the “i” series platforms.
configure flowstats timeout ports

configure flowstats timeout <minutes> ports [<portlist> | all]

Description
Configures the timeout value for flow records on the specified ports.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>Specifies the number of minutes to use in deciding when to export flow records. The default is five minutes.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports to which the timeout applies. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>indicates that the timeout should be set for all ports on this switch.</td>
</tr>
</tbody>
</table>

NOTE: The parameter any is not supported for the PoS module.

Default
Five minutes

Usage Guidelines
The timeout is used to export flow records on an age basis. All flow records are examined at least once every 30 minutes. If the age of the flow record is greater than the configured timeout, the record is exported. If the flow is still active, a new flow record will be created when the next packet arrives.

For the PoS module, the minutes parameter is an integer in the range [1-1440].

Example
The following command configures a timeout value of 15 minutes for ports 1-8:

configure flowstats timeout 15 ports 1-8

This means that flow records for these ports will be exported after they have aged 15 minutes.

History
This command was first available in ExtremeWare 6.1.5b20 for the PoS module only.

This command was first available in ExtremeWare 6.2 for all “i” series platforms.

Platform Availability
This command is available only on the “i” series platforms.
configure log display

    configure log display {<severity>}

**Description**

Configures the real-time log display.

**Syntax Description**

```plaintext
severity  Specifies a message severity. Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.
```

**Default**

If not specified, messages of all severities are displayed on the console display.

**Usage Guidelines**

You must enable the log display before messages are displayed on the log display. Use the `enable log display` command to enable the log display. This allows you to configure the system to maintain a running real-time display of log messages on the console.

Options for displaying the real-time log display include:

- **severity**—Filters the log to display messages with the selected severity or higher (more critical). Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.

In ExtremeWare 7.1.0, the ability to control logging to different targets was introduced. The new command equivalent to `configure log display` is the following:

```
configure log target console-display severity <severity>
```

To display the current configuration of the log display, use the following command:

```
show log configuration target console-display
```

**Example**

The following command configures the system log to maintain a running real-time display of log messages of critical severity:

```
configure log display critical
```

**History**

This command was first available in ExtremeWare 2.0.

The severity levels alert and emergency were deprecated to critical, and the levels debug-summary, debug-verbose, and debug-data were added in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
configure log filter events

configure log filter <filter name> [add | delete] {exclude} events [<event condition> | [all | <event component>] {severity <severity> {only}}]

Description
Configures a log filter by adding or deleting a specified set of events.

Syntax Description

<table>
<thead>
<tr>
<th>filter name</th>
<th>Specifies the filter to configure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Add the specified events to the filter</td>
</tr>
<tr>
<td>delete</td>
<td>Remove the specified events from the filter</td>
</tr>
<tr>
<td>exclude</td>
<td>Events matching the specified events will be excluded</td>
</tr>
<tr>
<td>event condition</td>
<td>Specifies an individual event.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all components and subcomponents.</td>
</tr>
<tr>
<td>event component</td>
<td>Specifies all the events associated with a particular component.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level of events (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies only events of the specified severity level.</td>
</tr>
</tbody>
</table>

Default
If the exclude keyword is not used, the events will be included by the filter. If severity is not specified, then the filter uses the default severity threshold for the component (see the note on page 676 when delete or exclude is specified).

Usage Guidelines
This command controls the incidents that pass a filter by adding or deleting a specified set of events. If you want to configure a filter to include or exclude incidents based on event parameter values (for example, MAC address or BGP Neighbor) see the command configure log filter events match on page 678.

When the add keyword is used, the specified event name, or set of events described by component and severity value, is added to the beginning of the filter item list maintained for this filter. The new filter item either includes the events specified or, if the exclude keyword is present, excludes the events specified.

The delete keyword is used to remove events from the filter item list that were previously added using the add command. All filter items currently in the filter item list that are identical to, or a subset of, the set of events specified in the delete command will be removed.

Event Filtering Process. From a logical standpoint, the filter associated with each enabled log target is examined to determine whether a message should be logged to that particular target. The determination is made for a given filter by comparing the incident with the most recently configured filter item first. If the incident matches this filter item, the incident is either included or excluded,
depending on whether the `exclude` keyword was used. Subsequent filter items on the list are compared
if necessary. If the list of filter items has been exhausted with no match, the incident is excluded.

**Events, Components, and Subcomponents.** As mentioned, a single event can be included or
excluded by specifying the event’s name. Multiple events can be added or removed by specifying an
ExtremeWare component name plus an optional severity. Some components, such as BGP, contain
subcomponents, such as Keepalive, which is specified as BGP.Keepalive. (BGP is supported only on the
“i” series switches.) Either components or subcomponents can be specified. The keyword `all` in place of
a component name can be used to indicate all ExtremeWare components.

**Severity Levels.** When an individual event name is specified following the `events` keyword, no
severity value is needed since each event has pre-assigned severity. When a component, subcomponent,
or the `all` keyword is specified following the `events` keyword, a severity value is optional. If no
severity is specified, the severity used for each applicable subcomponent is obtained from the
pre-assigned severity threshold levels for those subcomponents. For example, if STP is specified as the
component, and no severity is specified, then only messages with severity of `error` and greater are
passed, since the threshold severity for the STP component is `error`. If STP.InBPDU is specified as the
component, and no severity is specified, then only messages with severity of `warning` and greater are
passed, since the threshold severity for the STP.InPBDU subcomponent is `warning`. Use the `show log
components` command to see this information.

The severity keyword `all` can be used as a convenience when `delete` or `exclude` is specified. The use
of `delete` (or `exclude`) with severity `all` deletes (or excludes) previously added events of the same
component of all severity values.

**NOTE**

*If no severity is specified when delete or exclude is specified, severity all is used*

If the keyword `only` is present following the severity value, then only the events in the specified
component at that exact severity are included. Without the `only` keyword, events in the specified
component at that severity or more urgent are included. For example, using the option `severity
warning` implies critical, error, or warning events, whereas the option `severity warning only` implies
warning events only. Severity `all only` is not a valid choice.

EMS events with severity `debug-summary`, `debug-verbose`, or `debug-data` will not be logged unless
debug mode is enabled.

**Filter Optimization.** Each time a `configure log filter` command is issued for a given filter name,
the events specified are compared against the current configuration of the filter to try to logically
simplify the configuration.

For example, if the command:

```
configure log filter bgpFilter1 add events bgp.keepalive severity error only
```

were to be followed by the command:

```
configure log filter bgpFilter1 add events bgp severity info
```

the filter item in the first command is automatically deleted since all events in the `BGP.Keepalive`
subcomponent at severity `error` would be also included as part of the second command, making the
first command redundant.
As another example, a new exclude filter item may not need to be added if no current include filter items contain any of the events described in the exclude statement. To illustrate, suppose a new filter were created and configured as follows:

```
create log filter myFilter
configure log filter myFilter add events bgp.keepalive severity error only
```

then the following exclude item actually results in no change to the filter item list:

```
configure log filter myFilter add exclude events bgp.updatein severity all
```

Since the newly created filter called `myFilter` only includes some items from the subcomponent BGP.Keepalive, there are no BGP.UpdateIn events that need to be excluded.

**More Information.** See the command `show log` on page 775 for more information about severity levels.

To see a list of the components present in the system, use the following command:

```
show log components
```

To see a list of event condition definitions, use the following command:

```
show log events
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

**Example**

The following command adds all events in the STP.InBPDU component at severity `info` to the filter called `mySTPFilter`:

```
configure log filter mySTPFilter add events stp.inbpdu severity info
```

The following command adds events in the STP.OutBPDU component, at the pre-defined severity level for that component, to the filter `mySTpFilter`:

```
configure log filter mySTpFilter add events stp.outbpdu
```

The following command excludes one particular event, STP.InBPDU.Drop, from the filter:

```
configure log filter mySTpFilter add exclude events stp.inbpdu.drop
```

**History**

This command was first available in ExtremeWare 7.1.0.  
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure log filter events match

configure log filter <filter name> [add | delete] {exclude} events [<event condition>] | [all | <event component>] {severity <severity> {only}}] [match | strict-match] <type> <value> {and <type> <value> ...}

Description
Configures a log filter by adding or deleting a specified set of events and specific set of match parameter values.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter name</td>
<td>Specifies the filter to configure.</td>
</tr>
<tr>
<td>add</td>
<td>Adds the specified events to the filter.</td>
</tr>
<tr>
<td>delete</td>
<td>Removes the specified events from the filter.</td>
</tr>
<tr>
<td>exclude</td>
<td>Excludes events matching the filter.</td>
</tr>
<tr>
<td>event condition</td>
<td>Specifies the event condition.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all events.</td>
</tr>
<tr>
<td>event component</td>
<td>Specifies all the events associated with a particular component.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level of events (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies only events of the specified severity level.</td>
</tr>
<tr>
<td>match</td>
<td>Specifies events whose parameter values match the &lt;type&gt; &lt;value&gt; pair.</td>
</tr>
<tr>
<td>strict-match</td>
<td>Specifies events whose parameter values match the &lt;type&gt; &lt;value&gt; pair, and possess all the parameters specified.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the type of parameter to match</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the value of the parameter to match</td>
</tr>
<tr>
<td>and</td>
<td>Specifies additional &lt;type&gt; &lt;value&gt; pairs that must be matched</td>
</tr>
</tbody>
</table>

Default
If the exclude keyword is not used, the events will be included by the filter. If severity is not specified, then the filter will use the component default severity threshold (see the note on on page 676 when delete or exclude is specified).

Usage Guidelines
This command controls the incidents that pass a filter by adding or deleting a specified set of events that match a list of <type> <value> pairs. This command is an extension of the command configure log filter events, and adds the ability to filter incidents based on matching specified event parameter values to the event.

See the configure log filter events command on page 675 for more information about specifying and using filters, event conditions and components, and the details of the filtering process. The discussion here is about the concepts of matching <type> <value> pairs to more narrowly define filters.

Types and Values. Each event in ExtremeWare is defined with a message format and zero or more parameter types. The show log events detail command on page 788 can be used to display event
definitions (the event text and parameter types). The syntax for the parameter types (represented by <type> in the command syntax above) is:

```
[bgp [neighbor | routerid] <ip address>
| eaps <eaps domain name>
| {destination | source} [ipaddress <ip address> | L4-port | mac-address ]
| {egress | ingress} [slot <slot number> | ports <portlist>]
| netmask <netmask>
| number <number>
| string <match expression>
| vlan <vlan name>
| vlan tag <vlan tag>]
```

The <value> depends on the parameter type specified. As an example, an event may contain a physical port number, a source MAC address, and a destination MAC address. To allow only those incidents with a specific source MAC address, use the following command:

```
configure log filter myFilter add events bridge severity notice match source
mac-address 00:01:30:23:C1:00
```

The string type is used to match a specific string value of an event parameter, such as a user name. A string can be specified as a simple regular expression.

**Match Versus Strict-Match.** The `match` and `strict-match` keywords control the filter behavior for incidents whose event definition does not contain all the parameters specified in a `configure log filter events match` command. This is best explained with an example. Suppose an event in the XYZ component, named `XYZ.event5`, contains a physical port number, a source MAC address, but no destination MAC address. If you configure a filter to match a source MAC address and a destination MAC address, `XYZ.event5` will match the filter when the source MAC address matches regardless of the destination MAC address, since the event contains no destination MAC address. If you specify the `strict-match` keyword, then the filter will never match, since `XYZ.event5` does not contain the destination MAC address.

In other words, if the `match` keyword is specified, an incident will pass a filter so long as all parameter values in the incident match those in the match criteria, but all parameter types in the match criteria need not be present in the event definition.

The ExtremeWare CLI exposes the keywords `match`, `strict-match`, and individual parameter types only when they are valid given the set of events specified in the command. This behavior guides you to form more meaningful filter match criteria. For example, a MAC address is not used to match BGP events where MAC address parameters are not present.

**and Keyword.** Use the `and` keyword to specify multiple parameter type/value pairs that must match those in the incident. For example, to allow only those events with specific source and destination MAC addresses, use the following command:

```
configure log filter myFilter add events bridge severity notice match source
mac-address 00:01:30:23:C1:00 and destination mac-address 01:80:C2:00:00:02
```
**Multiple Match Commands.** Multiple configure log add events match commands are logically ORed together. For example, the following commands define a filter that allows layer 2 bridging incidents with a source MAC address of one of three possible values:

create log filter bridgeFilter

configure log bridgeFilter add events bridge severity notice match source mac-address 00:11:12:13:14:15

configure log bridgeFilter add events bridge severity notice match source mac-address 00:21:22:23:24:25

configure log bridgeFilter add events bridge severity notice match source mac-address 00:31:32:33:34:35

In order to exclude only incidents whose parameter values match the specified criteria, follow this two-step process. First, include the applicable event(s) using either the configure log filter events command or the configure log filter events match command described here, with a superset of the match criteria. Second, use the exclude keyword in the configure log filter events match command to exclude incidents with the specified parameter values.

As an example, the following commands define a filter that allows incidents in the BGP.Keepalive component at severity notice or more severe, except those incidents containing a BGP neighbor in the 10.1.2.0/24 subnet:

create log filter bgpFilter

configure log bgpFilter add events bgp.keepalive severity notice

configure log bgpFilter add exclude events bgp.keepalive severity notice match bgp neighbor 10.1.2.0/24

**Filter Optimization.** As explained for the configure log filter events command, each time a configure log filter match command is issued, an attempt is made to logically simplify the configuration. This simplification extends to cases where one set of match criteria is a superset of another. For example, if you issued the following commands:

create log filter bgpFilter1

configure log bgpFilter1 add events bgp.event severity notice match bgp neighbor 10.0.0.0/8

configure log bgpFilter1 add events bgp.event severity notice match bgp neighbor 10.1.2.0/24 and L4-port 80

then the third command is redundant and no filter item is actually added. The reason is that the IP subnet 10.1.2.0/24 is wholly contained within the IP subnet 10.0.0.0/8, which is already included in this filter, and with any value for the layer 4 port.

**More Information.** See the command show log on page 775 for more information about severity levels.

To see a list of the components present in the system, use the following command:

show log components
To see a list of event condition definitions, use the following command:

```
show log events
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

**Example**

By default, all log targets are associated with the built-in filter called DefaultFilter. Therefore, the most straightforward way to send additional messages to a log target is to modify DefaultFilter. In the following example, the command modifies the built-in filter to allow incidents in the STP component, and all subcomponents of STP, of severity critical, error, warning, notice and info. For any of these events containing a physical port number as a match parameter, limit the incidents to only those occurring on physical ports 3, 4 and 5 on slot 1, and all ports on slot 2:

```
configure log DefaultFilter add events stp severity info match ports 1:3-1:5, 2:*
```

You can use the `unconfigure log DefaultFilter` command to restore the DefaultFilter back to its original configuration.

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure log filter set severity

configure log filter <filter name> set severity <severity> events
[<event component> | all ]

Description
Sets the severity level of an existing filter item.

Syntax Description

| filter name | Specifies the filter to configure. |
| severity    | Specifies the severity level to send. |
| event component | Specifies all the events associated with a particular component. |

Default

N/A

Usage Guidelines

This command modifies the severity level of an existing filter item describing a particular set of events. Using this command is equivalent to deleting the filter item from the filter and then adding back a filter item describing the same set of events with a different severity level. The command can only be used to modify a filter item referring to a set of events with a severity level, as opposed to one that makes use of only a single severity. It can be used to modify either “exclude” or “include” filter items.

For example, to change the severity level of the filter item added with this command:

configure log filter bgpFilter2 add events bgp.keepalive severity notice

use the following command:

configure log filter bgpFilter2 set severity info events bgp.keepalive

Using this single command is preferred to using a delete command followed by an add command:

configure log filter bgpFilter2 delete events bgp.keepalive
configure log filter bgpFilter2 add events bgp.keepalive severity info

Using the single command eliminates the possibility of missing an event of interest between the separate delete and add commands.

Note that the severity of a filter item configured to include or exclude incidents based on event parameter values (for example slot number) can also be modified using the configure log filter set severity match command on page 684.

See the show log command on page 775 for a detailed description of severity levels.

To see the current configuration of a target, use the following command:

show log configuration target
To see the current configuration of a filter, use the following command:

```
show log configuration filter
```

**Example**

To change the severity level of the filter item added with this command:

```
configure log filter bgpFilter2 add events bgp.keepalive severity notice
```

use the following command:

```
configure log filter bgpFilter2 set severity info events bgp.keepalive
```

**History**

This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure log filter set severity match

configure log filter <filter name> set severity <severity> events
[<event condition> | [all | <event component>]] [match | strict-match]
<type> <value> {and <type> <value> ...}

Description
Sets the severity level of an existing filter item.

Syntax Description

<table>
<thead>
<tr>
<th>filter name</th>
<th>Specifies the filter to configure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>severity</td>
<td>Specifies the severity level to send.</td>
</tr>
<tr>
<td>event component</td>
<td>Specifies all the events associated with a particular component.</td>
</tr>
<tr>
<td>only</td>
<td>Specifies only events of the specified severity level.</td>
</tr>
<tr>
<td>match</td>
<td>Specifies events whose parameter values match the &lt;type&gt; &lt;value&gt; pair.</td>
</tr>
<tr>
<td>strict-match</td>
<td>Specifies events whose parameter values match the &lt;type&gt; &lt;value&gt; pair, and possess all the parameters specified.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies the type of parameter to match.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the value of the parameter to match.</td>
</tr>
<tr>
<td>and</td>
<td>Specifies additional &lt;type&gt; &lt;value&gt; pairs that must be matched.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command modifies the severity level of an existing filter item describing a particular set of events and the parameter values of the desired events. Using this command is equivalent to deleting the filter item from the filter and then adding back a filter item describing the same set of events with a different severity level. The command can only be used to modify a filter item referring to a set of events with a severity level, as opposed to one that makes use of only a single severity. It can be used to modify either “exclude” or “include” filter items.

For example, to change the severity level of the filter item added with this command:

```
configure log slbFilter2 add exclude events slb.conn severity notice match
source ipaddress 10.1.2.0/24
```

use the following command:

```
configure log slbFilter2 set severity info events events slb.conn match
source ipaddress 10.1.2.0/24
```

Using this single command is preferred to using a delete command followed by an add command:

```
configure log slbFilter2 delete exclude events slb.conn severity notice match
source ipaddress 10.1.2.0/24
configure log slbFilter2 add exclude events slb.conn severity info match
```
source ipaddress 10.1.2.0/24

Using the single command eliminates the possibility of missing an event of interest between the separate delete and add commands.

See the command `show log` on page 775 for a detailed description of severity levels.

To see the current configuration of a target, use the following command:

```
show log configuration target {console-display | memory-buffer | nvram | session | syslog [<host name/ip> {: <udp-port>} [local0 ... local7]]}
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter <filter name>
```

**Example**

To change the severity level of the filter item added with this command:

```
configure log filter bgpFilter2 add events bgp.keepalive severity notice
```

use the following command:

```
configure log filter bgpFilter2 set severity info events bgp.keepalive
```

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure log target filter

configure log target [console-display | memory-buffer | nvram | session | syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]] filter <filter name> {severity <severity> {only}}

Description
Associates a filter to a target.

Syntax Description

<table>
<thead>
<tr>
<th>target</th>
<th>Specifies the device to send the log entries.</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog remote server.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
<tr>
<td>filter name</td>
<td>Specifies the filter to associate with the target.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level to send (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only the specified severity level is to be sent.</td>
</tr>
</tbody>
</table>

Default
If severity is not specified, the severity level for the target is left unchanged.

Usage Guidelines
This command associates the specified filter and severity with the specified target. A filter limits messages sent to a target.

Although each target can be configured with its own filter, by default all targets are associated with the built-in filter called DefaultFilter. Each target can also be configured with its own severity level. This provides the ability to associate multiple targets with the same filter, while having a configurable severity level for each target.

A message is sent to a target if the target has been enabled, the message passes the associated filter, the message is at least as severe as the configured severity level, and the message output matches the regular expression specified. By default, the memory buffer and the NVRAM targets are enabled. For other targets, use the command enable log target on page 754. Table 14 describes the default characteristics of each type of target.
**configure log target filter**

The built-in filter DefaultFilter and a severity level of *info* are used for each new telnet session. These values may be overridden on a per-session basis by using the `configure log target filter` command and specifying the target as *session*. Use the following form of the command for per-session configuration changes:

`configure log target session filter <filter name> {severity <severity> {only}}`

Configurations changes to the current session target are in effect only for the duration of the session, and are not saved in FLASH memory. The *session* option can also be used on the console display, if the changes are desired to be temporary. If changes to the console-display are to be permanent (saved to FLASH memory), use the following form of the command:

`configure log target console-display filter <filter name> {severity <severity> {only}}`

In versions prior to ExtremeWare 7.1.0, so-called *static* messages with a severity level of *warning* and above were stored in NVRAM so they would be available across a reboot. This remains the default behavior for ExtremeWare releases, but message filtering for the NVRAM target is now configurable.

**Example**

The following command sends log messages that pass the filter myFilter and are of severity *warning* and above to the previously configured syslog host at 10.31.8.25, port 8993, and facility *local3*:

`configure log target syslog 10.31.8.25:8993 local3 filter myFilter severity warning`

The following command sends log messages that pass the filter myFilter and are of severity *warning* and above to the current session:

`configure log target session filter myFilter severity warning`

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.

---

**Table 14: Default Target Log Characteristics**

<table>
<thead>
<tr>
<th>Target</th>
<th>Enabled</th>
<th>Severity Level</th>
<th>Pre-7.1.0 Command to Set Log Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>console display</td>
<td>no</td>
<td>info</td>
<td><code>configure log display {&lt;severity&gt;}</code></td>
</tr>
<tr>
<td>memory buffer</td>
<td>yes</td>
<td>debug-data</td>
<td>N/A</td>
</tr>
<tr>
<td>NVRAM</td>
<td>yes</td>
<td>warning</td>
<td>N/A</td>
</tr>
<tr>
<td>session</td>
<td>no</td>
<td>info</td>
<td>N/A</td>
</tr>
<tr>
<td>syslog</td>
<td>no</td>
<td>debug-data</td>
<td><code>configure syslog add &lt;host name/ip&gt; (: &lt;udp-port&gt;) [local0... local7] &lt;severity&gt;</code></td>
</tr>
</tbody>
</table>

The built-in filter DefaultFilter and a severity level of *info* are used for each new telnet session. These values may be overridden on a per-session basis by using the `configure log target filter` command and specifying the target as *session*. Use the following form of the command for per-session configuration changes:

`configure log target session filter <filter name> {severity <severity> {only}}`

Configurations changes to the current session target are in effect only for the duration of the session, and are not saved in FLASH memory. The *session* option can also be used on the console display, if the changes are desired to be temporary. If changes to the console-display are to be permanent (saved to FLASH memory), use the following form of the command:

`configure log target console-display filter <filter name> {severity <severity> {only}}`

In versions prior to ExtremeWare 7.1.0, so-called *static* messages with a severity level of *warning* and above were stored in NVRAM so they would be available across a reboot. This remains the default behavior for ExtremeWare releases, but message filtering for the NVRAM target is now configurable.

**Example**

The following command sends log messages that pass the filter myFilter and are of severity *warning* and above to the previously configured syslog host at 10.31.8.25, port 8993, and facility *local3*:

`configure log target syslog 10.31.8.25:8993 local3 filter myFilter severity warning`

The following command sends log messages that pass the filter myFilter and are of severity *warning* and above to the current session:

`configure log target session filter myFilter severity warning`

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure log target format

configure log target [console-display | memory-buffer | nvram | session | syslog [<host name/ip> {:<udp-port}>] [local0 ... local7)]] format [date [dd-mm-yyyy | dd-Mmm-yyyy | mm-dd-yyyy | Mmm-dd | yyyy-mm-dd | none] | host-name [on | off] | event-name [component | condition | none | subcomponent] | priority [on | off] | process-id [on | off] | process-name [on | off] | sequence-number [on | off] | severity [on | off] | source-function [on | off] | source-line [on | off] | tag-id [on | off] | tag-name [on | off] | timestamp [seconds | hundredths | none]

Description

Configures the formats of the items that make up a message, on a per-target basis.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog target.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0...local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
<tr>
<td>timestamp</td>
<td>Specifies a timestamp formatted to display seconds, hundredths, or none.</td>
</tr>
<tr>
<td>date</td>
<td>Specifies a date formatted as specified, or none.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies whether to include the severity.</td>
</tr>
<tr>
<td>event-name</td>
<td>Specifies how detailed the event description will be. Choose from none, component, subcomponent, or condition.</td>
</tr>
<tr>
<td>host-name</td>
<td>Specifies whether to include the host name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies whether to include the priority.</td>
</tr>
<tr>
<td>tag-id</td>
<td>Specifies whether to include the internal task identifier.</td>
</tr>
<tr>
<td>tag-name</td>
<td>Specifies whether to include the task name.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>Specifies whether to include the event sequence number.</td>
</tr>
<tr>
<td>process-name</td>
<td>Specifies whether to include the internal process name.</td>
</tr>
<tr>
<td>process-id</td>
<td>Specifies whether to include the internal process identifier.</td>
</tr>
<tr>
<td>source-function</td>
<td>Specifies whether to include the source function name.</td>
</tr>
<tr>
<td>source-line</td>
<td>Specifies whether to include the source file name and line number.</td>
</tr>
</tbody>
</table>

Default

The following defaults apply to console display, memory buffer, NVRAM, and session targets:

- **timestamp**—hundredths
- **date**—mm-dd-yyyy
configure log target format

- severity—on
- event-name—condition
- host-name—off
- priority—off
- tag-id—off
- tag-name—off
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

The following defaults apply to syslog targets (per RFC 3164):

- timestamp—seconds
- date—mmm-dd
- severity—on
- event-name—none
- host-name—off
- priority—on
- tag-id—off
- tag-name—on
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

Usage Guidelines

This command configures the format of the items that make up log messages. You can choose to include or exclude items and set the format for those items, but you cannot vary the order in which the items are assembled.

When applied to the targets console-display or session, the format specified is used for the messages sent to the console display or telnet session. Configuration changes to the session target, be it either a telnet or console display target session, are in effect only for the duration of the session, and are not saved in FLASH.

When this command is applied to the target memory-buffer, the format specified is used in subsequent show log and upload log commands. The format configured for the internal memory buffer can be overridden by specifying a format on the show log and upload log commands.

When this command is applied to the target syslog, the format specified is used for the messages sent to the specified syslog host.
**Timestamps.** A timestamp refers to the time an event occurred. Timestamps can be output either in seconds, as described in RFC 3164 (for example, “13:42:56”), or in hundredths of a second (for example, “13:42:56.98”). They can also be suppressed altogether. To display timestamps as hh:mm:ss, use the `seconds` keyword; to display as hh:mm:ss.HH, use the `hundredths` keyword. To suppress timestamps altogether, use the `none` keyword. Timestamps are displayed in hundredths by default.

**Date.** The date an event occurred can be output as described in RFC 3164. Dates are output in different formats, depending on the keyword chosen. The following lists the `date` keyword options, and how the date “March 26, 2003” would be output:

- Mmm-dd—Mar 26
- mm-dd-yyyy—03/26/2003
- dd-mm-yyyy—26-03-2003
- yyyy-mm-dd—2003-03-26
- dd-Mmm-yyyy—26-Mar-2003

Dates are suppressed altogether by specifying `none`. Dates are displayed as `mm-dd-yyyy` by default.

**Severity.** A four-letter abbreviation of the severity of the event can be output by specifying `severity` on or suppressed by specifying `severity off`. The default setting is `severity on`. The abbreviations are: Crit, Erro, Warn, Noti, Info, Summ, Verb, and Data. These correspond to: Critical, Error, Warning, Notice, Informational, Debug-Summary, Debug-Verbose, and Debug-Data.

**Event Names.** An event name can be output in the following ways:

- As the component name alone by specifying `event-name component`
- As component and subcomponent name by specifying `event-name subcomponent`
- As component and subcomponent name with condition mnemonic by specifying `event-name condition`

Event names can be suppressed by specifying `event-name none`. The default setting is `event-name condition` to specify the complete name of the events.

**Host Name.** The configured SNMP name of the switch can be output as `HOSTNAME` described in RFC 3164 by specifying `host-name on` or suppressed by specifying `host-name off`. The default setting is `host-name off`.

**Tag ID.** The (internal) ExtremeWare task identifiers of the applications detecting the events can be output as the pid described in RFC 3164 by specifying `tag-id on` or suppressed by specifying `tag-id off`. The default setting is `tag-id off`.

**Tag Name.** The component name used by the application when detecting the events can be output as the tag described in RFC 3164 by specifying `tag-name on` or suppressed by specifying `tag-name off`. The default setting is `tag-name off`.

**Sequence Number.** Sequence numbers refer to the specific ordering of events as they occur. They can be output as an ASCII decimal integer by specifying `sequence-number on` or suppressed by specifying `sequence-number off`. The default setting is `sequence-number off`. 
**Process Name.** For providing detailed information to technical support, the (internal) ExtremeWare task names of the applications detecting the events can be displayed by specifying `process-name` on or suppressed by specifying `process-name off`. The default setting is `process-name off`.

**Process ID.** For providing detailed information to technical support, the (internal) ExtremeWare task identifiers of the applications detecting the events can be displayed by specifying `process-id` on or suppressed by specifying `process-id off`. The default setting is `process-id off`.

**Source Function.** For providing detailed information to technical support, the names of the application source functions detecting the events can be displayed by specifying `source-function` on or suppressed by specifying `source-function off`. The default setting is `source-function off`.

**Source Line.** For providing detailed information to technical support, the application source file names and line numbers detecting the events can be displayed by specifying `source-line` on or suppressed by specifying `source-line off`. The default setting is `source-line off`.

**Example**

In the following example, the switch generates the identical event from the component SNTP, using three different formats.

Using the default format for the session target, an example log message might appear as:

05/29/2003 12:15:25.00 <Warn:SNTP.RslvSrvrFail> The SNTP server parameter value (TheWrongServer.example.com) can not be resolved.

If you set the current session format using the following command:

```
configure log target session format date mm-dd-yyyy timestamp seconds event-name component
```

the same example would appear as:

05/29/2003 12:16:36 <Warn:SNTP> The SNTP server parameter value (TheWrongServer.example.com) can not be resolved.

In order to provide some detailed information to technical support, you set the current session format using the following command:

```
configure log target session format date mmm-dd timestamp hundredths event-name condition source-line on process-name on
```

In this case, the same example would appear as:

May 29 12:17:20.11 SNTP: <Warn:SNTP.RslvSrvrFail> tSntpc: (sntpcLib.c:606) The SNTP server parameter value (TheWrongServer.example.com) can not be resolved.

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure log target match

configure log target [console-display | memory-buffer | nvram | session | syslog [{host name/ip} {<udp-port>} {local0 ... local7}]] match [any |<match-expression>]

Description
Associates a match expression to a target.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog target.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0...local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that any messages will match. This effectively removes a previously configured match expression.</td>
</tr>
<tr>
<td>match-expression</td>
<td>Specifies a regular expression. Only messages that match the regular expression will be sent.</td>
</tr>
</tbody>
</table>

Default
By default, targets do not have a match expression.

Usage Guidelines
This command configures the specified target with a match expression. The filter associated with the target is not affected. A message is sent to a target if the target has been enabled, the message passes the associated filter, the message is at least as severe as the configured severity level, and the message output matches the regular expression specified.

See the show log command on page 775 for a detailed description of simple regular expressions. By default, targets do not have a match expression.

Specifying any instead of match-expression effectively removes a match expression that had been previously configured, causing any message to be sent that has satisfied all of the other requirements.

To see the configuration of a target, use the following command:
show log configuration target

To see the current configuration of a filter, use the following command:
show log configuration filter
Example
The following command sends log messages to the current session if they pass the current filter and severity level and contain the string “user5”:

```
configure log target session match user5
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure log target severity

configure log target [console-display | memory-buffer | nvram | session | syslog [{host name/ip} [: <udp-port>] [local0 ... local7]]] {severity <severity> {only}}

Description
Sets the severity level of messages sent to the target.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog target.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the least severe level to send (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only the specified severity level is to be sent.</td>
</tr>
</tbody>
</table>

Default
By default, targets are sent messages of the following severity level and above:

- console display—info
- memory buffer—debug-data
- NVRAM—warning
- session—info
- syslog—debug-data

Usage Guidelines
This command configures the specified target with a severity level. The filter associated with the target is not affected. A message is sent to a target if the target has been enabled, the message passes the associated filter, the message is at least as severe as the configured severity level, and the message output matches the regular expression specified.

See the show log command on page 775 for a detailed description of severity levels.

To see the current configuration of a target, use the following command:

```
show log configuration target
```

To see the current configuration of a filter, use the following command:

```
show log configuration filter
```
Example

The following command sends log messages to the current session that pass the current filter at a severity level of info or greater:

```plaintext
configure log target session severity info
```

History

This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
configure packet-mem-scan-recovery-mode

configure packet-mem-scan-recovery-mode [offline | online] [msm-a | msm-b | <slot number>]

**Description**

Configures packet memory scanning and the recovery mode setting on a BlackDiamond module.

**NOTE**

This command is available only on the BlackDiamond switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>offline</td>
<td>Specifies that a faulty BlackDiamond module is taken offline and kept offline if one of the following occurs:</td>
</tr>
<tr>
<td></td>
<td>• More than eight defects are detected.</td>
</tr>
<tr>
<td></td>
<td>• Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process.</td>
</tr>
<tr>
<td></td>
<td>• After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.</td>
</tr>
<tr>
<td>online</td>
<td>Specifies that a faulty module is kept online, regardless of how many errors are detected.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies the MSM module installed in slot A.</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies the MSM module installed in slot B.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies a module installed in a slot.</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Usage Guidelines**

Use this command to scan and check the health of an individual module rather than the overall system.

This command overrides the system health check auto-recovery setting. If you have the system health check alarm level configured, the individual packet memory scanning configuration is ignored.

This command is effective only if the system health check is configured for auto-recovery. If the system health checker is configured for auto-recovery, and you configure packet-mem-scan-recovery, you can define a specific slot’s behavior if an error is discovered.

To configure the system health check for auto-recovery, use the `configure sys-health-check auto-recovery` command.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.
Example
The following command enables packet memory scanning on slot 1, and specifies that the module be taken offline:
configure packet-mem-scan-recovery mode offline slot 1

The following command enables packet memory scanning on the MSM module in slot B, and specifies that the module be kept online
configure packet-mem-scan-recovery mode online slot msm-b

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available on BlackDiamond switches only.
configure sflow agent

configure sflow agent <ip-address>

Description
Configures the sFlow agent source IP address used in the sFlow UDP datagrams sent to the sFlow collector.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| ip-address | Specifies the IP address from which sFlow data is sent on the switch. |

Default
The default IP address is 0.0.0.0.

Usage Guidelines
This command allows you to configure the IP source address that the sFlow agent uses when sending data. Typically, you would set this to the IP address used to identify the switch in the network management tools that you use. We recommend that you not leave this parameter in its default value.

Example
The following command sets the source IP address to 10.2.0.1 for UDP datagrams sent out by the sFlow agent to the sFlow collector:

`configure sflow agent 10.2.0.1`

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available only on the “i” series platforms.
configure sflow backoff-threshold

configure sflow backoff-threshold <rate>

Description
Configures the maximum number of packets sent to the sFlow collector per second.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate</td>
<td>Specifies the maximum number of packets sent to the sFlow collector per second. The range is 100 - 5000</td>
</tr>
</tbody>
</table>

Default
The default is 50.

Usage Guidelines
This command configures the maximum number of samples sent to the CPU per second. If this rate is exceeded, the internal sFlow CPU throttling mechanism kicks in to limit the load on the CPU. Each time the limit is reached, the sample rate is halved (the value of number in the configure sflow sample-rate or configure sflow ports <portlist> sample-frequency <number> command is doubled) on the slot on which maximum number of packets are received.

This effectively doubles the sampling frequency of all the ports on that slot with a sub-sampling factor of 1. The sampling frequency of ports on that slot with a sub-sampling factor greater than 1 will not change; the sub-sampling factor is halved so that the same sample rate applies to that port.

Use the following command to reset the sFlow backoff threshold value to 0 (zero):

unconfigure sflow backoff-threshold

Example
The following command specifies that the sFlow backoff threshold should be set to a maximum of 256 packets per second:

configure sflow backoff-threshold 256

If the number of packets sent to the sFlow collector exceeds a rate of 256 packets per second, the sampling rate is doubled. For example, if a sampling rate of 512 is exceeded, the sampling rate is doubled to 1024.

History
This command was first available in ExtremeWare 7.3.0.
**Platform Availability**

This command is available only on the “i” series platforms.
configure sflow collector

    configure sflow collector <ip-address> port <udp-port>

Description
Configures the IP address and UDP port number identifying the sFlow collector.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip-address</td>
<td>Specifies the IP address to send the sFlow data.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number to send the sFlow data.</td>
</tr>
</tbody>
</table>

Default
The default UDP port number is 6343

Usage Guidelines
This command allows you to configure where to send the sFlow data. You must specify an IP address for the sFlow data collector, and a UDP port where the samples will be transmitted to and from the sFlow agent.

You can configure up to four sFlow collectors. Each unique combination of an IP address and a UDP port identifies a collector.

Using the unconfigure sflow collector command resets the collector parameters to the default.

NOTE
The notation : can be used instead of port, as in the examples.

Example
The following command specifies that the sFlow agent will send all samples to the collector with the address 123.123.123.123 and port number 9876:

    configure sflow collector 123.123.123.123 port 9876

or

    configure sflow collector 123.123.123.123:9876

History
This command was first available in ExtremeWare 7.3.0.
Platform Availability

This command is available only on the “i” series platforms.
configure sflow poll-interval

configure sflow poll-interval <seconds>

Description
Configures the sFlow counter polling interval at which the statistics counter values are sent to the sFlow collector.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| seconds | Specifies the number of seconds between polling each counter. The value can range from 1 to 3600 seconds. |

Default
The default polling interval is 20 seconds.

Usage Guidelines
Each sFlow statistics counter is polled at regular intervals, and this data is then sent to the sFlow collector. This command is used to set the polling interval. The same value is used for all data sources. The polling interval applies to each counter separately, and the polling is distributed among the counters. For example, if the polling interval is 20 seconds and there are two counters, data is collected alternately every 10 seconds.

Example
The following command sets the polling interval to 60 seconds:

```
configure sflow poll-interval 60
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available only on the “i” series platforms.
configure sflow sample-rate

configure sflow sample-rate <number>

Description
Configures the sample rate at which the sFlow agent collects network traffic samples.

**NOTE**
This command is available only on the “i” series switches.

Syntax Description

| number | Specifies the fraction (1/number) of packets to be sampled. |

Default
8192

Usage Guidelines
This command configures the sample rate at which the sFlow agent collects network traffic samples. One sample per <number> of packets received will be sent to the sFlow collector. If the sample rate is set to ‘0’ (zero), no samples will be sent to the collector.

Example
The following command sets the sample rate to one packet out of every 10000:

```
configure sflow sample-rate 10000
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available only on the “i” series platforms.
configure sys-health-check alarm-level

    configure sys-health-check alarm-level [log | system-down | traps | default]

Description
Configures the alarm response for the system health checker.

NOTE
This command is available only on the Alpine and the Summit "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Posts a CRIT message to the log.</td>
</tr>
<tr>
<td>system-down</td>
<td>Posts a CRIT message to the log, sends a trap, and turns off the system.</td>
</tr>
<tr>
<td>traps</td>
<td>Posts a CRIT message to the log and sends a trap.</td>
</tr>
<tr>
<td>default</td>
<td>Resets the alarm level to log.</td>
</tr>
</tbody>
</table>

Default
The default alarm level is log.

Usage Guidelines
This command allows you to configure the switch’s reaction to a failed health check.

The system health checker tests I/O modules, SMMi modules, and the backplane by forwarding packets every 4 seconds. Additional checking for the validity of these packets is completed by performing a checksum.

By isolating faults to a specific module, SMMi, or backplane connection, the system health checker prevents corrupted packets from being propagated to the CPU, upper layer modules, or the rest of your network. If you observe a failure, please contact Extreme Technical Support.

Depending on how you have configured the system health checker, failed system health checks may generate critical error messages in the syslog, and may also send a trap and/or shut down the system. The system health checker will continue to periodically forward test packets to failed components. If auto-recovery is configured, the system will attempt to automatically reset the faulty module and bring it back online.

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

In ExtremeWare versions prior to 6.2, you cannot use both mirroring and the system health checker at the same time. If you configure mirroring with the system health checker enabled, the health checker will indicate that it has been disabled by sending a message to the syslog. In ExtremeWare 6.2 or later, this restriction does not apply.
The auto-recovery option configures the number of times the system health checker attempts to automatically reset a faulty module and bring it online. If the system health checker fails more than the configured number of attempts, it sets the module to card-down.

**NOTE**

*This threshold applies only to BlackDiamond I/O modules.*

In ExtremeWare 6.2.1 or later, when auto-recovery is configured, the occurrence of three consecutive checksum errors causes the packet memory (PM) defect detection program to be run against the I/O module. Checksum errors may include internal and external MAC port parity errors, EDP checksum errors, and CPU packet or diagnostic packet checksum errors. If defects are detected, the module is taken offline, the memory defect information is recorded in the module EEPROM, the defective buffer is mapped out of further use, and the module is returned to operational state. A maximum of 8 defects can be stored in the EEPROM.

After the PM defect detection and mapping process has been run, a module is considered failed and is taken offline in the following circumstances:

* More than eight defects are detected.
* Three consecutive checksum errors were detected by the health checker, but no new PM defects were found by the PM defect detection process.
* After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.

The auto-recovery repetition value is ignored in these cases. In any of these cases, please contact Extreme Technical Support.

If you specify the online option, the module is kept online, but the following error messages are recorded in the log:

```<WARN:SYST> card_db.c 832: Although card 2 is back online, contact Tech. Supp. for assistance.<WARN:SYST> card_db.c 821: Card 2 has nonrecoverable packet memory defect.```

To view the status of the system health checker, use the `show diagnostics` command.

To enable the health checker, use the `enable sys-health-check` command.

To disable the health checker, use the `disable sys-health-check` command.

The alarm-level system-down option is especially useful in an ESRP configuration where the entire system is backed by an identical system. By powering down the faulty system, you ensure that erratic ESRP behavior in the faulty system does not affect ESRP performance and ensures full system failover to the redundant system.

If you are using ESRP with ESRP diagnostic tracking enabled in your configuration, the system health check failure will automatically reduce the ESRP priority of the system to the configured failover priority. This allows the healthy standby system to take over ESRP and become responsible for handling traffic.

I/O module faults are permanently recorded on the module’s EEPROM. A module that has failed a system health check cannot be brought back online.
To view the failure messages, use the `show diagnostics` command.

If you configure the system health check mode to `offline` and no new errors are detected, the device scanned now remains online. This behavior is identical to the current behavior if you use the `run diagnostics` command.

**Example**

The following command configures the system health checker to post a CRIT message to the log and send a trap:

```
configure sys-health-check alarm-level traps
```

**History**

This command was first available in ExtremeWare 6.1.9.

The system health check functionality was modified in ExtremeWare 6.2.1 to support packet memory defect detection and mapping on selected I/O modules.

This command was modified in ExtremeWare 6.2.2 to support system health check and checksum error checking and to add the `online` and `offline` parameters.

**Platform Availability**

This command is available only on the Alpine, BlackDiamond, and Summit “i” series switches.
configure sys-health-check auto-recovery

configure sys-health-check auto-recovery <number> [offline | online]

Description
Configures the auto-recovery function of the system health checker.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| number       | Specifies the number of times that the health checker attempts to auto-recover a faulty module. The range is from 0 through 255 times. Default is 3 times.  
   NOTE: This option is available only in BlackDiamond I/O modules. |
| offline      | Specifies that a faulty module is taken offline and kept offline if one of the following occurs:  
   • More than eight defects are detected.  
   • Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process.  
   • After defects were detected and mapped out, the same checksum errors are again detected by the system health checker. |
| online       | Specifies that a faulty module is kept online, regardless of memory scanning or memory mapping errors. |

Default
The default alarm level is log.

Usage Guidelines
This command allows you to configure the switch’s reaction to a failed health check.

The system health checker tests I/O modules, MSM modules, and the backplane by forwarding packets every 4 seconds. Additional checking for the validity of these packets is completed by performing a checksum.

By isolating faults to a specific module, MSM, or backplane connection, the system health checker prevents corrupted packets from being propagated to the CPU, upper layer modules, or the rest of your network. If you observe a failure, please contact Extreme Technical Support.

Depending on how you have configured the system health checker, failed system health checks can generate critical error messages in the syslog, and can also send a trap and/or shut down the system. The system health checker continues to periodically forward test packets to failed components. If auto-recovery is configured, the system attempts to automatically reset the faulty module and bring it back on line.

In ExtremeWare versions prior to 6.2, you cannot use both mirroring and the system health checker at the same time. If you configure mirroring with the system health checker enabled, the health checker indicates that it has been disabled by sending a message to the syslog. In ExtremeWare 6.2 or later, this restriction does not apply.
In the BlackDiamond switches, the auto-recovery option configures the number of times the system health checker attempts to automatically reset a faulty module and bring it online. If the system health checker fails more than the configured number of attempts, it sets the module to card-down. This threshold applies only to BlackDiamond I/O modules.

In ExtremeWare 6.2.1 or later, when auto-recovery is configured, the occurrence of three consecutive checksum errors causes the packet memory (PM) defect detection program to be run against the I/O module. Checksum errors can include internal and external MAC port parity errors, EDP checksum errors, and CPU packet or diagnostic packet checksum errors. If defects are detected, the module is taken off line, the memory defect information is recorded in the module EEPROM, the defective buffer is mapped out of further use, and the module is returned to operational state. A maximum of 8 defects can be stored in the EEPROM.

After the PM defect detection and mapping process has been run, a module is considered failed and is taken off line in the following circumstances:

- More than eight defects are detected.
- Three consecutive checksum errors were detected by the health checker, but no new defects were found by the memory scanning and mapping process.
- After defects were detected and mapped out, the same checksum errors are again detected by the system health checker.

The auto-recovery repetition value is ignored in these cases. In any of these cases, please contact Extreme Technical Support.

Auto-recovery mode only affects an MSM if the system has no slave MSM. If the faulty module is the only MSM in the system, auto recovery automatically resets the MSM and brings it back on line. Otherwise, auto-recovery has no effect on an MSM.

If you specify the online option, the module is kept on line, but the following error messages are recorded in the log:

```
<WARN:SYST> card_db.c 832: Although card 2 is back online, contact Tech. Supp. for assistance.
<WARN:SYST> card_db.c 821: Card 2 has nonrecoverable packet memory defect.
```

To view the status of the system health checker, use the show diagnostics command.

To enable the health checker, use the enable sys-health-check command.

To disable the health checker, use the disable sys-health-check command.

The alarm-level system-down option is especially useful in an ESRP configuration where the entire system is backed by an identical system. By powering down the faulty system, you ensure that erratic ESRP behavior in the faulty system does not affect ESRP performance and ensures full system failover to the redundant system.

If you are using ESRP with ESRP diagnostic tracking enabled in your configuration, the system health check failure will automatically reduce the ESRP priority of the system to the configured failover priority. This allows the healthy standby system to take over ESRP and become responsible for handling traffic.

I/O module faults are permanently recorded on the module EEPROM. A module that has failed a system health check cannot be brought back online.
If the faulty module is a master MSM, the slave MSM automatically becomes the master and sets the faulty MSM to card-down. The new master MSM re-initializes and brings up all the I/O modules.

If the faulty module is a master MSM and there is no slave MSM, the system continues operation in a “limited commands” mode. In the “limited commands” mode, the I/O slots are not initialized, and the only commands allowed are those that do not affect the switch hardware configuration.

If the faulty module is a slave MSM, the fault is recorded in the slave MSM NVRAM, and the slave MSM is taken off line.

To view the failure messages, use the show diagnostics command.

To clear the MSM failure messages posted to the log, use the clear log command. This command clears the error messages from the MSM NVRAM. If the MSM failed a system health check, this command restores the MSM to full functionality. This command should only be used for additional testing purposes and reproduction efforts of the original fault.

If you configure the system health check mode to offline and no new errors are detected, the device scanned now remains on line. This behavior is identical to the current behavior if you use the run diagnostics command.

**Example**

The following command configures the system health checker to try ten times to bring a faulty MSM back on line:

```
configure sys-health-check auto-recovery 10
```

**History**

This command was first available in ExtremeWare 6.1.9.

The system health check functionality was modified in ExtremeWare 6.2.1 to support packet memory defect detection and mapping on selected I/O modules.

This command was modified in ExtremeWare 6.2.2 to support system health check and checksum error checking on the BlackDiamond 6804 switch and to add the online and offline parameters.

**Platform Availability**

This command is available on the BlackDiamond switch only.

The packet-memory defect detection and mapping feature is supported only on selected I/O modules. See the release note for your version of ExtremeWare for information on the supported modules.
configure sys-health-check scan recovery

configure sys-health-check scan recovery [reset | remap]

Description
Configures the system health checker to reset the module with or without diagnostics.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>reset</td>
<td>Resets the module without running diagnostics.</td>
</tr>
<tr>
<td>remap</td>
<td>Resets the module and then runs diagnostics. This is the default option.</td>
</tr>
</tbody>
</table>

Default
Reset module and run diagnostics (remap).

Usage Guidelines
Extreme Networks support personnel can configure the action taken by the system health check if diagnostics are run or if checksum errors trigger diagnostics. If diagnostics are run or triggered in previous releases of ExtremeWare, the module is reset and diagnostics are run. Support personnel can use the following command to configure ExtremeWare to simply to reset the module without running diagnostics:
configure system-health-check scan recovery [reset | remap]

Entering this command generates the following message:
This command should only be used at the direction of Extreme Personnel. Do you wish you continue (y/n)?

Answering y immediately implements the change. Answering n implements no change and returns you to the command line.

Use the reset option to reset the module without running diagnostics. This option is useful for recovering from transient hardware failures. In these cases, resetting the module stops the checksum errors.

Use the remap option to reset the module and run diagnostics. This is the default.

Example
The following command configures the system health checker to reset the module without running diagnostics:
configure sys-health-check scan recovery reset
History
This command was first available in ExtremeWare 7.2.0b25.

Platform Availability
This command is only available on “i” series switches.
configure sys-recovery-level

For the “i” series switches:

configure sys-recovery-level [none | [all | critical] [msm-failover | reboot | shutdown | system-dump [maintenance-mode | msm-failover | reboot | shutdown]]

For the “e” series switches:

configure sys-recovery-level [none | [all | critical] [reboot ]

Description

Configures a recovery option for instances where an exception occurs in ExtremeWare.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Configures the level to no recovery. No action is taken when a task exception occurs; there is no system shutdown or reboot.</td>
</tr>
<tr>
<td>all</td>
<td>Configures ExtremeWare to log an error into the syslog and either shutdown or reboot the system after any task exception occurs.</td>
</tr>
<tr>
<td>critical</td>
<td>Configures ExtremeWare to log an error into the syslog and either shutdown or reboot the system after a critical task exception.</td>
</tr>
<tr>
<td>msm-failover</td>
<td>Triggers the slave MSM to take over control of the switch if there is a software exception on the master MSM. NOTE: This option is available only on BlackDiamond switches.</td>
</tr>
<tr>
<td>reboot</td>
<td>Reboots the switch.</td>
</tr>
<tr>
<td>shutdown</td>
<td>Shuts down the switch.</td>
</tr>
<tr>
<td>system-dump</td>
<td>Triggers a dump transfer, followed by the specified completion action (reboot, shutdown, msm-failover, or maintenance-mode). Maintenance mode leaves the switch in whatever state the dump transfer puts it in. Some subsystems may no longer behave correctly or operate at all after a system dump. The system-dump option should only be used with assistance from TAC. NOTE: This option is available only on switches with Ethernet management ports.</td>
</tr>
</tbody>
</table>

Default

None

Usage Guidelines

This command is used for system troubleshooting. If the system fails before the switch is booted, the switch automatically starts the console and allows access to the system to view the logs or debug the failure. You can also configure the system to respond to software failures automatically. You must specify one of the following parameters for the system to respond to software failures:

- none—No action is taken when a task exception occurs.
- all—The system will reboot or shut down if any task exception occurs.
- critical—The system will reboot or shut down if a critical task exception occurs. Critical tasks include the tBGTask, tNetTask, tEdpTask, and tESRPTask.
For ExtremeWare 6.1, the system always reboots after a task exception when the system recovery level is specified as all or critical.

For ExtremeWare 6.2 or later, you must specify whether the system should shut down or reboot upon a task exception if the recovery level is all or critical.

For BlackDiamond Switches. For ExtremeWare 6.2.2 or later, if `msm-failover` is specified on a BlackDiamond switch and there is a software exception on the master MSM, the interrupt handler triggers the slave MSM to take over control of the switch.

**Examples**

The following command configures a switch to reboot after a critical task exception occurs:

```
configure sys-recovery-level critical reboot
```

The following command configures the Master MSM to failover to the Slave MSM if a software exception occurs:

```
configure sys-recovery-level critical msm-failover
```

**History**

This command was first available in ExtremeWare 6.1.

Modified in ExtremeWare 6.2 to support the `shutdown` and `reboot` options.

Modified in ExtremeWare 6.2.2 to support the `msm-failover` option.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Modified in ExtremeWare 7.2e to support the `shutdown` and `reboot` options.

**Platform Availability**

This command is available on all i-series switches. The `msm-failover` option is available on the BlackDiamond switch only.
configure syslog add

configure syslog {add} <host name/ip> {: <udp-port>} [local0 ... local7] {<severity>}

Description
Configures the remote syslog server host address, and filters messages to be sent to the remote syslog target.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host name/ip</td>
<td>Specifies the remote syslog server host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0 ... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies a message severity. Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.</td>
</tr>
</tbody>
</table>

Default
If a severity level is not specified, all messages are sent to the remote syslog server target. If UDP port is not specified, 514 is used.

Usage Guidelines
Options for configuring the remote syslog server include:

- host name/ip—The name or IP address of the remote syslog server host.
- udp-port—The UDP port
- facility (local0– local7)—The syslog facility level for local use.
- severity—Filters the messages sent to the remote syslog server target to have the selected severity or higher (more critical). Severities include critical, error, warning, notice, info, debug-summary, debug-verbose, and debug-data.

The switch log overwrites existing log messages in a wrap-around memory buffer, which may cause you to lose valuable information once the buffer becomes full. The remote syslog server does not overwrite log information, and can store messages in non-volatile files (disks, for example).

Syslog is disabled by default. The `enable syslog` command must be issued for messages to be sent to the remote syslog server(s). A total of four syslog servers can be configured at one time.

When a syslog server is added, it is associated with the filter called DefaultFilter. Use the `configure log target filter` command to associate a different filter.

**On “i” series switches**, for version 4.0 and higher, the syslog facility level is defined as local0 – local7. The facility level is used to group syslog data.

Example
The following command configures the remote syslog server target with an critical severity:

configure syslog 123.45.67.78 local1 critical
History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure syslog delete

configure syslog delete <host name/ip> {:<udp-port>} [local0 ... local7]

Description
Deletes a remote syslog server address.

Syntax Description

<table>
<thead>
<tr>
<th>host name/ip</th>
<th>Specifies the remote syslog server host name or IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0 ... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
</tbody>
</table>

Default
If a UDP port number is not specified, 514 is used.

Usage Guidelines
This command is used to delete a remote syslog server target.

Example
The following command deletes the remote syslog server with an IP address of 10.0.0.1:
configure syslog delete 10.0.0.1 local1

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure transceiver-test failure-action

configure transceiver-test failure-action [log | sys-health-check]

Description
Configures the action the switch takes if too many failures are detected within the specified window.

NOTE
This command is available only on modular switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>log</td>
<td>Specifies that messages are sent to the syslog.</td>
</tr>
<tr>
<td>sys-health-check</td>
<td>Specifies that the configured system health check action is taken.</td>
</tr>
</tbody>
</table>

Default
Log

Usage Guidelines

If you select `log`, only one instance of an error message is logged at this level.

If you select `sys-health-check` and the switch detects too many failures, the switch takes the configured system health check action. To configure the system health checker, use the `configure sys-health-check alarm-level` or the `configure sys-health-check auto-recovery` command. The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

By default, the switch checks for errors within the last eight 20-second windows. Use the `configure transceiver-test window` command to modify the number of windows.

To determine if you have the transceiver test enabled and the failure action the switch takes, use the `show switch` command. The following is sample transceiver test output:

```
Transceiver Diag: Enabled. Failure action: log only
```

For ExtremeWare 6.2.2b108:

The default is `sys-health-check`, and the switch takes the configured system health check action.

Example

The following command configures the switch to perform the configured system health check action if too many failures are detected:

```
configure transceiver-test failure-action sys-health-check
```

History

This command was first available in ExtremeWare 6.2.2b108.
The default for this command was changed to \texttt{log} in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available only on modular switches.
configure transceiver-test period

    configure transceiver-test period <period <1-60>>

Description
Configures how often the switch runs the transceiver test.

NOTE
This command is available only on modular switches.

Syntax Description

period <1-60>  Specifies, in seconds, how often the transceiver test runs. The range is 1 to 60.

Default
12 seconds

Usage Guidelines
Use this feature when the switch can be brought off-line.

Configuring the transceiver test period to 11 seconds or less can affect system performance; therefore, Extreme Networks does not recommend changing the default transceiver test period. The default is adequate for most networks.

Example
The following command configure the transceiver test to run every 15 seconds:
configure transceiver-test period 15

History
This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available only on modular switches.
configure transceiver-test threshold

configure transceiver-test threshold <1-8>

Description
Configures the number of errors the switch accepts before an action is taken.

NOTE
This command is available only on modular switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>Specifies the number of errors. The range is 1 to 8 errors.</td>
</tr>
</tbody>
</table>

Default
Three errors

Usage Guidelines
Use this feature when the switch can be brought off line.

Extreme Networks does not recommend changing the default transceiver test threshold parameter. The default parameter is adequate for most networks.

Example
The following command configures the switch to accept 4 errors before an action is taken:
configure transceiver-test threshold 4

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available only on modular switches.
configure transceiver-test window

configure transceiver-test window <1-8>

Description
Configures the number of 20-second windows within which the configured number of errors can occur.

NOTE
This command is available only on modular switches.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>window</td>
<td>Specifies the number of 20-second windows. The range is 1 to 8 20-second windows.</td>
</tr>
</tbody>
</table>

Default
Eight windows

Usage Guidelines
Use this feature when the switch can be brought off line.

This configuration provides a sliding window. If you keep the window configuration at 8, the switch checks for errors within the last eight 20-second windows.

To determine the number of errors the switch accepts before it takes action, use the configure transceiver-test threshold command.

Extreme Networks does not recommend changing the default transceiver test window parameter. The default parameter is adequate for most networks.

Example
The following command configures the switch to check for errors within the last seven 20-second windows:

```
configure transceiver-test window 7
```

History
This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available only on modular switches.
create log filter

create log filter <name> (copy <filter name>)

Description
Create a log filter with the specified name.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the filter to create.</td>
</tr>
<tr>
<td>copy</td>
<td>Specifies that the new filter is to be copied from an existing one.</td>
</tr>
<tr>
<td>filter name</td>
<td>Specifies the existing filter to copy.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command creates a filter with the name specified. A filter is a customizable list of events to include or exclude, and optional parameter values. The list of events can be configured by component or subcomponent with optional severity, or by individual condition, each with optional parameter values. See the commands configure log filter events and configure log filter events match for details on how to add items to the filter.

The filter can be associated with one or more targets using the configure log target filter command to control the messages sent to those targets. The system has one built-in filter named DefaultFilter, which itself can be customized. Therefore, the create log filter command can be used to create a filter other than DefaultFilter. As its name implies, DefaultFilter initially contains the default level of logging in which every ExtremeWare component and subcomponent has a pre-assigned severity level.

If you need to create another filter similar to an existing filter, use the copy option to populate the new filter with the configuration of the existing filter. If the copy option is not specified, the new filter will have no events configured and therefore no incidents will pass through it.

The total number of supported filters, including DefaultFilter, is 20.

Example
The following command creates the filter named fdb2, copying its configuration from the filter DefaultFilter:

create log filter fdb2 copy DefaultFilter

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability

This command is available on all platforms.
delete log filter

    delete log filter [<filter name> | all]

Description
Delete a log filter with the specified name.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;filter name&gt;</td>
<td>Specifies the filter to delete.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all filters, except DefaultFilter, are to be deleted</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes the specified filter, or all filters except for the filter DefaultFilter. The specified filter must not be associated with a target. To remove that association, associate the target with DefaultFilter instead of the filter to be deleted, using the following command:

```bash
configure log target <target> filter DefaultFilter
```

Example
The following command deletes the filter named `fdb2`:

`delete log filter fdb2`

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable cli-config-logging

disable cli-config-logging

Description
Disables the logging of CLI configuration commands to the switch Syslog.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
The disable cli-config-logging command discontinues the recording of all switch configuration changes and their sources that are made using the CLI via telnet or the local console. After you disable configuration logging, no further changes are logged to the system log.

To view the status of configuration logging on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for configuration logging.

Example
The following command disables the logging of CLI configuration command to the Syslog:

disable cli-config-logging

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable flowstats

disable flowstats

Description
Disables the flow statistics feature on the switch.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
When this feature is disabled, no flow records are exported.

Example
The following command disables the NetFlow statistics feature on this switch:

disable flowstats

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available only on “i” series platforms.
disable flowstats filter ports

```
disabled flowstats filter <filter#> ports <portlist> {ingress | egress}
```

**Description**
Disables a specified flow record filter for the specified ports.

**Syntax Description**
- **filter#**: Specifies the flow record filter that should be disabled.
- **portlist**: Specifies a list of ports or slots and ports for which the filter should be disabled. May be in the form 1, 2, 3-5, 2:5, 2:6:2:8.
- **ingress**: Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to inbound flows.
  - NOTE: This option is available only on the PoS module.
- **egress**: Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to outbound flows.
  - NOTE: This option is available only on the PoS module.

**Default**
For the PoS module, filter #1 is enabled on all SONET ports, and the remaining filters are disabled.
For other switches or modules, filters are enabled by default when they are configured.

**Usage Guidelines**
The `filter#` parameter is an integer in the range 1 to 8.

For each SONET port on a PoS module, sixteen filters are supported—eight filters for ingress flows and another eight filters for egress flows. The `filter#` parameter and either the `ingress` or `egress` keyword are used to identify the particular filter that is being disabled.

One of either the `ingress` or `egress` keywords are required for SONET ports.

**Example**
The following command disables filter 3 for ports 1-8 on an “i” series switch:
```
disable flowstats filter 3 ports 1-8
```

The following command example disables ingress filter #2 on port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:
```
disable flowstats filter 2 ports 8:1 ingress
```
History
This command was first available in ExtremeWare 6.1.5b20 for the PoS module only. This command was modified in ExtremeWare 6.2 to support all “i” series platforms.

Platform Availability
This command is available only on the “i” series platforms.
disable flowstats ping-check

    disable flowstats ping-check {<group#> | all}

Description
Disables the flow statistics ping-check function for a specified group of collector devices.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| group#   | Specifies the export group for which the ping-check function should be disabled. |

Default
Disabled

Usage Guidelines
On the PoS module, if you do not include a group number, ping-check is disabled for all export groups. The group number is not optional for other Extreme “i” series devices.

Example
The following command disables the ping-check function for all export groups.

disable flowstats ping-check

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms.
disable flowstats ports

disable flowstats ports <portlist>

Description
Disables the flow statistics function on the specified ports.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports for which the flowstats function should be disabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
On the PoS module, flow statistics are collected only on SONET ports that are configured to use the IP control protocol IPCP. (In other words, flow statistics are not collected on ports that are configured to use the bridging control protocol BCP.) Also, there are no configuration restrictions that prohibit enabling of the flow statistics function on ports that are not configured to use IPCP; statistics are not collected on those ports.

Example
The following command disables NetFlow statistics for ports 1-8 on this switch:

disable flowstats ports 1-8

History
This command was first available in ExtremeWare 6.1.5b20 for the PoS module
This command was modified in ExtremeWare 6.2 to support all “i” series platforms.

Platform Availability
This command is available only on the “i” series platforms.
disable log debug-mode

   disable log debug-mode

Description
Disables debug mode. The switch stops logging events of severity debug-summary, debug-verbose, and debug-data.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command disables debug mode. Debug mode must be enabled before logging debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when you are advised to do so by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

Example
The following command disables debug mode:

disable log debug-mode

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable log display

disable log display

Description
Disables the sending of messages to the console display.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
If the log display is disabled, log information is no longer written to the serial console.

This command setting is saved to FLASH and determines the initial setting of the console display at boot-up.

In ExtremeWare 7.1.0, the ability to control logging to different targets was introduced. The new command equivalent to disable log display is the following:

disable log target console-display

Example
The following command disables the log display:

disable log display

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable log target

disable log target [console-display | memory-buffer | nvram | session | syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]]

Description
Stop sending log messages to the specified target.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog target.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0 ... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
</tbody>
</table>

Default
Enabled, for memory buffer and NVRAM; all other targets are disabled by default.

Usage Guidelines

This command stops sending messages to the specified target. By default, the memory buffer and the NVRAM targets are enabled. Other targets must be enabled before messages are sent to those targets.

Configuration changes to the session target are in effect only for the duration of the console display or telnet session, and are not saved in FLASH. Changes to the other targets are saved to FLASH.

In earlier versions of ExtremeWare, a similar command was used to disable displaying the log on the console. That command:

disable log display

is equivalent to:

disable log target console-display

Example

The following command disables log messages to the current session:

disable log target session

History

This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
disable rmon

disable rmon

Description
Disables the collection of RMON statistics on the switch.

Syntax Description
This command has no arguments or variables.

Default
By default, RMON is disabled. However, even when RMON is disabled, the switch responds to RMON queries and sets for alarms and events.

Usage Guidelines
The switch supports four out of nine groups of Ethernet RMON statistics. With RMON disabled, the switch continues to respond to the following two groups:

- Alarms—The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be auto calibrated or set manually.

- Events—The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

To view the status of RMON polling on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for RMON polling.

Example
The following command disables the collection of RMON statistics on the switch:

disable rmon

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable sflow

Description
Globally disables sFlow statistical packet sampling.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command disables sFlow globally on the switch. This command does not disable sFlow if it is enabled on individual ports. Before executing this command, you must first disable per-port sFlow using the following command:

disable sflow ports

Example
The following command disables sFlow sampling globally:

disable sflow

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available only on the “i” series platforms.
disable sflow backoff-threshold

    disable sflow backoff-threshold

Description
Disables the sFlow backoff-threshold feature, which limits the maximum number of packets sent to the sFlow collector per second.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command disables the backoff threshold feature, which is used to limit the number of packets sent to the sFlow collector in a second. The backoff threshold is set by using the following command:

    configure sflow backoff-threshold

If the number of packets sent to the collector exceeds the limit set by the configure sflow backoff-threshold command, the sampling rate is doubled.

The backoff threshold is enabled when the enable sflow backoff-threshold command is executed and the sample rate set by the configure sflow sample-rate command is greater than 0 (zero).

Example
The following command disables the sFlow backoff threshold feature:

    disable sflow backoff-threshold

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available only on the “i” series platforms.
disable sflow ports

disable sflow ports [<portlist> | all]

Description
Disables sFlow statistical packet sampling on a particular list of ports.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Applies the command to all ports.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines

This command disables sFlow statistical packet sampling on a particular list of ports. When sFlow is disabled on a port, sampling and polling stop on that port. If sFlow is disabled globally, all sampling and polling stops.

Use the following command to disable sFlow globally:

disable sflow

Sampling and polling must first be stopped on every port using the disable sflow ports command before all ports can be disabled globally with the disable sflow command.

Example

The following command disables sFlow sampling on port 3:1:

disable sflow ports 3:1

History

This command was first available in ExtremeWare 7.3.0.

Platform Availability

This command is available only on the “i” series platforms.
disable sys-health-check

disable sys-health-check

Description
Disables the BlackDiamond system health checker.

NOTE
This command is available only on the BlackDiamond switches.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
If the system health checker is disabled, it does not test I/O modules, MSM modules, and the backplane for system faults.

Example
The following command disables the BlackDiamond system health checker:
disable sys-health-check

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on BlackDiamond switches only.
disable syslog

disable syslog

Description
Disables logging to all remote syslog server targets.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
Disables logging to all remote syslog server targets, but not to the switch targets. This setting is saved in FLASH, and will be in effect upon boot-up.

Example
The following command disables logging to all remote syslog server targets:

disable syslog

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable temperature-logging

disable temperature-logging

Description
Stops recording the celsius system temperature to the syslog for the BlackDiamond and Alpine systems. (The temperature is recorded in degrees celsius.)

NOTE
This command is available only on modular switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
Use this command to stop recording the system temperature to the syslog.
If you have already enabled temperature logging, and you want to view the current temperature of the system, do the following:

1 Disable the temperature logging feature using the following command:
   disable temperature-logging
2 Re-enable the temperature logging feature using the following command:
   enable temperature-logging
3 Display the syslog using the following command:
   show log

Example
The following command stops recording the system temperature to the syslog:
disable temperature-logging

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This is supported and the command syntax changed from disable log temperature in ExtremeWare 7.1.0.
Platform Availability

This command is available on modular switches only.
disable transceiver-test

For an Alpine switch:

   disable transceiver-test [all | slot <slot number> {backplane} ]

For a BlackDiamond switch:

   disable transceiver-test [all | slot <slot number> | msm-a | msm-b]

**Description**

Disables the integrity testing of the transceivers used for communication between the ASICs and the CPU on an MSM or an SMMi module.

**NOTE**

This command is available only on modular switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all of the slots in the chassis.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies a single slot in the chassis.</td>
</tr>
<tr>
<td>backplane</td>
<td>Specifies the backplane of the chassis.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies the MSM module installed in slot A.</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies the MSM module installed in Slot B.</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Usage Guidelines**

To determine if you have the transceiver test enabled and the failure action the switch takes, use the `show switch` command. The following is sample transceiver test output:

```
Transceiver Diag: Enabled. Failure action: log only
```

To display the transceiver test statistics, use the `show diagnostics sys-health-check` command. The following is sample output:

```
Transceiver system health diag result
Pass/Fail Counters Are in HEX
Slot Cardtype Cardstate Test Pass Fail Time_last_fail
---- -------- --------- ---- -------- -------- --------------
  slot 1 Unknown
  slot 2 Unknown
  slot 3 FM8V Operational MAC 2b81b 0
```
disable transceiver-test

For ExtremeWare 6.2.2b108:

The default for the transceiver test is enabled. The test is enabled two minutes after the switch boots or immediately after you enable the test.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the transceiver test is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, the transceiver test is enabled. You must manually disable the transceiver test if you want the feature disabled.

**Example**

The following command disables the transceiver test on slot 4 of a modular switch:

disable transceiver-test slot 4

**History**

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available on modular switches only.
enable cli-config-logging

enable cli-config-logging

Description
Enables the logging of CLI configuration commands to the Syslog for auditing.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
ExtremeWare allows you to record all configuration changes and their sources that are made using the CLI by way of Telnet or the local console. The changes are logged to the system log. Each log entry includes the user account name that performed the changes and the source IP address of the client (if Telnet was used). Configuration logging applies only to commands that result in a configuration change.

To view the status of configuration logging on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for configuration logging.

Example
The following command enables the logging of CLI configuration commands to the Syslog:

```
enable cli-config-logging
```

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable flowstats

Description
Enables the flow statistics feature on the switch.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
None

Example
The following command enables NetFlow statistics feature on this switch:
```
enable flowstats
```

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms.
enable flowstats filter ports

enable flowstats filter <filter#> ports <portlist> {ingress | egress}

Description
Enables a specified flow record filter for the specified ports.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter#</td>
<td>Specifies the flow record filter that should be enabled.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports or slots and ports for which the filter should be enabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>ingress</td>
<td>Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to inbound flows on the SONET port(s).</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the PoS module.</td>
</tr>
<tr>
<td>egress</td>
<td>Use this keyword to specify that the filter being enabled or disabled is one of the eight filters to be applied to outbound flows on the SONET port(s).</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the PoS module.</td>
</tr>
</tbody>
</table>

Default
For the PoS module, filter #1 is enabled on all SONET ports, and the remaining filters are disabled.
For other switches or modules, filters are enabled by default when they are configured.

Usage Guidelines
The filter# parameter is an integer in the range [1-8]. A filter must be enabled to match a flow. For “i” series devices other than the PoS module, these apply only to outbound flows.

For each SONET port on a PoS module, sixteen filters are supported—eight filters for ingress flows and another eight filters for egress flows. The filter# parameter and either the ingress or egress keyword are used to identify the particular filter that is being disabled.

One of either the ingress or egress keywords are required for SONET ports.

Example
The following command enables filter 3 for ports 1-8 on the switch:

```
enable flowstats filter 3 ports 1-8
```

History
This command was first available in ExtremeWare 6.1.5b20 for the PoS module only.
This command was first available in ExtremeWare 6.2 for all “i” series platforms.
**Platform Availability**

This command is available on "i" series platforms.
enable flowstats ping-check

   enable flowstats ping-check {<group#>}

Description
Enables the flow statistics ping-check function for a specified group of collector devices.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>group#</th>
<th>Specifies the export group for which the ping-check function should be enabled.</th>
</tr>
</thead>
</table>

Default
Enabled

Usage Guidelines
If a flow-collector device is repeatedly unresponsive to ping requests, it is temporarily removed from the distribution list for any export groups of which it is a member. The device will be returned to the distribution list automatically when subsequent ping-checks are successful.

On the PoS module, if you do not include a group number, ping-check is enabled for all export groups.

Example
The following command enables the ping-check function for export group 3.

```
enable flowstats ping-check 3
```

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms.
enable flowstats ports

    enable flowstats ports <portlist>

Description
Enables the flow statistics function on the specified ports.

NOTE
This command is available only on the "i" series switches.

Syntax Description

| portlist | Specifies a list of ports or slots and ports for which the flowstats function should be enabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default
Disabled

Usage Guidelines
On the PoS module, flow statistics are only collected on SONET ports that are configured to use the IP control protocol, IPCP, (in other words, flow statistics are not collected on ports that are configured to use the bridging control protocol, BCP). Also, there are no configuration restrictions that prohibit enabling of the flow statistics function on ports that are not configured to use IPCP; statistics are not collected on those ports.

Example
The following command enables the ping-check function for all export groups.

    enable flowstats ping-check

History
This command was first available in ExtremeWare 6.1.5b20 for the PoS module
This command was modified in ExtremeWare 6.2 to support all “i” series platforms.

Platform Availability
This command is available on “i” series platforms.
enable log debug-mode

enable log debug-mode

**Description**
Enables debug mode. The switch allows debug events included in log filters to be logged.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled

**Usage Guidelines**
This command enables debug mode. Debug mode must be enabled prior to logging debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

**Example**
The following command enables debug mode:

```
enable log debug-mode
```

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
enable log display

 enable log display

Description
Enables a running real-time display of log messages on the console display.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
If you enable the log display on a terminal connected to the console port, your settings will remain in effect even after your console session is ended (unless you explicitly disable the log display).

You configure the messages displayed in the log using the configure log display, or configure log target console-display commands.

In ExtremeWare 7.1.0, the ability to control logging to different targets was introduced. The new command equivalent to enable log display is the following:

enable log target console-display

To change the log filter association, severity threshold, or match expression for messages sent to the console display, use the configure log target console-display command

Example
The following command enables a real-time display of log messages:

enable log display

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable log target

    enable log target [console-display | memory-buffer | nvram | session | syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]]

**Description**
Start sending log messages to the specified target.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog target.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0 ... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
</tbody>
</table>

**Default**
Enabled, for memory buffer and NVRAM; all other targets are disabled by default.

**Usage Guidelines**
This command starts sending messages to the specified target. By default, the memory-buffer and the NVRAM targets are enabled. Other targets must be enabled before messages are sent to those targets.

Configuration changes to the session target are in effect only for the duration of the console display or telnet session, and are not saved in FLASH. Others are saved in FLASH.

In earlier versions of ExtremeWare, a similar command was used to enable displaying the log on the console. That command:

    enable log display

is equivalent to:

    enable log target console-display

**Example**
The following command enables log messages on the current session:

    enable log target session

**History**
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability

This command is available on all platforms.
**enable rmon**

```
enable rmon
```

**Description**

Enables the collection of RMON statistics on the switch.

**Syntax Description**

This command has no arguments or variables.

**Default**

By default, RMON is disabled. However, even in the disabled state, the switch responds to RMON queries and sets for alarms and events. By enabling RMON, the switch begins the processes necessary for collecting switch statistics.

**Usage Guidelines**

The switch supports four out of nine groups of Ethernet RMON statistics. In an enabled state, the switch responds to the following four groups:

- **Statistics**—The RMON Ethernet Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts, and errors on a LAN segment or VLAN.
- **History**—The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.
- **Alarms**—The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds may be auto calibrated or set manually.
- **Events**—The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

**NOTE**

*You can use the RMON features of the system only if you have an RMON management application and have enabled RMON on the switch.*

RMON requires one probe per LAN segment, and standalone RMON probes have traditionally been expensive. Therefore, Extreme’s approach has been to build an inexpensive RMON probe into the agent of each system. This allows RMON to be widely deployed around the network without costing more than traditional network management. The switch accurately maintains RMON statistics at the maximum line rate of all of its ports.

For example, statistics can be related to individual ports. Also, because a probe must be able to see all traffic, a stand-alone probe must be attached to a nonsecure port. Implementing RMON in the switch means that all ports can have security features enabled.
To view the status of RMON polling on the switch, use the `show management` command. The `show management` command displays information about the switch including the enable/disable state for RMON polling.

**Example**

The following command enables the collection of RMON statistics on the switch:

```
enable rmon
```

**History**

This command was first available in ExtremeWare 4.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable sflow

   enable sflow

Description
Globally enables sFlow statistical packet sampling.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command enables sFlow globally on the switch. Sflow must be enabled globally before a “per data source” sFlow can be enabled through the following command:

   enable sflow ports <portlist>

Example
The following command enables sFlow sampling globally:

   enable sflow

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms.
enable sflow backoff-threshold

Description
Enables the sFlow backoff-threshold feature, limiting the maximum number of packets sent to the sFlow collector per second.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command enables the backoff threshold feature, which is used to limit the number of packets sent to the sFlow collector in a second. The backoff threshold is set by using the following command:

customdefine sflow backoff-threshold

If the number of packets sent to the collector exceeds the limit set by the configure sflow backoff-threshold command, the sampling rate will be doubled.

The backoff threshold is enabled when the enable sflow backoff-threshold command is executed and the sample frequency set by the configure sflow sample-rate command is greater than 0 (zero).

The following command disables the sFlow backoff threshold feature:

disable sflow backoff-threshold

Example
The following command enables the sFlow backoff threshold feature:

enable sflow backoff-threshold

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms.
enable sflow ports

   enable sflow ports <portlist>

Description

Enables sFlow statistical packet sampling on one or more ports.

NOTE

This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Specifies a list of ports or slots and ports. May be in the form 1, 2, 3-5, 2-5, 2-6-2-8.</th>
</tr>
</thead>
</table>

Default

Disabled

Usage Guidelines

This command enables sFlow on a particular list of ports. You will also need to enable sFlow globally in order to gather statistics and send the data to the collector. Traffic is sampled on enabled ports only. Once sFlow is enabled globally, and on the ports of interest, sampling and polling will begin.

Use the following command to enable sFlow globally:

   enable sflow

Example

The following command enables sFlow sampling on the port 3:1:

   enable sflow portlist 3:1

History

This command was first available in ExtremeWare 7.3.0.

Platform Availability

This command is available on “i” series platforms.
enable sys-health-check

Description
Enables the BlackDiamond system health checker.

NOTE
This command is available only on the BlackDiamond switches.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
The system health checker tests I/O modules, MSM modules, and the backplane by forwarding packets every 4 seconds. Additional checking for the validity of these packets is completed by performing a checksum.

By isolating faults to a specific module, MSM, or backplane connection, the system health checker prevents corrupted packets from being propagated to the CPU, upper layer modules, or the rest of your network. If you observe a failure, please contact Extreme Technical Support.

Depending on how you have configured the system health checker, failed system health checks may generate critical error messages in the syslog, and may also send a trap and/or shut down the system. The system health checker will continue to periodically forward test packets to failed components. If auto-recovery is configured, the system will attempt to automatically reset the faulty module and bring it back online.

In ExtremeWare versions prior to 6.2, you cannot use both mirroring and the system health checker at the same time. If you configure mirroring with the system health checker enabled, the health checker will indicate that it has been disabled by sending a message to the syslog. In version 6.2 or later, this restriction does not apply.

To configure the health checker, use the following command:

```
configure sys-health-check [alarm-level [card-down | default | log | system-down | traps] | auto-recovery <number of tries>]
```

The alarm-level and auto-recovery options are mutually exclusive; configuring an alarm-level disables auto-recovery, and configuring auto-recovery overrides the alarm-level setting.

Example
The following command enables the BlackDiamond system health checker:

```
enable sys-health-check
```
History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on BlackDiamond switches only.
enable syslog

enable syslog

Description
Enables logging to all remote syslog host targets.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
In order to enable remote logging, you must do the following:

- Configure the syslog host to accept and log messages.
- Enable remote logging by using the enable syslog command.
- Configure remote logging by using the configure syslog command.

When you use the enable syslog command, the exporting process of the syslog begins. This command also determines the initial state of an added remote syslog target.

Example
The following command enables logging to all remote syslog hosts:

```
enable syslog
```

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable temperature-logging

Description
Records the system temperature in celsius for the BlackDiamond and Alpine systems to the syslog.

NOTE
This command is available only on modular switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
When you enable temperature logging, the temperature is recorded every hour.

To view the temperature of the system, use the show log command. The following is sample temperature output from the show log command:

```
06/12/2003 19:50:59.00 <Info:ELRP> Current temperature reading [197] is 49C.
06/12/2003 18:50:59.00 <Info:ELRP> Current temperature reading [196] is 48C.
06/12/2003 17:50:59.00 <Info:ELRP> Current temperature reading [195] is 48C.
```

To clear all of the log statistics, including the system temperature output, use the clear log command. Since the temperature is recorded based on the time you enabled temperature logging, it may take up to one hour for a new temperature to be recorded to the syslog.

If you already enabled temperature logging, and you want to view the current temperature of the system, do the following:

1. Disable the temperature logging feature using the following command:
   ```
   disable temperature-logging
   ```
2. Re-enable the temperature logging feature using the following command:
   ```
   enable temperature-logging
   ```
3. Display the syslog using the following command:
   ```
   show log
   ```

Example
The following command records the system temperature to the syslog:

```
enable temperature-logging
```
**History**

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

The command was supported and the syntax changed from `enable log temperature` in ExtremeWare 7.1.0.

**Platform Availability**

This command is available on modular switches only.
enable transceiver-test

For an Alpine switch:

```
enable transceiver-test [all | slot <slot number> | backplane]
```

For a BlackDiamond switch:

```
enable transceiver-test [all | slot <slot number> | msm-a | msm-b]
```

**Description**

Enables an integrity test of the transceivers used for communication between the ASICs and the CPU on an MSM or an SMMi module.

**NOTE**

*This command is available only on modular switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all of the slots in the chassis.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies a single slot in the chassis.</td>
</tr>
<tr>
<td>backplane</td>
<td>Specifies the backplane of the chassis.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies the MSM module installed in slot A.</td>
</tr>
<tr>
<td>msm-b</td>
<td>Specifies the MSM module installed in Slot B.</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Usage Guidelines**

The `enable transceiver-test` command is a useful diagnostic tool. Use this command if you suspect a problem with the system and to test the integrity of the transceivers.

To determine if you have the transceiver test enabled and the failure action the switch takes, use the `show switch` command. The following is sample transceiver test output:

```
Transceiver Diag: Enabled. Failure action: log only
```

To display the transceiver test statistics, use the `show diagnostics sys-health-check` command. The following is sample output:

```
Transceiver system health diag result
Pass/Fail Counters Are in HEX
Slot Cardtype Cardstate Test Pass Fail Time_last_fail
---- --------- --------- ---- -------- ----------- -------
slot 1 Unknown
```
enable transceiver-test

For ExtremeWare 6.2.2b108:

The default for the transceiver test is enabled. The test is enabled two minutes after the switch boots or immediately after you enable the test.

For ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0:

The default for the transceiver test is disabled. If you load your saved ExtremeWare 6.2.2b108 configurations onto a switch with ExtremeWare 6.2.2b134 or ExtremeWare 7.1.0 or later, the transceiver test is enabled. You must manually disable the transceiver test if you want the feature disabled.

**Example**

The following command enables the transceiver test on slot 4 of a modular switch:

```
enable transceiver-test slot 4
```

**History**

This command was first available in ExtremeWare 6.2.2b108.

The default for this command was changed to disabled in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available only on modular switches.
save log

save log file ascii <local-filespec> {messages [memory-buffer | nvram]} {severity <severity> {only}} {starting [date <date> time <time> | date <date> | time <time>]} {ending [date <date> time <time> | date <date> | time <time>]} {match <match-expression>} {format <format>} {chronological}

Description
Saves the current log messages to the local file system.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>local-filespec</td>
<td>Specifies the local file name for storing the log.</td>
</tr>
<tr>
<td>messages</td>
<td>Specifies the location from which to display the log messages.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Show messages stored in volatile memory.</td>
</tr>
<tr>
<td>nvram</td>
<td>Show messages stored in NVRAM</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level to display (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only the specified severity level is to be displayed</td>
</tr>
<tr>
<td>starting</td>
<td>Show messages with timestamps equal to or greater than that specified</td>
</tr>
<tr>
<td>date</td>
<td>Specifies the date, where date is &lt;month (1-12)&gt; / &lt;day&gt; / &lt;year (yyyy)&gt;</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time, where time is &lt;hour (0-23)&gt; : &lt;minute (0-59)&gt; : &lt;seconds&gt;</td>
</tr>
<tr>
<td>match-expression</td>
<td>Specifies a regular expression. Only messages that match the regular expression will be displayed.</td>
</tr>
<tr>
<td>format</td>
<td>Specifies a format to use to override the format configured for the memory buffer.</td>
</tr>
<tr>
<td>chronological</td>
<td>Specifies uploading log messages in ascending chronological order (oldest to newest).</td>
</tr>
</tbody>
</table>

Default
The following defaults apply:

- messages—memory buffer
- severity—informational severity messages and higher
- starting, ending—if not specified, no timestamp restriction
- match—no restriction
- format—the format configured with the configure log target format command
- chronological—if not specified, show messages in order from newest to oldest

Usage Guidelines
This command is similar to the show log command, but instead of displaying the log contents on the command line, this command saves the log to a local file. For more details on most of the options of this
command, see the command `show log` on page 775, and for the `format` option see the command `configure log target format` on page 688.

**Example**

The following command saves messages with a critical severity to the filename `switch4critical.log`:

```bash
save log switch4critical.log critical
```

The following command saves messages with warning, error, or critical severity to the filename `switch4warn.log`:

```bash
save log switch4warn.log warning
```

The following command saves messages starting August 1, ending August 31, containing the string “slot 2” in order of oldest to newest to the filename `switch4aug03.log`:

```bash
save log switch4aug03.log starting date 8/1 ending date 8/31 match "slot 2"
```

**History**

This command was first available in ExtremeWare 7.1.0

**Platform Availability**

This command is available on MSM64si systems
show flowstats

Description
Displays status information for the flow statistics function.

NOTE
This command is available only on the “i” series switches.

Syntax Description
N/A

Default
Displays summary statistics information for all ports.

Usage Guidelines
The command with no arguments displays flowstats configuration information for all ports. The information is displayed in a format similar to the flowstats command syntax. The following information is displayed:

- Whether the flowstats feature is enabled or disabled
- Whether flowstats is enabled or disabled for individual ports
- The configuration of flow-collector devices (NetFlow Server Config)
- NetFlow Timeout configurations
- Whether NetFlow Filters are enable or disabled
- NetFlow filter specifications
- NetFlow ping-check configuration

Example
The show flowstats command with no options, for a switch with NetFlow statistics enabled on ports 1, 40, and 43, displays output similar to the following:

Summit48i: show flowstats

Flowstats enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Filter</th>
<th>proto</th>
<th>timeout</th>
<th>group</th>
<th>OverflowPkts</th>
<th>flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>IP</td>
<td>5</td>
<td>3</td>
<td>N/A</td>
<td>EIA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DestIP: 10.203.0.1/255.255.255.255</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DestPort: any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SrcIP: any</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SrcPort: any</td>
<td></td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>-</td>
<td>5</td>
<td>1</td>
<td>N/A</td>
<td>EIA</td>
</tr>
</tbody>
</table>
Dest/Src Info: match-all-flows

43  3  TCP  5  32  N/A  EIA
DestIP:  10.0.1.1/255.255.255.254  DestPort: any
SrcIP:  10.201.32.1/255.255.255.255  SrcPort: any

Flags:  E - Enable, D - Disable; I - Ingress, S - Egress; A - Aggregation

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms.
show flowstats

show flowstats <portlist>

Description
Displays status information for the flow statistics function for specified ports.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| portlist | Specifies a list of ports or slots and ports for which flow statistics should be displayed. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default
N/A

Usage Guidelines
This command displays flowstats configuration information for an individual port. The information is displayed in a format similar to the flowstats command syntax. The following information is displayed:

- Whether the flowstats feature is enabled or disabled
- Whether flowstats is enabled or disabled for the specified port
- NetFlow Timeout configuration for the port
- Whether NetFlow Filters are enabled or disabled for the port
- NetFlow filter specifications for the port

Example
The following command displays statistics for ports 1, 40, and 48:

Summit48i: show flowstats 1, 40, 48
Flowstats enabled

<table>
<thead>
<tr>
<th>Port</th>
<th>Filter</th>
<th>proto</th>
<th>timeout</th>
<th>group</th>
<th>OverflowPkts</th>
<th>flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>3</td>
<td>IP</td>
<td>5</td>
<td>3</td>
<td>N/A</td>
<td>EIA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DestIP: 10.203.0.1/255.255.255.255</td>
<td>DestPort: any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SrcIP: any</td>
<td>SrcPort: any</td>
</tr>
<tr>
<td>40</td>
<td>8</td>
<td>-</td>
<td>5</td>
<td>1</td>
<td>N/A</td>
<td>EIA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Dest/Src Info: match-all-flows</td>
<td></td>
</tr>
<tr>
<td>48</td>
<td>1</td>
<td>TCP</td>
<td>20</td>
<td>1</td>
<td>N/A</td>
<td>EIA</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>DestIP: 10.201.26.0/255.255.255.0</td>
<td>DestPort: any</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>SrcIP: 10.201.31.0/255.255.255.0</td>
<td>SrcPort: any</td>
</tr>
</tbody>
</table>
show flowstats

48         2       UDP          20         1         N/A           EIA
  DestIP:     10.201.26.0/  255.255.255.0         DestPort: any
  SrcIP:      10.201.31.0/  255.255.255.0          SrcPort: any
Flags:  E - Enable, D - Disable; I - Ingress, S - Egress; A - Aggregation

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms.
show flowstats export

    show flowstats export [ detail |{<group number> detail} ]

Description
Displays configuration information an export group.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| group number | Specifies a group number for which configuration information should be displayed. |

Default
N/A

Usage Guidelines
The information displayed by this command is displayed in a format similar to the configure flowstats export command. The following information is displayed:

- Whether the flowstats feature is enabled or disabled
- The configuration of flow-collector devices for the export group (NetFlow Server Config)
- NetFlow ping-check configuration

Example
The following command displays detailed configuration information for export group 1:

    show flowstats export 1 detail

Group: 1  ping-check: enable  Source ip_address: 10.201.26.217
ip_address 10.201.31.237   udp_port 9995 status up 0 times, outpkts 256

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms.
show log

show log {messages [memory-buffer | nvram]} {severity <severity> {only}} 
{starting [date <date> time <time> | date <date> | time <time>]} {ending 
[date <date> time <time> | date <date> | time <time>]} {match 
<match-expression>} {format <format>} {chronological}

**Description**
Displays the current log messages.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>messages</td>
<td>Specifies the target location from which to display the log messages.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Show messages stored in volatile memory (default).</td>
</tr>
<tr>
<td>nvram</td>
<td>Show messages stored in NVRAM.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level to display (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only the specified severity level is to be displayed</td>
</tr>
<tr>
<td>starting</td>
<td>Show messages with timestamps equal to or greater than that specified</td>
</tr>
<tr>
<td>date</td>
<td>Specifies the date, where date is &lt;month (1-12)&gt; / &lt;day&gt; / &lt;year (yyyy)&gt;</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time, where time is &lt;hour (0-23)&gt; / &lt;minute (0-59)&gt; / &lt;seconds&gt; / &lt;hundredths&gt;&gt;</td>
</tr>
<tr>
<td>ending</td>
<td>Show messages with timestamps equal to or less than that specified</td>
</tr>
<tr>
<td>match-expression</td>
<td>Specifies a regular expression. Only messages that match the regular expression will be displayed.</td>
</tr>
<tr>
<td>format</td>
<td>Specifies a format to use to override the format configured for the memory buffer.</td>
</tr>
<tr>
<td>chronological</td>
<td>Specifies displaying log messages in ascending chronological order (oldest to newest).</td>
</tr>
</tbody>
</table>

**Default**
The following defaults apply:
- messages—memory buffer
- severity—none (displays everything stored in the target)
- starting, ending—if not specified, no timestamp restriction
- match—no restriction
- format—the format configured with the configure log target format command
- chronological—if not specified, show messages in order from newest to oldest

**Usage Guidelines**
Switch configuration and fault information is filtered and saved to target logs, in a memory buffer, and in NVRAM. Each entry in the log contains the following information:
- Timestamp—records the month and day of the event, along with the time (hours, minutes, seconds, and hundredths).
- Severity Level—indicates the urgency of a condition reported in the log. Table 15 describes the severity levels assigned to events.
• Component, Subcomponent, and Condition Name—describes the subsystem in the software that
  generates the event. This provides a good indication of where a fault might lie.

• Message—a description of the event occurrence. If the event was caused by a user, the user name is
  also provided.

This command displays the messages stored in either the internal memory buffer or in NVRAM. The
messages shown can be limited by specifying a severity level, a time range, or a match expression.
Messages stored in the target have already been filtered as events occurred, and specifying a severity or
match expression on the show log command can only further limit the messages shown.

If the messages keyword is not present, the messages stored in the memory-buffer target are displayed.
Otherwise, the messages stored in the specified target are displayed.

If the only keyword is present following the severity value, then only the events at that exact severity
are included. Without the only keyword, events at that severity or more urgent are displayed. For
example, severity warning implies critical, error, or warning, whereas severity warning only implies
only warning.

Messages whose timestamps are equal or later than the starting time and are equal or earlier than the
specified ending time will be shown if they also pass the severity requirements and match expression, if
specified.

If the format phrase is specified, this format overrides the format already configured for the specified
log. See the command configure log target format on page 688 for more information on specifying
a format.

If a match phrase is specified, the formatted message must match the simple regular expression
specified by match-expression for it to be shown.

A simple regular expression is a string of single characters including the dot character (.), which are
optionally combined with quantifiers and constraints. A dot matches any single character while other
characters match only themselves (case is significant). Quantifiers include the star character (*) that
matches zero or more occurrences of the immediately preceding character or dot. Constraints include
the caret character (^) that matches at the beginning of a message, and the currency character ($) that
matches at the end of a message. Bracket expressions are not supported. There are a number of sources
available on the Internet and in various language references describing the operation of regular
expressions.

If the chronological keyword is specified, messages are shown from oldest to newest; otherwise,
messages are displayed newest to oldest.

Severity Level. The severity levels are critical, error, warning, notice, and info, plus three
severity levels for extended debugging, debug-summary, debug-verbose, and debug-data. In log
messages, the severity levels are shown by four letter abbreviations. The abbreviated forms are:

• Critical—Crit
• Error—Erro
• Warning—Warn
• Notice—Noti
• Info—Info
• Debug-Summary—Summ
• Debug-Verbose—Verb
• Debug-Data—Data
The three severity levels for extended debugging, debug-summary, debug-verbose, and debug-data, require that debug mode be enabled (which may cause a performance degradation). See the command enable log debug-mode on page 752.

Table 15: Severity Levels Assigned by the Switch

<table>
<thead>
<tr>
<th>Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>A serious problem has been detected which is compromising the operation of the system and that the system can not function as expected unless the situation is remedied. The switch may need to be reset.</td>
</tr>
<tr>
<td>Error</td>
<td>A problem has been detected which is interfering with the normal operation of the system and that the system is not functioning as expected.</td>
</tr>
<tr>
<td>Warning</td>
<td>An abnormal condition, not interfering with the normal operation of the system, has been detected which may indicate that the system or the network in general may not be functioning as expected.</td>
</tr>
<tr>
<td>Notice</td>
<td>A normal but significant condition has been detected, which signals that the system is functioning as expected.</td>
</tr>
<tr>
<td>Info (Informational)</td>
<td>A normal but potentially interesting condition has been detected, which signals that the system is functioning as expected and simply provides information or confirmation about the condition.</td>
</tr>
<tr>
<td>Debug-Summary</td>
<td>A condition has been detected that may interest a developer determining the reason underlying some system behavior.</td>
</tr>
<tr>
<td>Debug-Verbose</td>
<td>A condition has been detected that may interest a developer analyzing some system behavior at a more verbose level than provided by the debug summary information.</td>
</tr>
<tr>
<td>Debug-Data</td>
<td>A condition has been detected that may interest a developer inspecting the data underlying some system behavior.</td>
</tr>
</tbody>
</table>

1. In ExtremeWare version 7.1.0, the levels alert and emergency were deprecated. The equivalent level is critical.

Log entries remain in the NVRAM log after a switch reboot. Issuing a clear log command does not remove these static entries. To remove log entries from NVRAM, use the following command:

    clear log messages nvram

**NOTE**

If you download a configuration, the output of the show log command might not completely display commands longer than 240 characters. This is a display problem; the configuration loads correctly.

**NOTE**

If you download a configuration and use the show log command to view the parsing of the configuration, the log does not display the entire parsing. This is a display problem; the configuration parses and loads correctly.

**Example**

The following command displays messages with a critical severity:

    show log critical
The following command displays messages with warning, error, or critical severity:

```
show log warning
```

The following command displays messages containing the string “slot 2”:

```
show log match "slot 2"
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.2 to include the chronological option.

This command was modified in ExtremeWare 7.1.0 to include the messages, severity, only, starting, ending, match, and format options.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to include the messages, severity, only, starting, ending, chronological, match, and format options.

In ExtremeWare 7.3e, the Summit 300-48 replaced the priority keyword with the severity keyword.

**Platform Availability**

This command is available on all platforms.
show log components

    show log components (<event component> | all)

Description
Display the name, description and default severity for all components.

Syntax Description

<table>
<thead>
<tr>
<th>event component</th>
<th>Specifies component to display.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Displays all components.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command displays the name, description, and default severity defined for the specified components and subcomponents.

Example
The following command displays the log components:

```
show log components
```

The output produced by the `show log components` command is similar to the following:

```
Component | Title                                           | Severity Threshold
-----------|-------------------------------------------------|----------------------
          |                                                | Error
BGP        | Border Gateway Protocol                         | Error
Dampening  | BGP Route Flap Dampening                        | Error
Event      | BGP Finite State Machine                        | Error
Keepalive  | BGP Keepalive Messages                           | Error
Message    | BGP Messages (Open, Update, Notification)       | Error
Misc       | BGP Miscellaneous (Import, Aggregate, NextHop)  | Error
UpdateIn   | BGP Incoming Update Messages                     | Error
UpdateOut  | BGP Outgoing Update Messages                     | Error
Bridge     | Layer 2 Bridging                                | Error
Learning   | Layer 2 Bridge Learning                         | Error
EAPS       | Ethernet Automatic Protection Switching (EAPS)  | Error
            | EAPS MSM Failover                               | Error
            | EAPS SharedPort Domain                          | Error
EDP        | Extreme Discovery Protocol (EDP)                | Error
ELRP       | Extreme Loop Recovery Protocol (ELRP)           | Error
ESRP       | Extreme Standby Router Protocol (ESRP)          | Notice
            | ESRP Aware Processing                           | Notice
            | ESRP PDU Tx/Rx                                 | Error
            | ESRP MSM Failover                              | Error
            | ESRP State Transitions                          | Notice
```
### Commands for Status Monitoring and Statistics

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
<th>Availability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tracking</td>
<td>ESRP Tracking</td>
<td>Error</td>
</tr>
<tr>
<td>FDB</td>
<td>Forwarding Data Base</td>
<td>Error</td>
</tr>
<tr>
<td>IP</td>
<td>IP FDB</td>
<td>Error</td>
</tr>
<tr>
<td>IPMC</td>
<td>IP Multicast FDB</td>
<td>Error</td>
</tr>
<tr>
<td>Replacement FDB</td>
<td>Replacement FDB</td>
<td>Error</td>
</tr>
<tr>
<td>IGMP</td>
<td>Internet Group Management Protocol</td>
<td>Error</td>
</tr>
<tr>
<td>Snooping</td>
<td>IGMP Snooping</td>
<td>Error</td>
</tr>
<tr>
<td>IP AccessList</td>
<td>IP Access List</td>
<td>Error</td>
</tr>
<tr>
<td>Forwarding</td>
<td>IP Forwarding</td>
<td>Error</td>
</tr>
<tr>
<td>Log</td>
<td>Event Management System (EMS)</td>
<td>Error</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
<td>Error</td>
</tr>
<tr>
<td>Event</td>
<td>OSPF Events</td>
<td>Error</td>
</tr>
<tr>
<td>Hello</td>
<td>OSPF Hello</td>
<td>Error</td>
</tr>
<tr>
<td>LSA</td>
<td>OSPF Link-State Advertisement</td>
<td>Error</td>
</tr>
<tr>
<td>Neighbor</td>
<td>OSPF Neighbor</td>
<td>Error</td>
</tr>
<tr>
<td>SPF</td>
<td>OSPF Shortest Path First</td>
<td>Error</td>
</tr>
<tr>
<td>SNTP</td>
<td>Simple Network Time Protocol</td>
<td>Warning</td>
</tr>
<tr>
<td>STP</td>
<td>Spanning-Tree Protocol (STP)</td>
<td>Error</td>
</tr>
<tr>
<td>InBPDU</td>
<td>STP In BPDU subcomponent</td>
<td>Warning</td>
</tr>
<tr>
<td>OutBPDU</td>
<td>STP Out BPDU subcomponent</td>
<td>Warning</td>
</tr>
<tr>
<td>System</td>
<td>STP System subcomponent</td>
<td>Error</td>
</tr>
</tbody>
</table>

### History

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

### Platform Availability

This command is available on all platforms.
show log configuration

Description
Displays the log configuration for switch log settings, and for certain targets.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command displays the log configuration for all targets. The state of the target, enabled or disabled is displayed. For the enabled targets, the associated filter, severity, match expression, and format is displayed. The debug mode state of the switch is also displayed.

Example
The following command displays the configuration of all the log targets:
show log configuration

The output produced by the command is similar to the following:

```
Severities: Critical, Error, Warning, Notice, Info, Debug-Summary, Debug-Verbose, Debug-Data

Log Target      : session 1028 (10.38.0.42)
   Enabled     : no
   Filter Name : DefaultFilter
   Severity    : info (through critical)
   Match       : (none)

Log Target      : console-display
   Enabled     : no
   Filter Name : DefaultFilter
   Severity    : info (through critical)
   Match       : (none)
```

Remote syslog targets are disabled by default.
Debug-Mode is disabled.
**History**

This command was first available in ExtremeWare 2.0.

The additional EMS information was added in ExtremeWare 7.1.0

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e

**Platform Availability**

This command is available on all platforms.
show log configuration filter

    show log configuration filter (<filter name>)

Description
Displays the log configuration for the specified filter.

Syntax Description

| filter name | Specifies the filter to display. |

Default
If no options are specified, the command displays the configuration for all filters.

Usage Guidelines
This command displays the configuration for filters.

Example
The following command displays the configuration for the filter, myFilter:

    show log configuration filter myFilter

The output of this command is similar to the following:

```
Log Filter Name: myFilter

I/ E Comp. Sub-comp. Condition Severity Parameter(s) Even If
- ------- ----------- --------------- --------  ------ --------------------- -
I  BGP Event * CEWNISVD Type Value Missing
L4 80
E STP OutBPDU * CEWNISVD R-Nbr 10.1.2.0 / 24 N
I STP * * ------- N

Include/Exclude: I - Include, E - Exclude
Component Unreg: * - Component/Subcomponent is not currently registered
Severity Values: C - Critical, E - Error, W - Warning, N - Notice, I - Info
Debug Severity: S - Debug-Summary, V - Debug-Verbose, D - Debug-Data
(Caution: Debug Severities require "enable log debug-mode")
Parameter Flags: S - Source, D - Destination (as applicable)
I - Ingress, E - Egress, B - BGP
Parameter Types: Port - Physical Port list, Slot - Physical Slot #
MAC - MAC address, IP - IP Address/netmask, Mask - Netmask
VID - Virtual LAN ID (tag), VLAN - Virtual LAN name
L4 - Layer-4 Port #, Num - Number, Str - String
Nbr - Neighbor, Rtr - Rooterid, EAPS - EAPS Domain
Even If Parameters Missing: Y - Yes, N - No, or no parameters specified
```

The above output shows three filter items. The first item includes events from the BGP.Event subcomponent of severity notify and greater where the BGP neighbor matches the 10.1.2.0/24 subnet and the L4 port value is 80. (BGP is supported only on “i” series switches.) The second item excludes all
events from the STP.OutBPDU component. The third item includes the remaining events from the STP component. The severity value is show as “-”, indicating that the component’s default severity threshold controls which messages are passed.

**History**

This command was first available in ExtremeWare 7.1.0

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show log configuration target

show log configuration target {console-display | memory-buffer | nvram | session | syslog <host name/ip> {:<udp-port}[local0 ... local7]}

Description
Displays the log configuration for the specified target.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Show the log configuration for the console display.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Show the log configuration for volatile memory.</td>
</tr>
<tr>
<td>nvram</td>
<td>Show the log configuration for NVRAM.</td>
</tr>
<tr>
<td>session</td>
<td>Show the log configuration for the current session (including console display).</td>
</tr>
<tr>
<td>syslog</td>
<td>Show the configuration for the specified syslog target.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0 ... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
</tbody>
</table>

Default
If no options are specified, the command displays the configuration for the current session and console display.

Usage Guidelines
This command displays the log configuration for the specified target. The associated filter, severity, match expression, and format is displayed.

Example
The following command displays the log configuration:

```
show log configuration target
```

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show log counters

show log counters {<event condition> | [all | <event component>] {severity <severity> {only}}}

Description
Displays the incident counters for events.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event condition</td>
<td>Specifies the event condition to display.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all events are to be displayed.</td>
</tr>
<tr>
<td>event component</td>
<td>Specifies that all the events associated with a particular component or subcomponent should be displayed.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level of events to display (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only events of the specified severity level are to be displayed</td>
</tr>
</tbody>
</table>

Default
If severity is not specified, then events of all severity are displayed. If detail is not specified, then summary only information is displayed.

Usage Guidelines
This command displays the incident counters for each event specified. Two incident counters are displayed. One counter displays the number of times an event has occurred, and the other displays the number of times that notification for the event was made to the system (an incident record was injected into the system for further processing). Both incident counters reflect totals accumulated since reboot or since the counters were cleared using the clear log counters or clear counters command, regardless of whether it was filtered or not.

This command also displays a reference count (the column titled \( R_f \) in the output). The reference count is the number of enabled targets receiving notifications of this event.

See the command show log on page 775 for more information about severity levels.

To get a listing of the event conditions in the system, use the following command:

show log events

To get a listing of the components present in the system, use the following command:

show log components

Example
The following command displays the event counters for event conditions of severity debug-summary or greater in the component STP.InBPDU:

show log counters stp.inbpdu severity debug-summary
The output produced by the above command is similar to the following:

<table>
<thead>
<tr>
<th>Comp</th>
<th>SubComp</th>
<th>Condition</th>
<th>Severity</th>
<th>Rf Notified</th>
<th>Occurred</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>InBPDU</td>
<td>PDUDrop</td>
<td>Error</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDUIgn</td>
<td>Debug-Summary</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PDUTrace</td>
<td>Info</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

The following command displays the event counters for the event condition `PDUDrop` in the component `STP.InBPDU`:

```
show log counters "STP.InBPDU.PDUDrop"
```

The output produced by the above command is similar to the following:

<table>
<thead>
<tr>
<th>Comp</th>
<th>SubComp</th>
<th>Condition</th>
<th>Severity</th>
<th>Rf Notified</th>
<th>Occurred</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>InBPDU</td>
<td>PDUDrop</td>
<td>Error</td>
<td>1</td>
<td>0</td>
</tr>
</tbody>
</table>

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show log events

  show log events {<event condition> | [all | <event component>] {severity <severity> {only}}} {detail}

Description
Displays information about the individual events (conditions) that can be logged.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>event condition</td>
<td>Specifies the event condition to display.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all events are to be displayed.</td>
</tr>
<tr>
<td>event component</td>
<td>Specifies that all the events associated with a particular component should be displayed.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level of events to display (if the keyword <code>only</code> is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only events of the specified severity level are to be displayed</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that detailed information, including the message format and parameter types, be displayed</td>
</tr>
</tbody>
</table>

Default
If severity is not specified, then events of all severity are displayed. If detail is not specified, then summary only information is displayed.

Usage Guidelines
This command displays the mnemonic, message format, severity, and parameter types defined for each condition in the event set specified.

See the command `show log` on page 775 for more information about severity levels.

When the `detail` option is specified, the message format is displayed for the event conditions specified. The message format parameters are replaced by the value of the parameters when the message is generated.

To get a listing of the components present in the system, use the following command:

  `show log components`

Example
The following command displays the event conditions of severity debug-summary or greater in the component `STP.InBPDU`:

  `show log events stp.inbpdu severity debug-summary`
The output produced by the above command is similar to the following:

<table>
<thead>
<tr>
<th>Comp</th>
<th>SubComp</th>
<th>Condition</th>
<th>Severity</th>
<th>Parameters</th>
</tr>
</thead>
<tbody>
<tr>
<td>STP</td>
<td>InBPDU</td>
<td>PDUTrace</td>
<td>Info</td>
<td>2 Total</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 - string</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1 - ports</td>
</tr>
</tbody>
</table>

"Port=%1%: %0%"

**History**

This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show memory

    show memory {detail}

Description
Displays the current system memory information.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies task-specific memory usage.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
A BlackDiamond or Summit switch must have 32MB of DRAM to support the features in ExtremeWare version 4.0 and above.

Viewing statistics regularly allows you to see how well your network is performing. If you keep simple daily records, you will see developing trends and notice problems arising before they cause major network faults. This way, statistics can help you get the best out of your network.

The `show memory` command displays the following information in a tabular format:

- System memory information including the total DRAM size of your system.
- Current memory (both free and allocated memory) used by the system and the users.
- Cumulative memory (both free and allocated memory) used by the users.
- Software packet memory statistics including the type of packet, the number of allocated and free packets, the number of packet failures, and data and other blocks.
- Memory utilization statistics including the total blocks of memory available and the memory being used on your system. You can review how your memory is being utilized For example you can view memory utilization for the system, management, ESRP, IP, and other system functions.

This information may be useful for your technical support representative if you experience a problem.

For version 2.0 and 4.0:
- The `detail` parameter is not available.

Depending on the software version running on your switch, additional or different memory information may be displayed.

Example
The following command displays current system memory information:

    show memory
History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show packet-mem-scan-recovery-mode

Description
Displays the recovery mode setting for slot’s that have packet memory scanning enabled.

NOTE
This command is available only on the BlackDiamond switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
The show packet-mem-scan-recovery-mode command displays the following information:
- Global settings for the system health check
- Auto-recovery settings for slots that have packet memory scanning enabled

Example
The following command displays the settings for each slot that has packet memory scanning enabled:
show packet-mem-scan-recovery-mode

The following is sample output from this command:

Global sys-health-check ‘online’ setting is ONLINE
slot 3: AUTORECOVERY MODE is OFFLINE
MSM-B: AUTORECOVERY MODE is ONLINE

# NOTE Global setting is always online for sys-health-check alarm-level configurations.
   It is only offline when "sys-health-check auto-recovery <#> offline" is configured.

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.
Platform Availability

This command is available on BlackDiamond switches only.
show packet miscompare

    show packet miscompare <slot number> {verbose}

Description
Captures corrupted packet data to help in troubleshooting problems.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot number</td>
<td>Specifies the slot where the I/O module is installed.</td>
</tr>
<tr>
<td>verbose</td>
<td>(Optional) Specifies detail that may interest a developer analyzing some system behavior at a more verbose level than provided by the debug summary information.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command only at the direction of Extreme Networks personnel. Extreme Networks support personnel can capture corrupted packet data to help in troubleshooting problems using the following command:

    show packet miscompare <slot number> {verbose}

Example
The following command captures corrupted packet data for the module in slot 5:

    show packet miscompare 5

History
This command was first available in ExtremeWare 7.2.0b25.

Platform Availability
This command is available on “i” series platforms.
show ports rxerrors

```
show ports {mgmt | <portlist>| vlan <vlan name>} rxerrors
```

**Description**

Displays real-time receive error statistics.

For PoS modules, displays the rxerror information for the PoS ports. Only a subset of the statistics displayed by this command are applicable to PoS ports. The fields that do not apply to PoS ports are displayed with values of all zeroes.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan</td>
<td>Denotes the VLAN name for which the statistics are presented. For example, if VLAN name &quot;v1&quot; has ports x, y and z, the command <code>show port vlan v1 rxerror</code> displays the rxerror statistics for ports x, y, and z.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

If you do not specify a port number or range of ports, receive error statistics are displayed for all ports.

This status information may be useful for your technical support representative if you have a network problem.

The following port receive error information is collected by the switch:

- **Port Number**
- **Link Status**—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- **Receive Bad CRC Frames (RX CRC)**—The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Over)**—The total number of good frames received by the port greater than the supported maximum length of 1,522 bytes.
- **Receive Undersize Frames (RX Under)**—The total number of frames received by the port that were less than 64 bytes long.
- **Receive Fragmented Frames (RX Frag)**—The total number of frames received by the port were of incorrect length and contained a bad FCS value.
Commands for Status Monitoring and Statistics

- Receive Jabber Frames (RX Jabber)—The total number of frames received by the port that was of greater than the support maximum length and had a Cyclic Redundancy Check (CRC) error.
- Receive Alignment Errors (RX Align)—The total number of frames received by the port that occurs if a frame has a CRC error and does not contain an integral number of octets.
- Receive Frames Lost (RX Lost)—The total number of frames received by the port that were lost because of buffer overflow in the switch.

For version 2.0 and 4.0
- Disabled and Not Present are not available as link status indicators.

**Examples**

The following command displays receive error statistics for ports 1 through 3 on a stand-alone switch:

`show ports 1-3 rxerrors`

The following command displays receive error statistics for slot 1, ports 1 through 3 on a modular switch:

`show ports 1:1-1:3 rxerrors`

The following command displays receive error statistics for slot 1, ports 1 through 3 on a modular switch:

`show ports 1:1-1:3 rxerrors`

The output of either command is similar to:

```
Port Rx Error Monitor                                 Sun Sep 12 14:53:17 2004
Port          Link      Rx      Rx      Rx        Rx     Rx        Rx        Rx
Status    CRC     Over    Under     Frag   Jabber    Align    Lost
================================================================================
1            A        0        0        0        0        0        0        0
2            A        0        0        0        0        0        0        0
3            R        0        0        0        0        0        0        0
===============================================================================

=====Link Status: A-Active R-Ready D-Disabled NP-Not Present LB-Loopback
0->Clear Counters U->page up D->page down ESC->exit
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 6.0 to support the Disabled and Not Present link status indicators.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to add support for management ports.
Platform Availability
This command is available on all platforms.
show ports stats

  show ports {mgmt | <portlist> | vlan <vlan name>} stats {cable-diagnostics}

Description
Displays real-time port statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2.5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Denotes the VLAN name for which the statistics are presented. For example, if VLAN name “v1” has ports x, y, and z, the command show port stats vlan v1 stats displays the rxerror statistics for ports x, y, and z.</td>
</tr>
<tr>
<td>cable-diagnostics</td>
<td>Specifies that cable diagnostics information should be shown for the specified port or ports</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, statistics are displayed for all ports.

Jumbo frame statistics are displayed only for “i” series switches that are configured for jumbo frame support.

This status information may be useful for your technical support representative if you have a network problem.

The following port statistic information is collected by the switch:

- Port Number
- Link Status—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- Transmitted Packet Count (Tx Pkt Count)—The number of packets that have been successfully transmitted by the port.
- Transmitted Byte Count (Tx Byte Count)—The total number of data bytes successfully transmitted by the port.
- Received Packet Count (Rx Pkt Count)—The total number of good packets that have been received by the port.
- Received Byte Count (RX Byte Count)—The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.

- Received Broadcast (RX Bcast)—The total number of frames received by the port that are addressed to a broadcast address.

- Received Multicast (RX Mcast)—The total number of frames received by the port that are addressed to a multicast address.

For version 2.0 and 4.0
- Disabled and Not Present are not available as link status indicators.
- Chassis is available as a link status indicator. If chassis is listed, the link is connected to a Summit Virtual Chassis.

**Examples**
The following command displays port statistics for ports 1 through 3 on a stand-alone switch:
```
show ports 1-3 stats
```

The following command displays port statistics for slot 1, ports 1 through 3 on a modular switch:
```
show ports 1:1-1:3 stats
```

The following command displays port statistics for all ports:
```
show ports stats
```

The output produced by the `show ports stats` command is similar to the following:

```
Port Statistics Thu Jul 8 09:50:50 2004
<table>
<thead>
<tr>
<th>Port</th>
<th>Link Status</th>
<th>Tx Pkt Count</th>
<th>Tx Byte Count</th>
<th>Rx Pkt Count</th>
<th>Rx Byte Count</th>
<th>Rx Bcast</th>
<th>Rx Mcast</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>A</td>
<td>740131</td>
<td>61671211</td>
<td>201310</td>
<td>17023242</td>
<td>7</td>
<td>3963</td>
</tr>
<tr>
<td>1:2</td>
<td>A</td>
<td>292131</td>
<td>24686533</td>
<td>896516</td>
<td>183343391</td>
<td>37</td>
<td>21456</td>
</tr>
<tr>
<td>1:3</td>
<td>A</td>
<td>37273</td>
<td>4351318</td>
<td>37578</td>
<td>4721313</td>
<td>36</td>
<td>21551</td>
</tr>
<tr>
<td>1:4</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:5</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:6</td>
<td>A</td>
<td>1099</td>
<td>375858</td>
<td>11962</td>
<td>901306</td>
<td>4421</td>
<td>7541</td>
</tr>
<tr>
<td>1:7</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:8</td>
<td>A</td>
<td>1099</td>
<td>375858</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following command displays cable diagnostics information for all ports:
```
show ports stats cable-diagnostics
```

The output produced by the `show ports stats cable-diagnostics` command is similar to the following:

```
Port Statistics Thu Jul 8 09:52:19 2004
<table>
<thead>
<tr>
<th>Port</th>
<th>Link Status</th>
<th>Num Diags</th>
<th>Diags Success</th>
<th>Diags Fail</th>
<th>Diags Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:2</td>
<td>A</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:3</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:4</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```
### History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in Extreme 4.1 to discontinue support for the chassis link status indicator.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.3.0 to include the `cable-diagnostics` keyword.

### Platform Availability

This command is available on all platforms.
show ports txerrors

    show ports {mgmt | <portlist>| vlan <vlan name>} txerrors

Description
Displays real-time transmit error statistics.
For PoS modules, displays the txerror information for the PoS ports.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. NOTE: This option is available only on switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan</td>
<td>Denotes the VLAN name for which the statistics are presented. For example, if VLAN name “v1” has ports x, y, and z, the command show port vlan v1 txerrors displays the txerror statistics for ports x, y, and z.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, error statistics are displayed for all ports.
This status information may be useful for your technical support representative if you have a network problem.
For PoS modules, displays the txerror information for the PoS ports. Only a subset of the statistics displayed by this command is applicable to PoS ports. The fields that do not apply to PoS ports are displayed with values of all zeroes.
The following port transmit error information is collected by the switch:

- Port Number
- Link Status—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- Transmit Collisions (TX Coll)—The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- Transmit Late Collisions (TX Late Coll)—The total number of collisions that have occurred after the port’s transmit window has expired.
- Transmit Deferred Frames (TX Deferred)—The total number of frames that were transmitted by the port after the first transmission attempt was deferred by other network traffic.
Commands for Status Monitoring and Statistics

- Transmit Errored Frames (TX Error)—The total number of frames that were not completely transmitted by the port because of network errors (such as late collisions or excessive collisions).
- Transmit Lost Frames (TX Lost)—The total number of frames transmitted by the port that were lost.
- Transmit Parity Frames (TX Parity)—The bit summation has a parity mismatch.

For version 2.0 and 4.0
- Disabled and Not Present are not available as link status indicators.

Examples

The following command displays transmit error statistics for ports 1 through 3 on a stand-alone switch:

`show ports 1-3 txerrors`

The following command displays transmit error statistics for slot 1, ports 1 through 3 on a modular switch:

`show ports 1:1-1:3 txerrors`

The output produced by the `show ports txerrors` command is similar to the following:

<table>
<thead>
<tr>
<th>Port</th>
<th>Link</th>
<th>Tx Coll</th>
<th>Late Coll</th>
<th>Deferred</th>
<th>Error</th>
<th>Lost</th>
<th>Parity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>A</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>6</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>8</td>
<td>R</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Link Status: A-Active R-Ready D-Disabled NP-Not Present
0->Clear Counters U->page up D->page down ESC->exit

History

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support PoS modules.

This command was modified in ExtremeWare 6.0 to support the Disabled and Not Present link status indicators.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support management ports.
**Platform Availability**

This command is available on all platforms.
show sflow configuration

    show sflow configuration

Description
Displays the current sFlow configuration.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command displays all sFlow configuration information for the switch.

The following fields are displayed:

- Global Status—sFlow is globally enabled or disabled.
- Polling interval—How often data from each sampler is sent to the collector, in seconds.
- Sampling rate—Packets are sampled, on average, once for every rate-number of packets.
- BackOff Threshold—Enabled or disabled. Used to limit the number of packets sent to the collector in a second.
- BackOff Threshold (No. of Samples)—Configured threshold used to limit the number of packets sent to the collector in a second.
- Configured Agent IP—IP address of the operational sFlow agent.
- Collectors—Collected packet samples will be sent to this list of collector addresses.
- SFLOW Port Configuration: Port—List of all ports with sFlow enabled.
- SFLOW Port Configuration: Status—Enabled or disabled for statistics gathering.

Example
To display the sFlow configuration on your system, use the following command:

    show sflow

The output from this command is similar to the following:

SFLOW Global Configuration
Global Status: enabled
Polling interval: 30
Sampling rate: 512
Maximum cpu sample limit: 2000
show sflow configuration

SFLOW Configured Agent IP: 10.203.2.38 Operational Agent IP: 10.203.2.38
BackOff Threshold: disabled
BackOff Threshold (No. of Samples): 50
SFLOW Configured Agent IP: 10.201.6.100

Collectors
Collector IP 10.201.6.250, Port 6343
Collector IP 123.124.125.111 port 6344

SFLOW Port Configuration
Port      Status
3:9        enabled
3:10       enabled
3:11       enabled
3:12       enabled
5:33       enabled
5:34       enabled
5:35       enabled
5:36       enabled

**History**
This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**
This command is available on “i” series platforms.
show sflow statistics

show sflow statistics

Description
Displays sFlow statistics.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables

Default
N/A

Usage Guidelines
This command displays sFlow statistics collected on all enabled ports. (No per port status is displayed.)

The following fields are displayed:

- Received frames—Number of frames received on sFlow enabled ports
- Sampled Frames—Number of frames scheduled for sending to collector(s)
- Transmitted Frames—Number of UDP packets sent to remote collector(s)
- Broadcast Frames—Number of broadcast frames received on sFlow enabled ports
- Multicast Frames—Number of multicast frames received on sFlow enabled ports
- Packet Drops—Number of samples dropped
- Zero Sampling rate—
- No Receivers—

Example
To display sFlow statistics for your system, use the following command:

```
show sflow statistics
```

The output from this command is similar to the following:

```
SFLOW Statistics
Received frames : 1159044921
Sampled Frames : 104944
Transmitted Frames : 10518
Broadcast Frames : 0
Multicast Frames : 1055652
```
show sflow statistics

Packet Drops : 0
Zero Sampling rate : 0
No Receivers : 0

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms.
show version

    show version {detail}

Description
Displays the hardware serial numbers and versions, and software versions currently running on the
switch, and (if applicable) the modules.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies display of slot board name and chassis or platform name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
On modular switches, displays the switch serial number and version numbers of MSM modules
(BlackDiamond switch) and I/O modules (BlackDiamond and Alpine switches).

For ARM, ATM, MPLS or PoS modules, displays information that includes data about the particular
module and the BootROM version of the module. For these modules, the command also shows the
software version running on the module.

The following is an example of the type of information displayed when you execute the show version
command:
• System Serial Number—A collection of numbers and letters that make up the serial number of the
  switch.
• CPU Serial Number—A collection of numbers and letters that make up the serial number of the CPU
  running in the switch. A rev number may also be listed.
• Image—The ExtremeWare software version currently running on the switch. If you have two
  software images downloaded on the switch, only the currently running ExtremeWare version
  information is displayed. The information displayed includes the version number, build number, and
  the software build date.
• BootROM—The BootROM version currently running on the switch.

If you use the detail option (supported in ExtremeWare version 6.2.1 or later) you may also see the
following:
• Board/Chassis/Platform Name—The name of the system or module, inserted before the Serial
  Number in the display.

Depending on the model of your switch, the software running on your switch, and whether you have a
stackable or modular switch, different version information may be displayed.

Examples
The following command displays the hardware and software versions currently running on the switch:

    show version
On a stackable switch, this command produces output similar to the following:

System Serial Number: 800078-11-0035M02442
CPU Serial Number: 700027-11 0034M-01445 CPLD Rev 04
Daughtercard Serial Number: 703015-02 0029M-02701 CPLD Rev y
Image : Extremeware Version 6.2.0 (Build 60) by Release_Master 09/21/0120:53:17

On a BlackDiamond switch, this command produces output similar to the following:

Chassis: 801000-07-9946F00987
MSM A :
MSM B : 701021-08-0023F25758
SLOT 1 : 701026-03-0003Y00043
SLOT 2 : 701024-04-9949Y00055
SLOT 3 : 701005-09-9946F25172
SLOT 4 :
SLOT 5 :
SLOT 6 : 701028-01-0004Y00038
SLOT 7 :
SLOT 8 :
Image : Extremeware Version 6.2.0 (Build 60) by Release_Master 09/21/0120:53:17
BootROM : 7.2

Using the detail option in the show version command produces output similar to the following on a BlackDiamond switch:

Chassis : MSM64 801000-07-9946F00987
MSM A : MSM64i
MSM B : MSM64i 701021-08-0023F25758
SLOT 1 : F48Ti 701026-03-0003Y00043
SLOT 2 : G8Xi 701024-04-9949Y00055
SLOT 3 : F32T 701005-09-9946F25172
SLOT 4 : Empty
SLOT 5 : Empty
SLOT 6 : G8Ti 701028-01-0004Y00038
SLOT 7 : Empty
SLOT 8 : Empty
Image : Extremeware Version 6.2.1 (Build 18) by Release_Master 02/14/02 15:04:26
BootROM : 7.2

History

This command was first available in ExtremeWare 2.0.
This command was modified in ExtremeWare 6.2.1 to support the detail option.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2e to support the detail option.
Platform Availability

This command is available on all platforms.
unconfigure flowstats filter ports

unconfigure flowstats filter <filter#> ports <portlist>

**Description**
Removes the filter specification for the specified ports.

**NOTE**
This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter#</td>
<td>Specifies the filter specification that should be removed.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a set of ports or slots and ports from which the filter specification is removed. May be in the form 1, 2, 3-5, 2:* , 2:5 , 2:6-2:8</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
By unconfiguring the filter specification, this effectively disables this filter on all ports for which it was configured.

**Example**
The following command resets the values for filter 4 on slot 1, port s 2 and 3:
unconfigure flowstats filter 4 ports 1:2-1:3

**History**
This command was first available in ExtremeWare 6.2.

**Platform Availability**
This command is available on “i” series platforms.
unconfigure flowstats ports

    unconfigure flowstats ports [<portlist> | all]

Description
Resets the flow statistics configuration parameters for the specified ports to their default values.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a set of ports or slots and ports that should be reset. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all ports or slots and ports should be reset.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command does not affect the enabled or disabled status of flow collection on these ports, nor does it affect the configured export destinations.

Example
The following command resets the flow statistics configuration parameters for port 1 of slot 8 to their default values:

    unconfigure flowstats ports 8:1

History
This command was first available in ExtremeWare 6.1.5b20 for the PoS module
This command was modified in ExtremeWare 6.2 to support all “i” series platforms.

Platform Availability
This command is available on “i” series platforms.
unconfigure log filter

unconfigure log filter <filter name>

Description
Resets the log filter to its default values; removes all filter items.

Syntax Description

| filter name | Specifies the log filter to unconfigure. |

Default
N/A

Usage Guidelines
If the filter name specified is DefaultFilter, this command restores the configuration of DefaultFilter back to its original settings.
If the filter name specified is not DefaultFilter, this command sets the filter to have no events configured and therefore, no incidents will pass. This is the configuration of a newly created filter that was not copied from an existing one.

See the delete log filter command for information about deleting a filter.

Example
The following command sets the log filter myFilter to stop passing any events:

unconfigure log filter myFilter

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available all platforms.
unconfigure log target format

unconfigure log target [console-display | memory-buffer | nvram | session | syslog [<host name/ip> {:<udp-port>} [local0 ... local7]]] format

Description
Resets the log target format to its default values.

Syntax Description

<table>
<thead>
<tr>
<th>parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>console-display</td>
<td>Specifies the console display format.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Specifies the switch memory buffer format.</td>
</tr>
<tr>
<td>nvram</td>
<td>Specifies the switch NVRAM format.</td>
</tr>
<tr>
<td>session</td>
<td>Specifies the current session (including console display) format.</td>
</tr>
<tr>
<td>syslog</td>
<td>Specifies a syslog target format.</td>
</tr>
<tr>
<td>host name/ip</td>
<td>Specifies the syslog host name or IP address.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies the UDP port number for the syslog target.</td>
</tr>
<tr>
<td>local0 ... local7</td>
<td>Specifies the local syslog facility.</td>
</tr>
<tr>
<td>format</td>
<td>Specifies that the format for the target will be reset to the default value.</td>
</tr>
</tbody>
</table>

Default
When a target format is unconfigured, it is reset to the default values.

The following defaults apply to console display, memory buffer, NVRAM, and session targets:

- timestamp—hundredths
- date—mm-dd-yyyy
- severity—on
- event-name—condition
- host-name—off
- priority—off
- tag-id—off
- tag-name—off
- sequence-number—off
- process-name—off
- process-id—off
- source-function—off
- source-line—off

The following defaults apply to syslog targets (per RFC 3164):

- timestamp—seconds
- date—mmm-dd
Usage Guidelines

Use this command to reset the target format to the default format.

Example

The following command sets the log format for the target session (the current session) to the default:

```
unconfigure log target session format
```

History

This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available all platforms.
unconfigure packet-mem-scan-recovery-mode

unconfigure packet-mem-scan-recovery-mode slot [msm-a | msm-b | <slot number>]

Description
Disables packet memory scanning and the recovery mode on a BlackDiamond module, and returns the system to the configured system health check behavior.

NOTE
This command is available only on the BlackDiamond switches.

Syntax Description

+----------------+-------------------------------------------------------------------+
| Parameter      | Description                                                      |
+----------------+-------------------------------------------------------------------+
| msm-a          | Specifies the MSM module installed in slot A.                    |
| msm-b          | Specifies the MSM module installed in slot B.                    |
| slot number    | Specifies a module installed in a slot.                          |
+----------------+-------------------------------------------------------------------+

Default
N/A

Usage Guidelines
If you disable packet memory scanning on a BlackDiamond module, the system health check system resumes. However, if you have the system health check alarm level configured, individual packet memory scanning is ignored.

Example
The following command disables packet memory scanning on a module installed in slot 1:

unconfigure packet-mem-scan-recovery mode slot 1

The following command disables packet memory scanning on the MSM module installed in slot B:

unconfigure packet-mem-scan-recovery mode slot msm-b

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available on BlackDiamond switches only.
unconfigure sflow agent

Description
Resets the sFlow agent IP address to the default value.

**NOTE**
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
The default IP address is 0.0.0.0.

Usage Guidelines
This command resets the sFlow agent IP address to its default value.

Example
The following command resets the source IP address to 0.0.0.0 for UDP datagrams sent out by the sFlow agent:

```
unconfigure sflow agent
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms.
unconfigure sflow backoff-threshold

unconfigure sflow backoff-threshold

Description
Removes the configured value of the sFlow backoff threshold and resets it to 0 (zero).

NOTE
This command is available only on the “i” series switches.

Syntax Description
The command has no arguments or variables.

Default
The default backoff threshold rate is 0 packets per second.

Usage Guidelines
This command removes the configured sFlow backoff threshold value and resets it to 0 (zero). The backoff threshold feature is used to limit the number of packets sent to the sFlow collector in a second. The backoff threshold is set by using the following command:

configure sflow backoff-threshold

If the number of packets sent to the collector exceeds the limit set by the configure sflow backoff-threshold command, the sampling rate will be doubled.

The backoff threshold is enabled when the enable sflow backoff-threshold command is executed and the sample rate set by the configure sflow sample-rate command is greater than 0 (zero).

Example
The following command resets the sFlow backoff threshold value to 0 (zero):

unconfigure sflow backoff-threshold

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms.
unconfigure sflow collector

unconfigure sflow collector [<ip-address> | all]

**Description**
Removes the IP addresses of a selected sFlow collector so that sampled flows are no longer sent to that collector.

**NOTE**
This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ip-address</strong></td>
<td>Specifies the IP address of configured collector to reset.</td>
</tr>
<tr>
<td><strong>all</strong></td>
<td>Specifies the IP addresses of all configured collectors to reset.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command removes the IP address of one or all configured sFlow collectors. No counters or flow samples will be sent to these collectors.

**Example**
The following command removes IP addresses of all configured sFlow collectors:

```
configure sflow collector all
```

**History**
This command was first available in ExtremeWare 7.3.0.

**Platform Availability**
This command is available on “i” series platforms.
unconfigure transceiver-test failure-action

unconfigure transceiver-test failure-action

**Description**

Returns the switch to its default of sending transceiver test messages to the syslog if too many failures are detected within the specified window.

NOTE

*This command is available only on modular switches.*

**Syntax Description**

The command has no arguments or variables.

**Default**

N/A

**Usage Guidelines**

By default, the switch checks for errors within the *last* eight 20-second windows and sends messages to the syslog.

To configure the number of windows the switch waits to check for errors, use the `configure transceiver-test window` command. To modify how the switch responds if too many failures are detected, use the `configure transceiver-test failure-action` command.

**Example**

The following command returns the switch to its default of sending error messages to the syslog:

```
unconfigure transceiver-test failure-action
```

**History**

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available only on modular switches.
unconfigure transceiver-test period

Description
Returns the transceiver test period to the factory default of 12 seconds.

NOTE
This command is available only on modular switches.

Syntax Description
The command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this feature when the switch can be brought off-line.

Configuring the transceiver test period to 11 seconds or less can affect system performance; therefore, Extreme Networks does not recommend changing the default transceiver test period. The default is adequate for most networks.

Example
The following command returns the transceiver test period to 12 seconds:
unconfigure transceiver-test period

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available only on modular switches.
unconfigure transceiver-test threshold

unconfigure transceiver-test threshold

Description
Returns the transceiver test threshold to the factory default of 3 errors.

NOTE
This command is available only on modular switches.

Syntax Description
The command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this feature when the switch can be brought off line.

Extreme Networks does not recommend changing the default transceiver test period. The default is adequate for most networks.

Example
The following command returns the transceiver test threshold to 3 errors:
unconfigure transceiver-test threshold

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available only on modular switches.
unconfigure transceiver-test window

Description
Returns the transceiver test window to the factory default of eight 20-second windows.

NOTE
This command is available only on modular switches.

Syntax Description
The command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this feature when the switch can be brought off line.

This configuration provides a sliding window. When you return to the default window, the switch checks for errors within the last eight 20-second windows.

Extreme Networks does not recommend changing the default transceiver test window. The default is adequate for most networks.

Example
The following command returns the transceiver test window to eight 20-second windows:

```
configure transceiver-test window
```

History
This command was first available in ExtremeWare 6.2.2b108.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.

Platform Availability
This command is available only on modular switches.
upload log

upload log <host name/ip> <filename> {messages [memory-buffer | nvram]} {severity <severity> {only}} {starting [date <date> time <time> | date <date> | time <time>]} {ending [date <date> time <time> | date <date> | time <time>]} {match <match-expression>} {format <format>} {chronological}

Description
Uploads the current log messages to a TFTP server.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host name/ip</td>
<td>Specifies the TFTP server.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the file name for the log stored on the TFTP server.</td>
</tr>
<tr>
<td>messages</td>
<td>Specifies the location from which to display the log messages.</td>
</tr>
<tr>
<td>memory-buffer</td>
<td>Show messages stored in volatile memory.</td>
</tr>
<tr>
<td>nvram</td>
<td>Show messages stored in NVRAM.</td>
</tr>
<tr>
<td>severity</td>
<td>Specifies the minimum severity level to display (if the keyword only is omitted).</td>
</tr>
<tr>
<td>only</td>
<td>Specifies that only the specified severity level is to be displayed</td>
</tr>
<tr>
<td>starting</td>
<td>Show messages with timestamps equal to or greater than that specified</td>
</tr>
<tr>
<td>date</td>
<td>Specifies the date, where date is &lt;month (1-12)&gt; / &lt;day&gt; / &lt;year (yyyy)&gt;</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time, where time is &lt;hour (0-23)&gt; : &lt;minute (0-59)&gt; : &lt;seconds&gt; .</td>
</tr>
<tr>
<td>ending</td>
<td>Show messages with timestamps equal to or less than that specified.</td>
</tr>
<tr>
<td>match-expression</td>
<td>Specifies a regular expression. Only messages that match the regular expression will be displayed.</td>
</tr>
<tr>
<td>format</td>
<td>Specifies a format to use to override the format configured for the memory buffer.</td>
</tr>
<tr>
<td>chronological</td>
<td>Specifies uploading log messages in ascending chronological order (oldest to newest).</td>
</tr>
</tbody>
</table>

Default
The following defaults apply:

- messages—memory buffer
- severity—none (displays everything stored in the target)
- starting, ending—if not specified, no timestamp restriction
- match—no restriction
- format—the format configured with the `configure log target format` command
- chronological—if not specified, show messages in order from newest to oldest

Usage Guidelines
This command is similar to the `show log` command, but instead of displaying the log contents on the command line, this command saves the log to a file on the TFTP server you specify. For more details on
most of the options of this command, see the command `show log` on page 775, and for the `format` option see the command `configure log target format` on page 688.

**Example**

The following command uploads messages with a critical severity to the filename `switch4critical.log` on TFTP server at 10.31.8.25:

```plaintext
upload log 10.31.8.25 switch4critical.log critical
```

The following command uploads messages with warning, error, or critical severity to the filename `switch4warn.log` on TFTP server at 10.31.8.25:

```plaintext
upload log 10.31.8.25 switch4warn.log warning
```

The following command uploads messages starting August 1, ending August 31, containing the string “slot 2” in order of oldest to newest to the filename `switch4aug03.log` on TFTP server at 10.31.8.25:

```plaintext
upload log 10.31.8.25 switch4aug03.log starting date 8/1 ending date 8/31 match "slot 2"
```

**History**

This command was first available in ExtremeWare 7.1.0

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
This chapter describes commands for:

- Creating and configuring routing access policies
- Creating and configuring IP access lists
- Creating and configuring route maps (“i” series switches only)
- Managing MAC address access to the switch
- Managing the switch using SSH2
- Setting up switch user authentication through a RADIUS client
- Setting up switch user authentication through TACACS+
- Protecting the switch from denial of service (DoS) attacks
- Configuring network login
- Configuring Trusted MAC or OUI configuration
- Configuring secure access for all wired and wireless stations through Unified Access™ Security

Controlling Access

Access policies are a generalized category of features that affect forwarding and route forwarding decisions. Access policies are used primarily for security and quality of service (QoS) purposes.

IP access lists (also referred to as access lists or ACLs) consist of IP access rules. They are used to perform packet filtering and forwarding decisions on incoming traffic. Each packet arriving on an ingress port is compared to the access list in sequential order and is either forwarded to a specified QoS profile or dropped. Using access lists has no impact on switch performance.

Access lists are typically applied to traffic that crosses layer 3 router boundaries, but it is possible to use access lists within a layer 2 VLAN. Extreme products are capable of performing this function with no additional configuration.

Routing access policies are used to control the advertisement or recognition of routing protocols, such as RIP, OSPF, IS-IS, or BGP. (IS-IS and BGP are supported only on “i” series switches.) Routing access policies can be used to “hide” entire networks or to trust only specific sources for routes or ranges of routes. The capabilities of routing access policies are specific to the type of routing protocol involved, but are sometimes more efficient and easier to implement than access lists.
**Route maps** are used to modify or filter routes redistributed between two routing domains. They are also used to modify or filter the routing information exchanged between the domains.

---

**NOTE**

*Route maps are supported only on the “i” series switches.*

### MAC Address Security

The switch maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered. You can control the way the forwarding database (FDB) is learned and populated. By managing entries in the FDB, you can block, assign priority (queues), and control packet flows on a per-address basis.

You can limit the number of dynamically learned MAC addresses allowed per virtual port or “lock” the FDB entries for a virtual port, so that the current entries will not change, and no additional addresses can be learned on the port. Commands for these functions are described in Chapter 4. In addition, you can set a timer on the learned addresses that limits the length of time the learned addresses will be maintained if devices are disconnected or become inactive. Commands for this function are described in this chapter.

### SSH

Secure Shell 2 (SSH2) is a feature of ExtremeWare that allows you to encrypt session data between a network administrator using SSH2 client software and the switch, or to send encrypted data from the switch to an SSH2 client on a remote system. Image and configuration files may also be transferred to the switch using the Secure Copy Program 2 (SCP2).

### User Authentication

Remote Authentication Dial In User Service (RADIUS, RFC 2138) is a mechanism for authenticating and centrally administrating access to network nodes. The ExtremeWare RADIUS client implementation allows authentication for telnet, Vista, or console access to the switch.

Extreme switches can send RADIUS accounting information. You can configure RADIUS accounting servers to be the same as the authentication servers, but this is not required.

Terminal Access Controller Access Control System Plus (TACACS+) is a mechanism for providing authentication, authorization, and accounting on a centralized server, similar in function to the RADIUS client. The ExtremeWare version of TACACS+ is used to authenticate prospective users who are attempting to administer the switch. TACACS+ is used to communicate between the switch and an authentication database.
Network Login

Network login is a feature designed to control the admission of user packets into a network by giving network access only to users that have been properly authenticated. Network login is controlled by an administrator on a per port, per VLAN basis and uses an integration of DHCP, user authentication over the web interface or 802.1x client software, and a RADIUS server to provide a user database or specific configuration details.

Network login has two modes of operation:

- Campus mode, used when a port in a VLAN will move to another VLAN after authentication has been completed successfully. This mode is for the roaming user who will not always be using the same port for authentication. Campus mode requires a DHCP server and a RADIUS server configured for Extreme network login.

- ISP mode, used when the port and VLAN used will remain constant. All network settings are configured for that VLAN.

A DHCP server is included to support network login functionality.

Denial of Service

You can configure ExtremeWare to protect Extreme switches in the event of a denial of service (DoS) attack. During a typical denial of service attack, the CPU on the switch is flooded with packets from multiple attackers, potentially causing the switch to fail. To protect against this type of attack, you can configure the software so that when the number of packets received is more than the configured threshold limit of packets per second, a hardware ACL is enabled. (In the “e” series switches, a specific type of traffic on the port is blocked.)

Unified Access Security

The Extreme Unified Access™ Security architecture provides secure access for all wired and wireless stations within the unified network. You can maintain the network with a single, unified security policy, provide service to all stations without requiring upgrades, and take advantage of integrated policy and management capabilities not available in overlay networks or those with “thick” access points. Unified Access Security provides the following capabilities:

- Consolidated management—greater network support with reduced management overhead
- Scalable encryption—ASIC based AES encryption, WPA with TKIP support, and RC4 based WEP support on the Altitude 300 wireless port
- 802.1x Authentication—802.1x authentication (PEAP, EAP-TTLS, EAP-TLS)
- Web-based network login—http and https based user authentication

The unified structure simplifies security policies without compromising protection and provides the following benefits:

- Single user experience—Same authentication procedures for wired and wireless users
- Unified management—Single management platform for wired and wireless networks
- Unified configuration—Consistent CLI for wired and wireless functions
- Single authentication infrastructure—Single set of policies, RADIUS, and certificate servers
clear netlogin state

clear netlogin state port <portlist> vlan <vlan name>

Description
Clears and initializes the network login sessions on a VLAN port.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports to clear.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN to clear.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
Clear the states of every MAC learned on this VLAN port and put the port back to unauthenticated state. The port will be moved to its original VLAN if configured in campus mode.

Example
The following example clears the network login state of port 9 in VLAN corp:

```
clear netlogin state port 9 vlan corp
```

History
This command was first available in ExtremeWare 7.0.0.

The MAC states were not cleared by this command until ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
clear netlogin state mac-address

clear netlogin state mac-address <hex-octet>

Description
Initialize or reset the network login sessions for a specified supplicant.

Syntax Description

| hex-octet | Specifies the MAC address of the supplicant. |

Default
N/A

Usage Guidelines
This command is essentially equivalent to a particular supplicant’s logging out. The MAC address is cleared from the FDB, the port is put back to its original VLAN (for campus mode), and the port state is set to unauthenticated, if this was the last authenticated MAC on this port.

Example
The following example resets the network login session for the supplicant with the MAC address of 00:e0:18:01:32:1f:

clear netlogin state mac-address 00:e0:18:01:32:1f

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure access-profile add

For the “i” series switches:

    configure access-profile <access profile> add {<seq_number>} {permit | deny} [ipaddress <ip address> <mask> {exact} | as-path <path-expression> | bgp-community [internet | no-export | no-advertise | no-export-subconfed | <as_no:number> | number <community>] | ipxnet <netid> <netid mask> | ipxsap <sap_type> <service_name> | vlan]

For the “e” series switches:

    configure access-profile <access profile> add {<seq_number>} {permit | deny} [ipaddress <ip address> <mask> {exact} | as-path <path-expression> | vlan]

Description

Adds an entry to the access profile.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>seq-number</td>
<td>Specifies the order of the entry within the access profile. If no sequence number is specified, the new entry is added to the end of the access-profile and is automatically assigned a value of 5 more than the sequence number of the last entry.</td>
</tr>
<tr>
<td>permit</td>
<td>Per-entry permit specification. The per-entry attribute takes effect only if the access-profile mode is none. Otherwise, the overall access profile type takes precedence.</td>
</tr>
<tr>
<td>deny</td>
<td>Per-entry deny specification. The per-entry attribute takes effect only if the access-profile mode is none. Otherwise, the overall access profile type takes precedence.</td>
</tr>
<tr>
<td>ip address/mask</td>
<td>Specifies an IP address and mask as an entry in the profile list.</td>
</tr>
<tr>
<td>exact</td>
<td>Specifies that an exact match with address and mask will be performed. Subnets within the address range will not match entry against entry.</td>
</tr>
<tr>
<td>path-expression</td>
<td>Specifies a regular expression string to match against the autonomous system path.</td>
</tr>
<tr>
<td>internet</td>
<td>Specifies a match against all routes, because all routes belong to the internet community.</td>
</tr>
<tr>
<td>no-export</td>
<td>Match against communities with the no-export attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Match against communities with the no-advertise attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Match against communities with the no-export-subconfed attribute.</td>
</tr>
<tr>
<td>as_no:number</td>
<td>Match against a BGP community number, specified in as_no:number format.</td>
</tr>
<tr>
<td>community</td>
<td>Match against a BGP community number specified as an unsigned 32-bit integer in decimal format.</td>
</tr>
</tbody>
</table>

NOTE: This option is available only on “i” series switches.
configure access-profile add

Default

N/A

Usage Guidelines

You can specify the sequence number for each access profile entry. If you do not specify a sequence number, entries are sequenced in the order they are added. Each entry is assigned a value of 5 more than the sequence number of the last entry.

The explicit sequence number and the permit or deny attribute should be specified if the access profile mode is none.

The subnet mask specified in the access profile command is interpreted as a reverse mask. A reverse mask indicates the bits that are significant in the IP address. In other words, a reverse mask specifies the part of the address that must match the IP address to which the profile is applied.

The as-path keyword uses a regular expression string to match against the AS path. Regular expression notation can include any of the characters listed in Table 16.

### Table 16: Regular Expression Notation

<table>
<thead>
<tr>
<th>Character</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>AS number</td>
</tr>
<tr>
<td>$N_1 - N_2$</td>
<td>Range of AS numbers, where $N_1$ and $N_2$ are AS numbers and $N_1 &lt; N_2$</td>
</tr>
<tr>
<td>[N_k ... N_y]</td>
<td>Group of AS numbers, where $N_k$ and $N_y$ are AS numbers or a range of AS numbers</td>
</tr>
<tr>
<td>[^N_k ... N_y]</td>
<td>Any AS numbers other than the ones in the group</td>
</tr>
<tr>
<td>.</td>
<td>Matches any number</td>
</tr>
<tr>
<td>^</td>
<td>Matches the beginning of the AS path</td>
</tr>
<tr>
<td>$</td>
<td>Matches the end of the AS path</td>
</tr>
<tr>
<td>-</td>
<td>Matches the beginning or end, or a space</td>
</tr>
<tr>
<td>-</td>
<td>Separates the beginning and end of a range of numbers</td>
</tr>
<tr>
<td>*</td>
<td>Matches 0 or more instances</td>
</tr>
<tr>
<td>+</td>
<td>Matches 1 or more instances</td>
</tr>
<tr>
<td>?</td>
<td>Matches 0 or 1 instance</td>
</tr>
<tr>
<td>{</td>
<td>Start of AS SET segment in the AS path</td>
</tr>
<tr>
<td>}</td>
<td>End of AS SET segment in the AS path</td>
</tr>
<tr>
<td>(</td>
<td>Start of a confederation segment in the AS path</td>
</tr>
<tr>
<td>)</td>
<td>End of a confederation segment in the AS path</td>
</tr>
</tbody>
</table>
Examples
The following command adds an IP subnet address to access profile nosales, as the next available entry:
```bash
configure access-profile nosales add ipaddress 10.1.33.0/24
```
The following command configures the access profile AS1 to permit AS paths beginning with AS number 1, followed by any AS number from 2 - 8, and ending with either AS number 11, 13, or 15:
```bash
configure access-profile AS1 add 15 permit as-path "^1 2-8 [11 13 15]$"
```

History
A limited version of this command was first available in ExtremeWare 4.0.
This form of the command was available in ExtremeWare 6.1. Support for IPX NetID and IPX SAP matching was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2e to support for the as-path, ipxnet and ipxsap options.

Platform Availability
This command is available on all platforms.
configure access-profile delete

configure access-profile <access profile> delete <seq_number>

Description
Deletes an access profile entry using the sequence number.

Syntax Description

<table>
<thead>
<tr>
<th>access profile</th>
<th>Specifies an access profile name.</th>
</tr>
</thead>
</table>
|   seq-number       | Specifies the order of the entry within the access profile. If no sequence number is specified, the new entry is added to the end of the access-profile and is automatically assigned a value of 5 more than the sequence number of the last entry.

Default
N/A

Usage Guidelines
None

Example
The following command deletes the entry with sequence number 15 from the access profile AS1:
configure access-profile AS1 delete 15

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure access-profile mode

configure access-profile <access profile> mode [permit | deny | none]

Description
Configures the access profile mode to permit or deny access, or to require per-entry access control.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>permit</td>
<td>Allows the addresses that match the access profile description.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies the addresses that match the access profile description.</td>
</tr>
<tr>
<td>none</td>
<td>Permits and denies access on a per-entry basis. Each entry must be added to the profile as either type permit or deny.</td>
</tr>
</tbody>
</table>

Default
Permit

Usage Guidelines
The access list mode determines whether the items in the list are to be permitted access or denied access.

Example
The following command configures the access profile no_subnet_33 to deny access:
configure access-profile no_subnet_33 mode deny

The following command specifies that the access profile no_subnet_33 uses per-entry access control:
configure access-profile no_subnet_33 mode none

History
This command was first available in ExtremeWare 4.0.

The per-entry access control was added in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure auth mgmt-access local

configure auth mgmt-access local

Description
Configures local authentication for management sessions. If local authentication is configured for management sessions, users are authenticated through local user database.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
RADIUS or TACACS servers are used only if they are enabled. When RADIUS or TACACS is not enabled, authentication is performed locally even if the configure auth mgmt-access local command is not used.

Use this command to authenticate all the management sessions using the local users database. Network login sessions can be configured for RADIUS authentication independently of the management session authentication method. TACACS authentication cannot be used with network login.

The following types of management sessions can be configured:
- Telnet
- SSH
- Console
- HTTP

If local authentication is configured for management sessions, users are authenticated through the local user database even if RADIUS or TACACS is enabled and servers are configured.

Example
The following command sequence configures RADIUS authentication for network login sessions and local authentication for management sessions:

```bash
enable radius
enable tacacs
configure radius primary server 10.1.2.254 1812 client-ip 10.1.2.1
configure radius secondary server 10.1.1.154 1812 client-ip 10.1.2.1
configure auth mgmt-access local
configure auth netlogin radius primary 10.1.2.254 secondary 10.1.1.254
```

History
This command was first available in ExtremeWare 7.4.
Platform Availability

This command is available on all platforms.
configure auth mgmt-access radius

configure auth mgmt-access radius primary [<ipaddress> | <hostname>]
{secondary [<ipaddress> | hostname]}

Description
Configures authentication of management sessions for RADIUS servers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary RADIUS authentication server that is used for management sessions.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary RADIUS authentication server that is used for management sessions.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address of the authentication server.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the authentication server.</td>
</tr>
</tbody>
</table>

Default
Uses RADIUS for authentication for management sessions. If RADIUS is not enabled, TACACS+ servers are used. If neither RADIUS nor TACACS+ servers are configured, local authentication is used.

Usage Guidelines
Use this command to authenticate all the management sessions through RADIUS servers. The RADIUS server should be configured before using this command. This command fails if the primary and secondary RADIUS servers are not configured.

The following types of management sessions can be configured:

- Telnet
- SSH
- Console
- HTTP

If you are using RADIUS authentication servers, you should only use RADIUS accounting servers for accounting management sessions. RADIUS authentication servers should be configured before configuring RADIUS accounting servers for management sessions.

Example
In the following example, management sessions are configured for RADIUS:

```
```

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure auth mgmt-access radius-accounting

configure auth mgmt-access radius-accounting primary [<ipaddress> | <hostname>] {secondary [<ipaddress> | <hostname>]}
configure auth mgmt-access tacacs

configure auth mgmt-access tacacs primary [<ipaddress> | <hostname>] {secondary [<ipaddress> | <hostname>]}
Platform Availability

This command is available on all platforms.
configure auth mgmt-access tacacs-accounting

configure auth mgmt-access tacacs-accounting primary [<ipaddress> | <hostname>] {secondary [<ipaddress> | <hostname>]} }]

Description
Configures TACACS accounting servers for accounting management sessions.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary TACACS+ accounting server that is used for management sessions.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary TACACS+ accounting server that is used for management sessions.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address of the primary and secondary accounting servers.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the primary and secondary accounting servers.</td>
</tr>
</tbody>
</table>

Default
Unconfigured. Uses RADIUS for authentication for management sessions. If RADIUS is not enabled, TACACS+ servers are used. If neither RADIUS nor TACACS+ servers are configured, local authentication is used.

Usage Guidelines
Use this command to authenticate all the management sessions through TACACS+ servers. The TACACS+ server should be configured before using this command. This command fails if the primary and secondary TACACS+ servers are not configured.

The following types of management sessions can be configured:
- Telnet
- SSH
- Console
- HTTP

If you are using TACACS+ authentication servers, you should only use TACACS+ accounting servers for accounting management sessions. TACACS+ authentication servers should be configured before configuring TACACS+ accounting servers for management sessions.

Example
In the following example, management sessions for both the primary and secondary servers are configured for TACACS+ accounting:

```
```

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.
Platform Availability

This command is available on all platforms.
configure auth netlogin radius

configure auth netlogin radius primary [<ipaddress> | <hostname>] {secondary [<ipaddress> | <hostname>]}

Description
Configures authentication of netlogin sessions through RADIUS servers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary RADIUS authentication server that is used for netlogin sessions.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary RADIUS authentication server that is used for netlogin sessions.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP addresses of the primary or secondary server.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the authentication server.</td>
</tr>
</tbody>
</table>

Default
Unconfigured. Uses RADIUS for authentication for login sessions. If RADIUS is not enabled, TACACS+ servers are used. If neither RADIUS nor TACACS+ servers are configured, local authentication is used.

Usage Guidelines
The RADIUS server must be configured before this command is used. The command fails if the given primary and secondary RADIUS servers are not configured or if RADIUS authentication is not configured for netlogin sessions.

The following types of netlogin sessions can be configured:

- Dot1x-based netlogin
- Web-based netlogin

If you are using RADIUS authentication servers, you should only use RADIUS accounting servers for accounting management sessions. RADIUS authentication servers should be configured before configuring RADIUS accounting servers for management sessions.

Examples
In the following example, both primary and secondary RADIUS servers are configured for netlogin:

```
```

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure auth netlogin radius-accounting

configure auth netlogin radius-accounting primary [<ipaddress> | <hostname>] [secondary [<ipaddress> | <hostname>]]

**Description**

Configures the use of RADIUS accounting servers for netlogin session accounting.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary RADIUS accounting server that is used for netlogin sessions.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary RADIUS accounting server that is used for netlogin sessions.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address of the primary or secondary accounting server.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the primary or secondary accounting server.</td>
</tr>
</tbody>
</table>

**Default**

Unconfigured. Uses RADIUS for authentication for login sessions. If RADIUS is not enabled, TACACS+ servers are used. If neither RADIUS nor TACACS+ servers are configured, local authentication is used.

**Usage Guidelines**

The RADIUS accounting servers should be configured before this command is used. This command returns an error if the given primary and secondary RADIUS servers are not configured or if RADIUS authentication is not configured for netlogin sessions.

The following types of netlogin sessions can be configured:

- Dot1x-based netlogin
- Web-based netlogin

If you are using RADIUS authentication servers, you should only use RADIUS accounting servers for accounting management sessions. RADIUS authentication servers should be configured before configuring RADIUS accounting servers for management sessions.

**Example**

This example configures both primary and secondary RADIUS accounting servers for network login:

```
```

**History**

This command was first available in ExtremeWare 7.3.0 and in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure cpu-dos-protect alert-threshold

    configure cpu-dos-protect alert-threshold <packets per second>

**Description**
Configures the number of packets per second that the switch needs to receive on a port for an access list to be enabled for denial of service protection.

**Syntax Description**

<table>
<thead>
<tr>
<th>packets per second</th>
<th>Configures the number of packets per second that the switch needs to receive on a port for an access list to be enabled. Range is 150 to 100,000 packets per second.</th>
</tr>
</thead>
</table>

**Default**
4000 packets per second

**Usage Guidelines**
When heavy traffic reaches the alert threshold, a hardware ACL is created that blocks the traffic for the timeout number of seconds.

**Example**
The following command configures a threshold of 3000 or more packets.

```
configure cpu-dos-protect alert-threshold 3000
```

**History**
This command was first available in ExtremeWare 6.2.2.
The filter-type-allowed keyword was added in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure cpu-dos-protect filter-precedence

configure cpu-dos-protect filter-precedence <number>

Description
Configures the access list precedence for denial of service protection. If you set the filter-precedence to 0, the ACLs created by DoS protection will be overwritten by the default VLAN QoS profile.

Syntax Description

| filter-precedence | Configures the access list precedence. |

Default
The default is 10.

Usage Guidelines
When heavy traffic reaches the alert threshold, a hardware ACL is created that blocks the traffic for the timeout number of seconds.

Example
The following command configures filter-precedence of 5:

```
configure cpu-dos-protect filter-precedence 5
```

History
This command was first available in ExtremeWare 6.2.2.
The filter-type-allowed keyword was added in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure cpu-dos-protect filter-type-allowed

configure cpu-dos-protect filter-type-allowed <destination | source>

Description
Configures the type of access list allowed for denial of service protection.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>destination</td>
<td>Specifies that destination ACLs can be created.</td>
</tr>
<tr>
<td>source</td>
<td>Specifies that source ACLs can be created.</td>
</tr>
</tbody>
</table>

Default
The default is destination.

Usage Guidelines
When heavy traffic reaches the alert threshold, a hardware ACL is created that blocks the traffic for the timeout number of seconds.

Example
The following command specifies that source ACLs can be created:

configure cpu-dos-protect filter-type-allowed source

History
This command was first available in ExtremeWare 6.2.2.
The filter-type-allowed keyword was added in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure cpu-dos-protect messages

configure cpu-dos-protect messages [on | off]

Description
Configures messaging for denial of service protection.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Turns messaging on.</td>
</tr>
<tr>
<td>off</td>
<td>Turns messaging off.</td>
</tr>
</tbody>
</table>

Default
The default is on.

Usage Guidelines
None

Example
The following command sets messaging to be off:
configure cpu-dos-protect messages off

History
This command was first available in ExtremeWare 6.2.2.
The filter-type-allowed keyword was added in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure cpu-dos-protect notice-threshold

configure cpu-dos-protect notice-threshold <packets per second>

Description
Configures the number of packets per second that the switch needs to receive on a port for messages to be logged. Used for denial of service protection.

Syntax Description

| packets per second | Configures the number of packets per second that the switch needs to receive on a port for messages to be logged. The range is 150 to 100,000 packets per second. |

Default
The default is 4000.

Usage Guidelines
None

Example
The following command configures a notice threshold of 2000:
configure cpu-dos-protect notice-threshold 2000

History
This command was first available in ExtremeWare 6.2.2.
The filter-type-allowed keyword was added in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure cpu-dos-protect timeouts

configure cpu-dos-protect timeouts <seconds>

Description
Configures the number of seconds prior to timeout for denial of services.

Syntax Description

| seconds | Specifies the number of seconds before a timeout takes place. |

Default
None

Usage Guidelines
When heavy traffic reaches the alert threshold, a hardware ACL is created that blocks the traffic for the timeout number of seconds.

Example
The following command configures timeout of 10 seconds:
configure cpu-dos-protect timeouts 10

History
This command was first available in ExtremeWare 6.2.2.
The filter-type-allowed keyword was added in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure cpu-dos-protect trusted-ports

configure cpu-dos-protect trusted-ports [add <slot number> | all | delete <slot number> | none | <slot number>]

Description
Specifies the ports to be trusted when considering denial of service threats.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds trusted port protection.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all ports are trusted.</td>
</tr>
<tr>
<td>delete</td>
<td>Deletes a trusted port.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no ports are trusted.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies trust for a given slot number.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
When heavy traffic reaches the alert threshold, a hardware ACL is created that blocks the traffic for the timeout number of seconds.

Example
The following command specifies that all ports are to be trusted:

```
configure cpu-dos-protect trusted-ports all
```

The following command adds port 1:4 to the trusted list:

```
configure cpu-dos-protect trusted-ports add 1:4
```

The following command deletes ports 1:4 and 1:5 from the trusted list:

```
configure cpu-dos-protect trusted-ports delete 1:4, 1:5
```

History
This command was first available in ExtremeWare 6.2.2.

The filter-type-allowed keyword was added in ExtremeWare 7.0.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure cpu-dos-protect (Port-Based)

    configure cpu-dos-protect [ports <portnumber> | all] alert-threshold <pkts>
    interval-time <seconds>

Description
Sets the maximum allowed limit before invoking denial of service (DoS) protection and discarding packets.

NOTE
This command is available only on the “e” series switches.

Syntax Description

| portnumber | Specifies one or more port numbers. May be in the form 1, 2, 3-5. |
| pkts       | Configures the maximum number of packets, or threshold level, where packets are discarded. Range is 50 to 20000 packets per second. Default is 150. |
| seconds    | Configures a duration in seconds. Range is 1 to 20 seconds. Default is 1 second. |

Default
All ports are disabled for DoS protection.

Usage Guidelines
Use this command to set thresholds beyond which broadcasts are blocked on specified ports. You can also use it to identify layer 3 misses to the CPU or when too many IP multicasts are coming on a port.

Examples
The following example configures an alert threshold of 500 packets on port 8 every 3 seconds:

    config cpu-dos-protect port 8 disable alert-threshold 500 interval-time 3

History
This command was first introduced in ExtremeWare 7.2e.

Platform Availability
This command is available on “e” series platforms only.
configure cpu-dos-protect trusted-ports

configure cpu-dos-protect trusted-ports [add <port number> | delete <port number> | all | none]

**Description**

Configures the trusted port feature at a system level.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port number</td>
<td>Specifies a port.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports as trusted.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no ports are trusted.</td>
</tr>
</tbody>
</table>

**Default**

By default, no ports are trusted.

**Usage Guidelines**

Use this command to define one or more ports as trusted ports, to delete trusted ports, or to specify that no ports are trusted. Typically, you would use the `all` parameter when you want to set the denial of service protection to only a few of the ports on a switch. Use the `all` parameter, then use the command `configure cpu-dos-protect trusted-ports delete <port number>` to set ports that should not be trusted (that denial of service protection should be applied to).

**Example**

The following command configures a port as trusted, so that denial of service protection is not applied to port 3:

```
configure cpu-dos-protect trusted-port add 3
```

**History**

This command was first available in ExtremeWare 7.0.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure enhanced-dos-protect ipfdb agingtime

configure enhanced-dos-protect ipfdb agingtime <aging> ports <portlist>

**Description**

Configures the aging time on untrusted ports for enhanced denial of service protection.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>aging</td>
<td>Specifies the number of seconds for the aging time per port. The aging value is the software cache timeout: the duration of time to be considered to reach the threshold. The valid range is 1-300 seconds. The default value is 30 seconds.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

**Default**

The default aging time is 30 seconds.

**Usage Guidelines**

Use this command to change the aging time values for selected untrusted ports. To verify configuration, use the `show enhanced-dos-protect` command and view data in the Aging column.

**Example**

The following command configures the aging time on port 2 to 100 seconds:

```
configure enhanced-dos-protect ipfdb agingtime 100 ports 2
```

**History**

This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure enhanced-dos-protect ipfdb cache-size

configure enhanced-dos-protect ipfdb cache-size <cache-size>

**Description**
Configures the cache size on untrusted ports for enhanced denial of service protection.

**Syntax Description**

| cache-size | Specifies the cache size limit in kilobytes. The default value is 256. The maximum value is 256000. |

**Default**
The default cache size value is 256.

**Usage Guidelines**
Enhanced DoS protection maintains the number of IPFDB entries according to the cache-size limit. Use this command to set the cache size to a value other than the default value of 256K.

Use the following command to reset the cache size to the 256K default value:

```
unconfigure enhanced-dos-protect ipfdb cache-size
```

**Example**
The following command configures the cache size at 512K:

```
configure enhanced-dos-protect ipfdb cache-size 512
```

**History**
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure enhanced-dos-protect ipfdb learn-limit

configure enhanced-dos-protect ipfdb learn-limit <learn-limit> ports <portlist>

Description
Configures the learning limit on untrusted ports for enhanced denial of service protection.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>learn-limit</td>
<td>Specifies the number of packets allowed on the selected ports within the learning window before the rate limit is applied; or before the software can create an IPFDB entry in the hardware. The valid value range is 100-1953125. The default on Fast Ethernet ports is 100 pkts/learn window. The default on Gigabyte ports is 100 pkts/learn window.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*; 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

Default
The default learn-limit on Fast Ethernet ports is 100 pkts/learn window.
The default learn-limit on Gigabyte ports is 100 pkts/learn window.

Usage Guidelines
Use this command to configure a learning limit value to define the number of packets to be counted before ExtremeWare can create an IPFDB entry in the hardware.

To reset the learning limit for enhanced denial of service protection to default values for selected ports, use the following command:

unconfigure enhanced-dos-protect ipfdb learn-limit

Example
The following command configures the learn limit on port 3 at 75 packets within the learning window before the IPFDB entry is created:

configure enhanced-dos-protect ipfdb learn-limit 75 ports 3

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure enhanced-dos-protect ipfdb learn-window

configure enhanced-dos-protect ipfdb learn-window <learn-window> ports <portlist>

Description
Configures the learning window on untrusted ports for the enhanced denial of service protection IPFDB learning qualifier.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>learn-window</td>
<td>Specifies the number of seconds for the learning window per port. This value is the duration of time to be considered to reach the threshold. The valid range is 5-300 seconds. The default value is 10 seconds.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

Default
The default learning window is 10 seconds.

Usage Guidelines
Use this command to change the learning window values for selected untrusted ports. To verify configuration, use the following command:

show enhanced-dos-protect ipfdb ports <portlist>

Example
The following command configures the learn window on port 2 at 80 seconds:

configure enhanced-dos-protect ipfdb learn-window 80 ports 2

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure enhanced-dos-protect ports

configure enhanced-dos-protect ports [trusted | untrusted] <portlist>

Description
Configures ports as trusted, so that enhanced denial of service protection is not applied to the ports; or configures ports as untrusted, so that enhanced denial of service protection is applied to the ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>trusted</td>
<td>Specifies the selected ports as trusted, so that enhanced denial of service is not applied to the ports.</td>
</tr>
<tr>
<td>untrusted</td>
<td>Specifies the selected ports as untrusted, so that enhanced denial of service is applied to the ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
By default, ports are trusted.

Usage Guidelines
You can configure each port as trusted or untrusted. A trusted port behaves as a normal port. An untrusted port behaves according to the configuration parameter used in IPFDB thrashing.

To verify the status of each port, use the following command:

show enhanced-dos-protect [rate-limit | ipfdb] ports <portlist>

Example
The following command configures a range of ports as trusted, so that enhanced denial of service protection is not applied to ports 2 through 4:

configure enhanced-dos-protect ports trusted 2-4

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure enhanced-dos-protect rate-limit

configure enhanced-dos-protect rate-limit [threshold <threshold> | drop-probability <drop-probability> | learn-window <learn-window> | protocol [all | icmp]] ports <portlist>

Description
Configures rate limiting for enhanced denial of service protection.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>Specifies the number of packets allowed on a given port within the learning window before the rate limit is applied. The valid value range is 100-1953125. The default on Fast Ethernet ports is 100 pkts/learn window. The default on Gigabyte ports is 100 pkts/learn window.</td>
</tr>
<tr>
<td>drop-probability</td>
<td>Specifies the percentage of slow-path traffic to be dropped per port. The valid range is 0-100 percent. The default value is 50 percent.</td>
</tr>
<tr>
<td>learn-window</td>
<td>Specifies the number of seconds for the learning window per port. This value is the duration of time to be considered to reach the rate limit threshold. The valid range is 5-300 seconds. The default value is 10 seconds.</td>
</tr>
<tr>
<td>protocol [all</td>
<td>icmp]</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:, 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

Default
The default threshold on Fast Ethernet ports is 100 pkts/learn window.
The default threshold on Gigabyte ports is 100 pkts/learn window.
The default drop-probability is 50 percent.
The default learn-window value is 10 seconds.
Rate limiting is applied by default to ICMP packets.

Usage Guidelines
Use this command to configure the rate-limit threshold, drop probability, learning window, or packet protocol. To verify settings, use the show enhanced-dos-protect rate-limit ports <portlist> command. To remove ports from rate limiting, use the unconfigure enhanced-dos-protect rate-limit command.

Examples
The following command sets the rate limiting threshold on port 3 to 200 packets:
configure enhanced-dos-protect rate-limit threshold 200 ports 3
The following command sets the rate limiting drop probability on port 4 to 60 percent:
configure enhanced-dos-protect rate-limit drop-probability 50 ports 4
The following command sets the rate limiting learn window on ports 2 and 3 to 90 seconds:
```
configure enhanced-dos-protect rate-limit learn-window 90 ports 2,3
```
The following command sets the rate limiting protocol to all packet types on ports 1 through 3:
```
configure enhanced-dos-protect rate-limit protocol all ports 1-3
```

**History**

This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure ip-subnet-lookup maskbits

configure ip-subnet-lookup maskbits <length>

Description
This command changes the length of the IPDA subnet lookup mask.

NOTE
This command is available only on the “i” series switches.

Syntax Description

| length | Specifies the number of maskbits for the IPDA subnet lookup mask. Default is 24. |

Default
The default length of the subnet lookup mask is 24 bits.

Usage Guidelines
For a new setting to be effective, system rebooting is needed.

Example
The following example changes the length of the IPDA subnet lookup mask to 18 bits:
configure ip-subnet-lookup maskbits 18

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on “i” series platforms only.
configure mac-lockdown-timeout ports aging-time

configure mac-lockdown-timeout ports [<portlist> | all] aging-time <seconds>

Description
This command configures the MAC address lockdown timeout value in seconds for the specified port or group of ports or for all ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>seconds</td>
<td>Sets the length of the timeout value in seconds. Default is 15; range is 15 to 2,000,000.</td>
</tr>
</tbody>
</table>

Default
15 seconds

Usage Guidelines
This timer overrides the FDB aging time.

This command only sets the duration of the MAC address lockdown timer. To enable the lockdown timer, use the enable mac-lockdown-timeout ports command.

Example
The following example sets a MAC address lockdown timeout duration of 300 seconds for ports 3, 4, and 5.

configure mac-lockdown-timeout ports 3-5 aging-time 300

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
configure netlogin base-url

configure netlogin base-url <url>

Description
This command configures the base URL for network login.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>url</td>
<td>Specifies the base URL for network login.</td>
</tr>
</tbody>
</table>

Default
The base URL default value is “network-access.net”.

Usage Guidelines
When you log in using a web browser, you are redirected to the specified base URL, which is the DNS name for the switch.

You must configure a DNS name of the type “www.xx...xx.xxx” or “xx...xx.xxx”.

This command applies only to the web-based authentication mode of network login.

Example
The following example configures the base URL as access.net:

```
configure netlogin base-url access.net
```

History
This command was first available in ExtremeWare 7.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure netlogin mac-address

configure netlogin  mac-address [ <mac-address> {mask <mask>} | default ] {<password>}

Description
Configures the MAC address/mask pairs that are used for authentication in MAC-based network login.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Used as the default entry password the supplicant's mac-address does not match any of the entries in the table.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a mask.</td>
</tr>
<tr>
<td>password</td>
<td>Sets a password other than the MAC address.</td>
</tr>
</tbody>
</table>

Default
By default, MAC-based authentication for network login is disabled.

Usage Guidelines
MAC-based RADIUS authentication uses the MAC address of the client for authentication. This feature is useful for devices that cannot function as 802.1x supplicants, such as IP phones. RADIUS is used as the transport protocol for authentication.

Only one default entry can be configured; this will be used if none of the configured entries match.

If no mask is specified, the default mask ff:ff:ff:ff:ff:ff will be assigned to the MAC entry.

If a password is not configured locally, the user name sent in the RADIUS Access-Request is used as the password.

Example
The following example adds a MAC address/mask pair to the table used for authentication and defines a password:

```
configure netlogin mac-address 00:11:33:55:77:99 mask ff:ff:ff:ff:ff:00 pngs2r
```

The following command configures the MAC address and mask using the default entry password pngs2r:

```
configure netlogin mac-address default pngs2r
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
configure netlogin mac auth-retry-count

configure netlogin mac auth-retry-count <value>

Description
Configures the maximum number of times the RADIUS client tries again to authenticate a port using the MAC address before it times out.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Specifies the maximum number of retries for MAC-based RADIUS authentication. The range of values is 3–100.</td>
</tr>
</tbody>
</table>

Default
The default number of retries is three.

Usage Guidelines
When a new MAC address is detected on a port enabled for MAC-based network login, an authentication message (RADIUS Access-Request message) is sent from the RADIUS client to the RADIUS server for validation. This command specifies the maximum number of times the RADIUS client tries again if the validation request fails. After the third retry, the authentication attempt times out.

Example
The following example sets a retry count of 8:

```
configure netlogin mac auth-retry-count 8
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
configure netlogin mac reauth-period

configure netlogin mac reauth-period <seconds>

Description
Configures the reauthentication interval for ports using MAC-based RADIUS authentication.

Syntax Description

| seconds | Specifies the interval between successive RADIUS Access-Request messages that reauthenticate the port. The range of values is 600-60000. |

Default
1800 seconds

Usage Guidelines
While a port is in an authenticated state, the reauthentication mechanism periodically sends a RADIUS Access-Request message to the RADIUS server to reauthenticate the port. This command specifies the number of seconds between successive reauthentication messages.

Example
The following example sets a reauthentication period of 300 seconds:

```
configure netlogin mac reauth-period 300
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
configure netlogin redirect-page

    configure netlogin redirect-page <url>

Description
Configures the redirect URL for network login.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;url&gt;</td>
<td>Specifies the redirect URL for network login.</td>
</tr>
</tbody>
</table>

Default
The redirect URL default value is “http://www.extremenetworks.com”.

Usage Guidelines
In ISP mode, you can configure network login to be redirected to a base page after successful login using this command. If a RADIUS server is used for authentication, then base page redirection configured on the RADIUS server takes priority over this configuration.

You must configure a complete URL starting from either http:// or https://

This command applies only to the web-based authentication mode of network login.

Example
The following example configures the redirect URL as http://www.extremenetworks.com:

    configure netlogin redirect-page http://www.extremenetworks.com

History
This command was first available in ExtremeWare 7.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure radius server

For the “i” series switches:

configure radius [primary | secondary] server [<ipaddress> | <hostname>] {<L4 port no>} client-ip [<ipaddress>]

For the “e” series switches:

configure radius [primary | secondary] server [<ipaddress> | <hostname>] client-ip [<ipaddress>]

Description
Configures the primary and secondary RADIUS authentication server.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary RADIUS authentication server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary RADIUS authentication server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>IP address of the server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Host name of the server being configured. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>IP address used by the switch to identify itself when communicating with the RADIUS authentication server.</td>
</tr>
<tr>
<td>L4 port no</td>
<td>L4 port used to contact the RADIUS server.</td>
</tr>
</tbody>
</table>

NOTE: This option is available only on the “i” series switches.

Default
The default UDP port setting is 1645.

Usage Guidelines
Use this command to specify RADIUS server information. You can configure up to two primary and two secondary RADIUS authentication servers.

Use of the hostname parameter requires that DNS be enabled.

The RADIUS server defined by this command is used for user name authentication and CLI command authentication.

Example
The following command configures the primary RADIUS server on host radius1 using the default UDP port (1645) for use by the RADIUS client on switch 10.10.20.30:

configure radius primary server radius1 client-ip 10.10.20.30

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
configure radius shared-secret

configure radius [primary | secondary] shared-secret (encrypted) [<string>]

Description
Configures the authentication string used to communicate with the RADIUS authentication server.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the authentication string for the primary RADIUS server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the authentication string for the secondary RADIUS server.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Indicates that the secret should be encrypted.</td>
</tr>
<tr>
<td>string</td>
<td>The string to be used for authentication.</td>
</tr>
</tbody>
</table>

Default
Unconfigured

Usage Guidelines
The secret must be the same between the client switch and the RADIUS server.
The RADIUS server must first be configured for use with the switch as a RADIUS client.
If the server address is not specified, it configures shared-secret for all configured primary and secondary RADIUS authentication servers.
You must configure the RADIUS server first before configuring the shared secret for a specific server.

Example
The following command configures the shared secret as “purplegreen” on the primary RADIUS server:
configure radius primary shared-secret purplegreen

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure radius timeout

configure radius {[primary | secondary] {server <ipaddress> | <hostname>}}
timeout <seconds>

Description
Configures the timeout interval for RADIUS authentication requests.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the timeout for the primary RADIUS server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the timeout for the secondary RADIUS server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the server being configured.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds to wait before retrying accounting requests. Range is 3 to 120 seconds.</td>
</tr>
</tbody>
</table>

Default
The default is 3 seconds.

Usage Guidelines
This command configures the timeout interval for RADIUS authentication requests. When the timeout has expired, another authentication attempt is made. After three failed attempts to authenticate, the alternate server is used. After five failed attempts, local user authentication is used.

Examples
This example configures a timeout interval of 10 seconds for RADIUS authentication. After 30 seconds (three attempts), the alternate RADIUS server is used. After 50 seconds (five attempts) local user authentication is used:

```bash
configure radius timeout 10
```

This example configures a timeout interval of 10 seconds for the primary RADIUS authentication server. After 30 seconds (three attempts), the alternate RADIUS server is used. After 50 seconds (five attempts) local user authentication is used:

```bash
configure radius primary timeout 10
```

This example configures a timeout interval of 10 seconds for RADIUS secondary server 192.168.4.4 authentication. After 30 seconds (three attempts), the alternate RADIUS server is used. After 50 seconds (five attempts) local user authentication is used:

```bash
configure radius secondary server 192.168.4.4 timeout 10
```

History
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
**Platform Availability**
This command is available on all platforms.
configure radius-accounting server

configure radius-accounting [primary | secondary] server [<ipaddress> | <hostname>] {<L4 port no>} client-ip [<ipaddress>]

Description
Configures the primary and secondary RADIUS accounting servers.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configure the primary RADIUS accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configure the secondary RADIUS accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address of the accounting server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>The host name of the accounting server being configured.</td>
</tr>
<tr>
<td>udp_port</td>
<td>The UDP port to use to contact the RADIUS accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address used by the switch to identify itself when communicating with the RADIUS accounting server.</td>
</tr>
</tbody>
</table>

Default
The default UDP port setting is 1646.

Usage Guidelines
Use this command to specify the RADIUS accounting server information for up to two primary and two secondary RADIUS accounting servers.

The accounting server and the RADIUS authentication server can be the same.

Use of the <hostname> parameter requires that DNS be enabled.

Example
The following command configures RADIUS accounting on host radius1 using the default UDP port (1646) for use by the RADIUS client on switch 10.10.20.30:

configure radius-accounting primary server radius1 client-ip 10.10.20.30

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure radius-accounting shared-secret

configure radius-accounting [primary | secondary] shared-secret {encrypted} [<string>]

Description
Configures the authentication string used to communicate with the RADIUS accounting server.

Syntax Description

<table>
<thead>
<tr>
<th>primary</th>
<th>Configures the authentication string for the primary RADIUS accounting server.</th>
</tr>
</thead>
<tbody>
<tr>
<td>secondary</td>
<td>Configures the authentication string for the secondary RADIUS accounting server.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Indicates that the secret should be encrypted</td>
</tr>
<tr>
<td>string</td>
<td>The string to be used for authentication.</td>
</tr>
</tbody>
</table>

Default
Unconfigured

Usage Guidelines
The secret must be the same between the client switch and the RADIUS accounting server.
If the server address is not specified, shared-secret is configured on all primary and secondary RADIUS accounting servers.
You must configure the RADIUS accounting server first before configuring the shared secret for a specific server.

Example
The following command configures the shared secret as “purpleaccount” on the primary RADIUS accounting server:
configure radius-accounting primary shared-secret purpleaccount

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure radius-accounting timeout

configure radius-accounting ([primary | secondary] {server <ipaddress> | <hostname>}) timeout <seconds>

Description
Configures the timeout interval for RADIUS-Accounting authentication requests.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the timeout for the primary RADIUS accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the timeout for the secondary RADIUS accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the server being configured.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds to wait before retrying accounting requests. Range is 3 to 120 seconds</td>
</tr>
</tbody>
</table>

Default
The default is 3 seconds.

Usage Guidelines
This command configures the timeout interval for RADIUS accounting authentication requests. When the timeout expires, another authentication attempt is made. After three failed attempts to authenticate, the alternate server is used. After five failed attempts, local user authentication is used.

Examples
This example configures the timeout interval for RADIUS accounting authentication to 10 seconds. After 30 seconds (three attempts), the alternate RADIUS server is used:

```
configure radius-accounting timeout 10
```

This example configures the timeout interval for RADIUS accounting authentication to 10 seconds on the primary server. After 30 seconds (three attempts), the alternate RADIUS server is used:

```
configure radius-accounting primary timeout 10
```

This example configures the timeout interval for RADIUS accounting authentication to 10 seconds for the secondary server. After 30 seconds (three attempts), the alternate RADIUS server is used:

```
configure radius-accounting secondary server 192.168.4.12 timeout 10
```

History
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure route-map add

configure route-map <route-map> add <seq_number> [permit | deny] {match-one | match-all} {set lpm-routing | set iphost-routing}

Description
Adds an entry in the route map with the specified sequence number and action.

**NOTE**

*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>The name of the route map to which this entry should be added.</td>
</tr>
<tr>
<td>seq-number</td>
<td>Specifies a sequence number that uniquely identifies the entry, and determines the position of the entry in the route map.</td>
</tr>
<tr>
<td>permit</td>
<td>Permits the route.</td>
</tr>
<tr>
<td>deny</td>
<td>Denies the route. This is applied only if the match is successful.</td>
</tr>
<tr>
<td>match-one</td>
<td>The route map is successful as long as at least one of the matching statements is true.</td>
</tr>
<tr>
<td>match-all</td>
<td>The route map is successful only when all match statements are true. This is the default setting.</td>
</tr>
<tr>
<td>set lpm-routing</td>
<td>Specifies how packets are to be routed for route-map matched IP prefixes. If the lpm-routing property is added to a route-map, packets are forwarded to the IP prefixes’ next hop by the ARM/MPLS module using LPM routing.</td>
</tr>
<tr>
<td>set iphost-routing</td>
<td>Specifies how packets are to be routed for route-map matched IP prefixes. If the iphost-routing property is added to a route-map, packets are forwarded to the IP prefixes’ next hop using the Inferno hardware host-based IP FDB. The set lpm-routing keyword is significant only for routes learned on VLANs that are not LPM routing enabled. The set iphost-routing keyword is significant only for routes learned on VLANs that are LPM routing enabled.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The sequence number determines the order of the entry in the route map.

The action (permit or deny) specifies the action to be taken on a successful match against the statements in the route map.

After an entry has been added to the route map, statements must be added to define the routes that should be matched, using the configure <route-map> add match command.

This command can be used to override the VLAN LPM routing configuration for specific routes. The set lpm-routing and set iphost-routing keywords specify how packets are to be routed for route-map matched IP prefixes. If the lpm-routing property is added to a route-map, packets are forwarded to the IP prefixes’ next hop by the ARM/MPLS module using LPM routing.

If the set iphost-routing property is added to a route-map, packets are forwarded to the IP prefixes’ next hop using the Inferno hardware host-based IP FDB. The set lpm-routing keyword is significant only for routes learned on VLANs that are not LPM routing enabled. The set iphost-routing keyword is significant only for routes learned on VLANs that are LPM routing enabled.
**Examples**

The following command adds an entry to the route-map named `bgp-out` that denies all matching routes:

```
configure route-map bgp-out add 10 deny
```

The following command adds an entry to the route-map named `bgp-out` that will be evaluated after the previous entry, and that permits all matching routes:

```
configure route-map bgp-out add 20 permit
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available only on the “i” series platforms.
configure route-map add goto

configure route-map <route_map> <seq_number> add goto <new_route_map>

Description
Configures a route map goto statement to transfer evaluation to another route map.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>The name of the route map to which this statement should be added.</td>
</tr>
<tr>
<td>seq-number</td>
<td>Specifies the sequence number of the entry in the route map to which this statement should be added.</td>
</tr>
<tr>
<td>new-route-map</td>
<td>The name of another route map that should be evaluated.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
A route map goto statement is evaluated only after all match and set statements have been evaluated.

Example
The following command adds a goto statement to entry 25 in route map map1 that causes evaluation control to transfer to route map map2:

```bash
configure route-map map1 25 add goto map2
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available only on the “i” series platforms.
configure route-map add match

configure route-map <route-map> <seq_number> add match [nlri-list <access profile> | as-path [access-profile <access profile> | <as_number>]] | community [access-profile <access profile> | <as_number>:<number> | number <community> | no-advertise | no-export | no-export-subconfed] | next-hop <ip address> | med <number> | tag <number> | origin [igp | egp | incomplete]]

Description
Configures a route map match statement.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>The name of the route map to which this statement should be added.</td>
</tr>
<tr>
<td>seq-number</td>
<td>Specifies the sequence number of the entry in the route map to which this statement should be added.</td>
</tr>
<tr>
<td>nlri-list &lt;access profile&gt;</td>
<td>Specifies an access profile against which the NLRI should be matched.</td>
</tr>
<tr>
<td>as-path access-profile</td>
<td>Specifies an access profile against which the AS path in the path attributes should be matched.</td>
</tr>
<tr>
<td>as-number</td>
<td>Specifies an AS number against which the AS path in the path attributes should be matched.</td>
</tr>
<tr>
<td>community access-profile</td>
<td>Specifies a BGP community access profile against which the community attribute should be matched.</td>
</tr>
<tr>
<td>as_number:number</td>
<td>Specifies a BGP community number, specified in as_number:number format, against which the community attribute should be matched.</td>
</tr>
<tr>
<td>community</td>
<td>Specifies a BGP community number, specified as an unsigned 32-bit integer in decimal format, against which the community attribute should be matched.</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies that the community attribute should be matched against the no-export attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that the community attribute should be matched against the no-advertise attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Specifies that the community attribute should be matched against the no-export-subconfed attribute.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address against which the next hop attribute in the path attribute should be matched.</td>
</tr>
<tr>
<td>med_number</td>
<td>Specifies a MED number against which the MED in the path attribute should be matched.</td>
</tr>
<tr>
<td>origin [igp</td>
<td>egp</td>
</tr>
<tr>
<td>tag_number</td>
<td>Specifies a tag value against which the tag associated with the redistributed OSPF route should be matched.</td>
</tr>
</tbody>
</table>

Default
N/A
Usage Guidelines

A match operation specifies a criterion that must be matched for the route to be successful. If there are multiple statements in a route table entry, match statements are evaluated before set or goto statements.

When an entry has multiple match statements, the primitive match-one or match-all in the entry determines how many matches are required for success. If an entry has no match statements, the entry is always considered a successful match.

Example

The following command adds a statement to entry 10 in route map bgp-out that matches the NLRI against the access profile named iplist:

```
configure bgp-out 10 add match nlri-list iplist
```

The following command adds a statement to entry 15 in route map bgp-out that matches the AS path attribute against the access profile named aslist:

```
configure bgp-out 15 add match as-path access-profile aslist
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available only on the “i” series platforms.
configure route-map add set

configure route-map <route-map> <seq_number> add set [as-path <as_number> | community [ [access-profile <access-profile> | <as_number>:<number> | number <community> | no-advertise | no-export | no-export-subconfed] | remove | [add | delete] [access-profile <access-profile> | <as no> : <number> | number <community> | no-advertise | no-export | no-export-subconfed]] | next-hop <ip address> | med [internal | <med_number> | remove | [add | delete] <med_number>] local-preference <number> | weight <number> | origin [igp | egp | incomplete] | tag <tag_number> | accounting index <index_number> value <value_number> | cost <number> | cost-type [ase-type-1 | ase-type-2]]

Description
Configures a route map set entry.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>The name of the route map to which this statement should be added.</td>
</tr>
<tr>
<td>seq-number</td>
<td>Specifies the sequence number of the entry in the route map to which this</td>
</tr>
<tr>
<td></td>
<td>statement should be added.</td>
</tr>
<tr>
<td>as_number</td>
<td>Prepends the specified AS number to the AS path in the path attribute.</td>
</tr>
<tr>
<td>as_access_profile</td>
<td>Sets the community in the path attribute to the specified access profile.</td>
</tr>
<tr>
<td>as_number:number</td>
<td>Sets the community in the path attribute to the specified BGP community</td>
</tr>
<tr>
<td></td>
<td>number, specified in as_number:number format, in the path attribute.</td>
</tr>
<tr>
<td>community</td>
<td>Sets the community in the path attribute to the specified BGP community</td>
</tr>
<tr>
<td></td>
<td>number, specified as an unsigned 32-bit integer in decimal format.</td>
</tr>
<tr>
<td>no-export</td>
<td>Sets the community in the path attribute to the no-export attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Sets the community in the path attribute to the no-advertise attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Sets the community in the path attribute to the no-export-subconfed attribute.</td>
</tr>
<tr>
<td>remove</td>
<td>Removes the community attribute, if present.</td>
</tr>
<tr>
<td>add I delete</td>
<td>Adds or deletes the specified access profile to or from the existing</td>
</tr>
<tr>
<td></td>
<td>community in the path attribute.</td>
</tr>
<tr>
<td>add I delete</td>
<td>Adds or deletes the specified BGP community number, specified in</td>
</tr>
<tr>
<td></td>
<td>as_number:number format, to or from the existing community in the path</td>
</tr>
<tr>
<td>add I delete</td>
<td>attribute.</td>
</tr>
<tr>
<td>add I delete</td>
<td>Adds or deletes the specified BGP community number, specified as an</td>
</tr>
<tr>
<td></td>
<td>unsigned 32-bit integer in decimal format, to or from the existing</td>
</tr>
<tr>
<td>add I delete</td>
<td>community in the path attribute.</td>
</tr>
<tr>
<td>add I delete</td>
<td>Adds or deletes the no-export attribute to or from the existing community</td>
</tr>
<tr>
<td></td>
<td>in the path attribute.</td>
</tr>
<tr>
<td>add I delete</td>
<td>Adds or deletes the no-advertise attribute to or from the existing community</td>
</tr>
<tr>
<td></td>
<td>in the path attribute.</td>
</tr>
<tr>
<td>add I delete</td>
<td>Adds or deletes the no-export-subconfed attribute to or from the existing</td>
</tr>
<tr>
<td></td>
<td>community in the path attribute.</td>
</tr>
</tbody>
</table>
next-hop <ipaddress>  Sets the next hop in the path attribute to the specified IP address.
internal  When used in the BGP neighbor output route map, sets the MED attribute to a value equal to the metric to reach the next hop.
med_number  Sets the MED attribute to the specified value.
remove  Removes the MED attribute, if present.
add | delete <med_number>  Adds or deletes the specified value to or from the MED that is received. The final result is bound by 0 and 2147483647.
local-preference <number>  Sets the local preference in the path attribute to the specified local preference number.
weight <number>  Sets the weight associated with the NLRI to the specified number.
origin [igp | egp | incomplete]  Sets the origin in the path attributes to the specified origin.
tag <tag_number>  Sets the tag in the route to the specified number.
accounting index <index_number>  Specifies the index number of an accounting index to be set.
value <value_number>  Specifies the value to which the accounting index should be set.
cost <number>  Sets the cost of the route to the specified number.
cost-type <number>  Sets the cost type associated with the route (ase-type-1 or ase-type-2).

**Default**

N/A

**Usage Guidelines**

Route map set statements are evaluated after match statements, but before the goto statement.

When you change the route maps used to modify or filter NLRI information exchanged with neighbors, these changes are immediately effective on the routing information exchanged after the policy changes. The changes can be applied on the NLRI information that had been exchanged before the policy changes by issuing a soft reset on the ingress or egress side, depending on the changes. For soft resets to be applied on the ingress side, the changes must be previously enabled on the neighbor.

Changes to the route maps associated with network aggregation or redistribution commands becomes effective after a maximum interval of 30 seconds. You can immediately apply them by using the soft reconfiguration command.

**Example**

The following command modifies the routing information for a route that matches a statement in entry 15 of route table bgp-out include a MED value of 200:

```
configure bgp-out 15 add set med 200
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available only on the “i” series platforms.
configure route-map delete

    configure route-map <route_map> delete <seq_number>

Description
Deletes an entry from the route map.

⚠️ NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_map</td>
<td>The name of the route map to which this entry should be added.</td>
</tr>
<tr>
<td>seq_number</td>
<td>Specifies a sequence number that uniquely identifies the entry, and determines the position of the entry in the route map.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes the entry with sequence number 20 from the route-map named bgp-out:

    configure route-map bgp-out delete 20

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available only on the “i” series platforms.
configure route-map delete goto

    configure route-map <route_map> <seq_number> delete goto <new_route_map>

**Description**

Deletes a route map `goto` statement.

**NOTE**

This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route_map</td>
<td>The name of the route map from which this statement should be deleted.</td>
</tr>
<tr>
<td>seq_number</td>
<td>The sequence number of the entry in the route map from which this statement should be deleted.</td>
</tr>
<tr>
<td>new_route_map</td>
<td>The name of another route map.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

None

**Example**

The following command deletes the `goto` statement from entry 25 in route map `map1` that specifies transfer to route map `map2`:

```
configure route-map map1 25 delete goto map2
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available only on the “i” series platforms.
configure route-map delete match

configure route-map <route-map> <seq_number> delete match [nlri-list <access-profile> | as-path [access-profile <access-profile> | <as_number>] | community [access-profile <access-profile> | <as_number>:<number> | number <community> | no-advertise | no-export | no-export-subconfed] | next-hop <ip address> | med <number> | tag <number> | origin [igp | egp | incomplete]]

**Description**

Deletes a route map match statement.

**NOTE**

*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>The name of the route map from which this statement should be deleted.</td>
</tr>
<tr>
<td>seq-number</td>
<td>The sequence number of the entry in the route map from which this statement should be deleted.</td>
</tr>
<tr>
<td>nlri_access_profile</td>
<td>Specifies an NRLI-list access profile.</td>
</tr>
<tr>
<td>as_access_profile</td>
<td>Specifies an AS path access profile.</td>
</tr>
<tr>
<td>as-number</td>
<td>Specifies an AS number.</td>
</tr>
<tr>
<td>com_access_profile</td>
<td>Specifies a BGP community access profile.</td>
</tr>
<tr>
<td>as_number:number</td>
<td>Specifies a BGP community number in as_number:number format.</td>
</tr>
<tr>
<td>community</td>
<td>Specifies a BGP community number, specified as an unsigned 32-bit integer in decimal format.</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies the no-export community attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies the no-advertise community attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Specifies the no-export-subconfed community attribute.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address of the next hop attribute.</td>
</tr>
<tr>
<td>med_number</td>
<td>Specifies a MED number.</td>
</tr>
<tr>
<td>origin [igp</td>
<td>egp</td>
</tr>
<tr>
<td>tag_number</td>
<td>Specifies a tag value.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

None
Example

The following command deletes the statement from entry 15 in route map `bgp-out` that specifies that the access profile `aslist` should be used to match the AS path:

```
configure bgp-out 15 add match as-path access-profile aslist
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available only on the “i” series platforms.
configure route-map delete set

```bash
configure route-map <route-map> <seq_number> delete set [as-path <as_number> | community [access-profile <access-profile> | <as_number>:<number> | number <community> | no-advertise | no-export | no-export-subconfed] | remove | [add | delete] [access-profile <access-profile> | <as_number>:<number> | number <community> | no-advertise | no-export | no-export-subconfed] | next-hop <ip address> | med <number> | local-preference <number> | weight <number> | origin [igp | egp | incomplete] | tag <number> | accounting index <number> value <number> | cost <number> | cost-type [ase-type-1 | ase-type-2]]
```

**Description**

Deletes a route map set entry.

**NOTE**

This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>The name of the route map from which this statement should be deleted.</td>
</tr>
<tr>
<td>seq-number</td>
<td>The sequence number of the entry in the route map from which this statement should be deleted.</td>
</tr>
<tr>
<td>as-number</td>
<td>Specifies an AS number.</td>
</tr>
<tr>
<td>as_access_profile</td>
<td>Specifies an AS path access profile.</td>
</tr>
<tr>
<td>as_number:number</td>
<td>Specifies a BGP community number, in as_number:number format.</td>
</tr>
<tr>
<td>community</td>
<td>Specifies a BGP community number, as an unsigned 32-bit integer in decimal format.</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies the no-export attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies the no-advertise attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Specifies the no-export-subconfed attribute.</td>
</tr>
<tr>
<td>remove</td>
<td>Specifies removing the community attribute.</td>
</tr>
<tr>
<td>add</td>
<td>delete &lt;as_access_profile&gt;</td>
</tr>
<tr>
<td>add</td>
<td>delete &lt;as_number:number&gt;</td>
</tr>
<tr>
<td>add</td>
<td>delete &lt;community&gt;</td>
</tr>
<tr>
<td>add</td>
<td>delete &lt;no-export&gt;</td>
</tr>
<tr>
<td>add</td>
<td>delete &lt;no-advertise&gt;</td>
</tr>
<tr>
<td>add</td>
<td>delete &lt;no-export-subconfed&gt;</td>
</tr>
<tr>
<td>next-hop &lt;ipaddress&gt;</td>
<td>Specifies the IP address of the next hop.</td>
</tr>
<tr>
<td>internal</td>
<td>Specifies setting the MED attribute to a value equal to the metric to reach the next hop.</td>
</tr>
<tr>
<td>med_number</td>
<td>Specifies setting the MED attribute to a specified value.</td>
</tr>
<tr>
<td>remove</td>
<td>Specifies removing the MED attribute.</td>
</tr>
</tbody>
</table>
Security Commands

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>delete &lt;med_number&gt;</td>
</tr>
<tr>
<td>local-preference &lt;number&gt;</td>
<td>Specifies a local preference number.</td>
</tr>
<tr>
<td>weight &lt;number&gt;</td>
<td>Specifies a weight associated with the NLRI.</td>
</tr>
<tr>
<td>origin [igp</td>
<td>egp</td>
</tr>
<tr>
<td>tag &lt;tag_number&gt;</td>
<td>Specifies the tag in the route to the specified number.</td>
</tr>
<tr>
<td>accounting index &lt;index_number&gt;</td>
<td>Specifies the index number of an accounting index to be set.</td>
</tr>
<tr>
<td>value &lt;value_number&gt;</td>
<td>Specifies a value for the accounting index.</td>
</tr>
<tr>
<td>cost &lt;number&gt;</td>
<td>Specifies the cost of the route.</td>
</tr>
<tr>
<td>cost-type &lt;number&gt;</td>
<td>Specifies the cost type.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

None

Example

The following command deletes the set statement from entry 15 of route table bgp-out that specified setting a MED value of 200:

```
configure bgp-out 15 delete set med 200
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available only on the “i” series platforms.
configure security-profile default-user-vlan

    configure security-profile <name> default-user-vlan <vlan>

Description
Configures the default data VLAN for wireless users.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the security profile.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies the name of the default VLAN for wireless users.</td>
</tr>
</tbody>
</table>

Default
Wireless management default VLAN

Usage Guidelines
Wireless users are placed in default-user-vlan after authentication. Users who do not have a VSA-VLAN assignment on the RADIUS server are placed in this VLAN.

Example
The following example sets the security profile open-auth to use the VLAN open-vlan:

    config security-profile open-auth default-user-vlan open-vlan

History
This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile dot11-auth network-auth encryption

configure security-profile <name> dot11-auth <open | shared> network-auth <none | dot1x | mac-radius | web-based | wpa | wpa-psk | wpa2 | wpa2-psk> encryption <none | aes | tkip | aes-tkip | wep64 | wep128>

Description
Enables dot11 authentication, network authentication, and encryption.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the names of the security profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>open</td>
<td>Indicates that no 802.11 level authentication is imposed.</td>
</tr>
<tr>
<td>shared</td>
<td>Indicates shared key authentication</td>
</tr>
<tr>
<td>none</td>
<td>Indicates that no network authentication is imposed.</td>
</tr>
<tr>
<td>dot1x</td>
<td>Specifies that 802.1x network authentication is used.</td>
</tr>
<tr>
<td>mac-radius</td>
<td>Specifies MAC level authentication using the RADIUS server</td>
</tr>
<tr>
<td>web-based</td>
<td>Specifies use of network login for authentication.</td>
</tr>
<tr>
<td>wpa</td>
<td>Specifies WPA1 authentication with RADIUS.</td>
</tr>
<tr>
<td>wpa-psk</td>
<td>Specifies WPA1 authentication with pre-shared keys.</td>
</tr>
<tr>
<td>wpa2</td>
<td>Specifies 802.11i (WPA2) authentication with RADIUS.</td>
</tr>
<tr>
<td>wpa2-psk</td>
<td>Specifies 802.11i (WPA2) authentication with pre-shared keys.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no encryption is used.</td>
</tr>
<tr>
<td>aes</td>
<td>Specifies that Advanced Encryption Standard (AES) is used.</td>
</tr>
<tr>
<td>aes-tkip</td>
<td>Specifies that AES or TKIP can be used.</td>
</tr>
<tr>
<td>tkip</td>
<td>Specifies that Temporal Key Integrity Protocol (TKIP) is used.</td>
</tr>
<tr>
<td>wep64</td>
<td>Specifies that Wired Equivalent Privacy (WEP) encryption is used with 64-bit keys.</td>
</tr>
<tr>
<td>wep128</td>
<td>Specifies that Wired Equivalent Privacy (WEP) encryption is used with 128-bit keys.</td>
</tr>
</tbody>
</table>

Default

N/A
## Usage Guidelines

The following table lists the valid combinations of authentication and encryption:

<table>
<thead>
<tr>
<th>Dot11 Authentication</th>
<th>Network Authentication</th>
<th>Encryption</th>
</tr>
</thead>
<tbody>
<tr>
<td>open</td>
<td>none</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
<tr>
<td>open</td>
<td>web-based</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
<tr>
<td>open</td>
<td>mac-radius</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- none</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
<tr>
<td>open</td>
<td>dot1x</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
<tr>
<td>open</td>
<td>wpa</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- tkip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- aes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- aes-tkip</td>
</tr>
<tr>
<td>open</td>
<td>wpa-psk</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- tkip</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- aes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- aes-tkip</td>
</tr>
<tr>
<td>open</td>
<td>wpa2</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- aes</td>
</tr>
<tr>
<td>open</td>
<td>wpa2-psk</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- aes</td>
</tr>
<tr>
<td>shared</td>
<td>none</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
<tr>
<td>shared</td>
<td>web-based</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
<tr>
<td>shared</td>
<td>mac-radius</td>
<td>Choices:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep64</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- wep128</td>
</tr>
</tbody>
</table>
Examples
The following command sets WPA2 authentication and encryption with AES encryption:

```
configure security-profile secure1 dot11-auth open network-auth wpa2 encryption aes
```

History
This command was first available in ExtremeWare 6.2s.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile dot1x-wpa-timers group-update-timer

configure security-profile <name> dot1x-wpa-timers group-update-timer <minutes>

Description
When the network-authentication is set to dot1x, WPA or WPA2, this command configures the interval when group keys for dot1x and WPA clients are updated.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of the security profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>Specifies the interval in minutes. Valid values are between 10 and 1440. The default value is 10 minutes.</td>
</tr>
</tbody>
</table>

Default
10 minutes

Usage Guidelines
Use this command to change WPA and dot1x key update time values. Change timers only when you do not want the keys to be updated frequently.

Example
The following command sets the interval for updating keys to 29 minutes in the security profile called open-profile:

configure security-profile open-profile dot1x-wpa-timers group-update-timer 29

History
This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile dot1x-wpa-timers pairwise-update-timer

configure security-profile <name> dot1x-wpa-timers pairwise-update-timer <minutes>

Description
When the network-authentication is set to dot1x, WPA or WPA2, this command configures the interval when pairwise keys for dot1x and WPA clients are updated.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of the security profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>Specifies the interval in minutes. Valid values are between 10 and 1440. The default value is 10 minutes.</td>
</tr>
</tbody>
</table>

Default
10 minutes

Usage Guidelines
Use this command to change WPA and dot1x key update time values. Change timers only when you do not want the keys to be updated frequently.

Examples
The following example sets the interval for updating keys to 60 minutes:

```
configure security-profile open-profile dot1x-wpa-timers pairwise-update-timer 60
```

History
This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile dot1x-wpa-timers reauth-period

configure security-profile <name> dot1x-wpa-timers reauth-period <seconds>

**Description**

When the network-authentication is set to dot1x, WPA or WPA2, this command configures the interval when clients are re-authenticated.

**Syntax Description**

| name    | Specifies the name of the security profile. |
| seconds | Specifies the interval in seconds. Valid values are between 600 and 60000. The default value is 600 seconds. |

**Default**

600 seconds

**Usage Guidelines**

Use this command to change the re-authentication interval time values for a security profile. Change timers only when you do not want the client to be re-authenticated frequently.

**Examples**

The following command sets the re-authentication interval for clients to 2 minutes:

```
configure security-profile open-profile dot1x-wpa-timers reauth-period 120
```

**History**

This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile ess-name

    configure security-profile <name> ess-name <ess_name>

Description
Sets the name of the wireless network for the 802.11 interface associated with the security profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the security profile.</td>
</tr>
<tr>
<td>ess_name</td>
<td>Specifies the ESS name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
ESS names can be shared across wireless ports and interfaces.

Example
The following example assigns the name shared_ess to the security profile shared-auth:

    config security-profile shared-auth ess-name shared_ess

History
This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile ssid-in-beacon

configure security-profile <name> ssid-in-beacon {on | off}

**Description**

Establishes whether the service set identifier (SSID) is advertised in the beacon frame.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the security profile.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies that the beacon contains the SSID.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that the beacon does not contain the SSID.</td>
</tr>
</tbody>
</table>

**Default**

On

**Usage Guidelines**

The beacon turns on whether or not the SSID is published in the beacon. If you set this command to off, the beacon does not contain the SSID, and the client must know the SSID before it can associate. Sniffing on the beacon shows an empty SSID.

Configuration changes take effect immediately and are propagated to all ports sharing the named profile. If the command fails, none of the changes is propagated to any of the ports.

**Example**

The following command configures the security profile called secure1 not to publish the SSID in the beacon:

```
configure security-profile secure1 ssid-in-beacon off
```

**History**

This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile use-dynamic-vlan

configure security-profile <name> use-dynamic-vlan {y | n}

Description
Determines whether or not the security profile uses the dynamic VLAN (VLAN pushed by the RADIUS server through a VSA (Vendor Specific Attribute)).

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the security profile.</td>
</tr>
<tr>
<td>y</td>
<td>Specifies yes, to use the dynamic VLAN. The default is y (yes).</td>
</tr>
<tr>
<td>n</td>
<td>Specifies no, not to use the dynamic VLAN.</td>
</tr>
</tbody>
</table>

Default
Y (yes)

Usage Guidelines
If the variable is set to Y (yes), and if the RADIUS server is configured to push back VSA 203 or 209, the pushed back VSAs will override the default-user-vlan setting. (If both VSAs are configured, then they must point to the same VLAN.) The user will be placed in the VLAN indicated by the VSA after authentication.

If the variable is set to N (no), the user will be placed in the VLAN indicated by default-user-vlan regardless of any VSAs from the RADIUS server.

NOTE
In systems with the Basic software license (“i” series) or Edge software license (“e” series), users are placed in the VLAN indicated default-user-vlan, regardless of the VSAs pushed back from the RADIUS server.

Use the following command to configure the default-user-vlan:

```plaintext
configure security-profile <name> default-user-vlan <vlan>
```

Example
The following example sets the security profile called open-profile to use the dynamic VLAN:

```plaintext
configure security-profile open-profile use-dynamic-vlan y
```

History
This command was first available in ExtremeWare 6.2a. It was added to the “e” series in 7.3e and to the “i” series in 7.3.0.
Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile wep default-key-index

configure security-profile <name> wep default-key-index <index>

**Description**
Sets the default key index for the security profile in case of static WEP encryption.

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the names of the security profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Specifies the index of the WEP key. Valid ranges are 0-3.</td>
</tr>
</tbody>
</table>

**Default**
Zero (0)

**Usage Guidelines**
Sets the index of the WEP key. The key at the specified index must be configured before you can set the default index for WEP auth/encryption.

Configuration changes take effect immediately and are propagated to all ports sharing the named profile. If the command fails, none of the changes is propagated to any of the ports.

The index value is used when a user sets the WEP key using the following command:

```
configure security-profile wep key add
```

**Examples**
The following example sets the index of the WEP key to 3:

```
configure security-profile wep-secure wep default-key-index 3
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile wep key add

configure security-profile <name> wep key add <index> [hex <hexoctet> | plaintext <string>]

Description
Adds the given WEP key at the specified index.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the names of the security profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>index</td>
<td>Specifies the index. Valid values are 0-3.</td>
</tr>
<tr>
<td>hexoctet</td>
<td>Specifies to use the hexadecimal value as the WEP key.</td>
</tr>
<tr>
<td>string</td>
<td>Specifies a plain text value as the WEP key.</td>
</tr>
</tbody>
</table>

Default
Hexadecimal

Usage Guidelines
This key is used for WEP encryption. If you use hex mode, the key should be made up of hexadecimal digits. (That is, if encryption-length is 64, the key should be 10 hexadecimal digits (64-24 (ICV) = 40bits = 5 bytes = 10 hexadecimal digits.) When you specify plaintext mode, the key is simply the ASCII value of the letters in the specified key (for example, A = 35 and so on...). Plaintext does not mean passphrase.

Configuration changes take effect immediately and are propagated to all ports sharing the named profile. If the command fails, none of the changes is propagated to any of the ports.

Examples
The following example adds the first WEP key (0) with the hexadecimal encryption code 1234567891:

```
configure security-profile wep-secure wep key add 0 hex 1234567891
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile wep key delete

configure security-profile <name> wep key delete [all | <integer>]

Description
Deletes the specified WEP key.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the security profile.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all WEP keys are deleted.</td>
</tr>
<tr>
<td>integer</td>
<td>Specifies the numeric value identifying the WEP key.</td>
</tr>
</tbody>
</table>

Default
Zero (0).

Usage Guidelines
When you delete a WEP key whose index is the default WEP key index, the default index is changed automatically to the lowest specified WEP key (or N/A if no WEP keys have been specified).

Configuration changes take effect immediately and are propagated to all ports sharing the named profile. If the command fails, none of the changes is propagated to any of the ports.

Example
The following example deletes the first WEP key (0).

configure security-profile wep-secure wep key delete 0

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile wpa-psk

    configure security-profile <name> wpa-psk [hex <hexadecimal_digit> | passphrase <alphanumeric_string>]

Description
Configures the WPA pre-shared key to have the specified hexadecimal or alphanumeric value.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the security profile.</td>
</tr>
<tr>
<td>hex</td>
<td>Specifies the WPA pre-shared key type as hexadecimal.</td>
</tr>
<tr>
<td>hexadecimal_digit</td>
<td>Specifies a 64-byte hexadecimal key.</td>
</tr>
<tr>
<td>alphanumeric_string</td>
<td>Specifies a passphrase name in ASCII alphanumeric notation (8-63 characters long)</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to configure the WPA pre-shared key using a hexadecimal (64 bytes) digit or ASCII alphanumeric string (8 to 63 characters long).

Examples
The following example configures the WPA pre-shared key “abcdefgh” for the security profile sec_prof1:

configure security-profile sec_prof1 wpa-psk passphrase abcdefgh

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile wpa2-psk

    configure security-profile <name> wpa2-psk [hex <hexadecimal_digit> | passphrase <alphanumeric_string>]

**Description**
Configures the WPA2 pre-shared key to have the specified hexadecimal or alphanumeric value.

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the names of the security profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>hex</td>
<td>Specifies the WPA2 pre-shared key type as hexadecimal.</td>
</tr>
<tr>
<td>digit</td>
<td>Specifies a 64-byte hexadecimal key.</td>
</tr>
<tr>
<td>string</td>
<td>Specifies a passphrase name in ASCII alphanumeric notation (8-63 characters long)</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to configure the WPA2 pre-shared key using a hexadecimal (64 bytes) digit or ASCII alphanumeric string (8 to 63 characters long).

**Examples**
The following example configures the WPA2 pre-shared key “abcdefg” for the security profile sec_prof1:

configure security-profile sec_prof1 wpa2-psk passphrase abcdefgh

**History**
This command is introduced in ExtremeWare 7.4.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure security-profile wpa-only

    configure security-profile <name> wpa-only [on | off]

Description
Prohibits use of wpa2 when wpa is selected as the network-authentication algorithm (see “configure security-profile dot11-auth network-auth encryption” on page 892).

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies name of the security-profile.</td>
</tr>
<tr>
<td>on</td>
<td>Prohibits use of wpa2 when wpa is selected as the network authentication algorithm.</td>
</tr>
<tr>
<td>off</td>
<td>Permits use of WPA2 in addition to WPA when WPA is selected as the network authentication algorithm.</td>
</tr>
</tbody>
</table>

Default
The default setting is off.

Usage Guidelines
This command is generally not required, because the default behavior permits both WPA and WPA2 security. Configuring the on option for the command may be required to pass the WPA2 system interoperability test.

Examples
The following command sequence configures WPA security with AES encryption and forces only WPA to be used (not WPA2):

```bash
configure security-profile secure1 dot11-auth open network-auth wpa encryption aes
configure security-profile secure1 wpa-only on
```

History
This command is first introduced in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.


**configure ssh2 key**

`configure ssh2 key {pregenerated}`

**Description**

Generates the Secure Shell 2 (SSH2) host key.

**Syntax Description**

| pregenerated | Indicates that the SSH2 authentication key has already been generated. The user will be prompted to enter the existing key. |

**Default**

The switch generates a key for each SSH2 session.

**Usage Guidelines**

Secure Shell 2 (SSH2) is a feature of ExtremeWare that allows you to encrypt session data between the switch and a network administrator using SSH2 client software, or to send encrypted data from the switch to an SSH2 client on a remote system. Image and configuration files may also be transferred to the switch using the Secure Copy Program (SCP) or the Secure File Transfer Protocol (SFTP).

Before you can enable SSH2, you must first obtain a security license from Extreme Networks. After you receive the license, you must enable SSH2 and generate a host key. To enable SSH2, use the `enable ssh2` command. To generate an SSH2 host key, use the `configure ssh2 key` command.

An authentication key must be generated before the switch can accept incoming SSH2 sessions. This can be done automatically by the switch, or you can enter a previously generated key.

If you elect to have the key generated, you are prompted to enter a set of random characters to be used in generating the key. The key generation process takes approximately ten minutes, and cannot be canceled after it has started. When the key has been generated, you should save your configuration to preserve the key.

To use a key that has been previously created, use the `pregenerated` keyword. You are prompted to enter the pregenerated key. You can use the `show configuration` command to list the previously generated key, and then copy and paste it after the prompt from the `configure ssh2 key pregenerated` command.

The key generation process generates the SSH2 private host key. The SSH2 public host key is derived from the private host key, and is automatically transmitted to the SSH2 client at the beginning of an SSH2 session.
Example

The following command generates an authentication key for the SSH2 session:

```
configure ssh2 key
```

The command responds with the following messages:

```
WARNING: Generating new server host key
This will take approximately 10 minutes and cannot be canceled.
Continue? (y/n)
```

If you respond yes, the command prompts as follows:

```
Enter some random characters. End with a newline
```

Type in a series of random characters, and then press the Enter or Return key. The key generation process proceeds.

To configure an SSH2 session using a previously generated key, use the following command:

```
configure ssh2 key pregenerated
```

The command responds with the following message:

```
Please enter the server key
```

Enter the previously-generated key (you can copy and paste it from the saved configuration file).

History

This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
configure ssl certificate pregenerated

configure ssl certificate pregenerated

Description
Obtains the pre-generated certificate from the user.

Syntax Description
This command has no parameters or variables.

Default
N/A

Usage Guidelines
This command is also used when downloading or uploading the configuration. The certificate information stored in the uploaded configuration file should not be modified, because it is signed using the issuer’s private key.

The certificate and private key file should be in PEM format and generated using RSA as the cryptography algorithm.

Example
The following command obtains the pre-generated certificate from the user:

configure ssl certificate pregenerated

Next, the user will open the certificate and then file, copy, and paste the certificate into the console/telnet session, followed by a “.” (period) to end the command.

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available in all platforms that use the SSH image except for the Summit “i” platform switches that use the SSH Base image.
configure ssl certificate privkeylen country organization common-name

configure ssl certificate privkeylen <length> country <code> organization <org_name> common-name <name>

**Description**

Creates a self-signed certificate and private key that can be saved in NVRAM.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>length</td>
<td>Specifies the private key length in bytes. Valid values are between 1024 and 4096.</td>
</tr>
<tr>
<td>code</td>
<td>Specifies the country code in 2-character format. For a list of supported country codes, see “configure wireless country-code” on page 1262.</td>
</tr>
<tr>
<td>org_name</td>
<td>Specifies the organization name. The org_name can be up to 64 characters long.</td>
</tr>
<tr>
<td>name</td>
<td>Specifies the common name. The common name can be up to 64 characters long.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Creates a self signed certificate and private key that can be saved in NVRAM. The certificate generated is in X509v3 format. The certificate generated is in PEM format.

Any existing certificate and private key is overwritten.

Most web browsers check whether the common-name field in the received server certificate is the same as the URL used to reach the site, otherwise they give a warning.

The size of the certificate generated depends on the RSA key length (privkeylen) and the length of the other parameters (country, organization name, and so forth) supplied by the user. If the RSA key length is 1024, the certificate size is ~1kb and the private key length is ~1kb. For RSA Key length of 4096, the certificate length is ~2kb and the private key length is ~3kb.

**Example**

The following command creates an SSL certificate in the USA for a website called bigcats:

```
configure ssl certificate privkeylen 2048 country US organization IEEE common-name bigcats
```

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.
Platform Availability

This command is available in all platforms that use the SSH image except for the Summit “i” platform switches that use the SSH Base image.
configure ssl privkey pregenerated

Description
Obtains the pre-generated private key from the user.

NOTE
This command is available only for the Alpine 3800 and Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
N/A

Usage Guidelines
This command is also used when downloading or uploading the configuration. Because the private key is stored in the uploaded configuration file in an encrypted format using a hard-coded passphrase, you should not modify the private key information in the configuration file.

The certificate and private key file should be in PEM format and generated using RSA as the cryptography algorithm.

Example
The following command obtains the pre-generated private key from the user:

configure ssl privkey pregenerated

Next, the user will open the certificate and then file, copy, and paste the certificate into the console/telnet session, followed by a “.” (period) to end the command.

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

Platform Availability
This command is available in all platforms that use the SSH image except for the Summit “i” platform switches that use the SSH Base image.
configure tacacs server

For the “i” switches:

    configure tacacs [primary | secondary] server [<ipaddress> | <hostname>] 
        {<L4 port no>} client-ip <ipaddress>

For the “e” switches:

    configure tacacs [primary | secondary] server [<ipaddress> | <hostname>] 
        {<L4 port no>} client-ip [<ipaddress>]

Description
Configures the server information for a TACACS+ authentication server.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary TACACS+ server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary TACACS+ server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the TACACS+ server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the TACACS+ server being configured. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>L4 port no</td>
<td>Specifies the L4 port used to contact the TACACS+ server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address used by the switch to identify itself when communicating with the TACACS+ server.</td>
</tr>
</tbody>
</table>

Default
TACACS+ uses TCP port 49.

Usage Guidelines
Configure the server information for a TACACS+ server.

To remove a server, use the following command:

    unconfigure tacacs

Use of the hostname parameter requires that DNS be enabled.

Example
The following command configures server tacacs1 as the primary TACACS+ server for client switch 10.10.20.35:

    configure tacacs primary server tacacs1 client-ip 10.10.20.35

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
configure tacacs server timeout

configure tacacs [primary | secondary] server <ipaddress> timeout <seconds>

Description
Configures the timeout interval for TACAS+ authentication requests for the primary and secondary servers.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the primary or secondary server.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds for authentication requests. Range is 3 to 120 seconds</td>
</tr>
</tbody>
</table>

Default
The default is 3 seconds.

Usage Guidelines
This command configures the timeout interval for TACACS+ authentication requests. When the timeout has expired, another authentication attempt will be made to the next alternative authentication method.

Example
The following command configures the timeout interval for TACACS+ authentication to 10 seconds:

configure tacacs primary server 192.168.14.8 timeout 10

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms only.
configure tacacs shared-secret

    configure tacacs [primary | secondary] shared-secret {encrypted} <string>

Description
Configures the shared secret string used to communicate with the TACACS+ authentication server.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the authentication string for the primary TACACS+ server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the authentication string for the secondary TACACS+ server.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Indicates that the secret should be encrypted.</td>
</tr>
<tr>
<td>string</td>
<td>Specifies the string to be used for authentication.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

The secret must be the same between the client switch and the TACACS+ server.

The TACACS+ server must first be configured for use with the switch as a RADIUS client.

If the server address is not specified, shared secret is configured for all primary and secondary TACACS+ authentication servers.

You must first configure the TACACS+ server information before configuring the shared secret for a specific server.

Example

The following command configures the shared secret as “purplegreen” on the primary TACACS+ server:

    configure tacacs-accounting primary shared-secret purplegreen

History

This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
configure tacacs timeout

    configure tacacs [primary | secondary] {server <ipaddress> | <hostname)}> timeout <seconds>

Description
Configures the timeout interval for TACAS+ authentication requests.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the timeout for the primary TACACS+ server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the timeout for the secondary TACACS+ server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the TACACS+ server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the TACACS+ server being configured.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds for authentication requests. Range is 3 to 120 seconds</td>
</tr>
</tbody>
</table>

Default
The default is 3 seconds.

Usage Guidelines
This command configures the timeout interval for TACACS+ authentication requests. When the timeout has expired, another authentication attempt will be made to the next alternative authentication method.

Examples
The following command (for “i” platforms) configures the timeout interval for TACACS+ authentication to 10 seconds:

    configure tacacs timeout 10

The following command (for “e” platforms) configures the timeout interval for the secondary TACACS+ authentication to 10 seconds:

    configure tacacs secondary timeout 10

The following command (for “e” platforms) configures the timeout interval for TACACS+ authentication to 10 seconds:

    configure tacacs primary server 192.168.14.8 timeout 10

History
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2.e.

Platform Availability
This command is available on all platforms.
configure tacacs-accounting server

configure tacacs-accounting [primary | secondary] server [<ipaddress> | <hostname>] {<tcp_port>} client-ip <ipaddress>

Description
Configures the primary and secondary TACACS+ accounting servers.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the primary TACACS+ accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the secondary TACACS+ accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the TACACS+ server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the TACACS+ server being configured. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>tcp_port</td>
<td>Specifies the TCP port to use to contact the TACACS+ server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>The IP address used by the switch to identify itself when communicating with the TACACS+ accounting server.</td>
</tr>
</tbody>
</table>

Default
Unconfigured

Usage Guidelines
You can use the same TACACS+ server for accounting and authentication.

Use this command to specify the TACACS+ accounting server information for up to two primary and two secondary TACACS+ accounting servers.

Use of the hostname parameter requires that DNS be enabled.

To remove a server, use the following command:

unconfigure tacacs

Example
The following command configures server tacacs1 as the primary TACACS+ accounting server for client switch 10.10.20.35:

configure tacacs-accounting primary server tacacs1 client-ip 10.10.20.35

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure tacacs-accounting shared-secret

configure tacacs-accounting [primary | secondary] shared-secret {encrypted} <string>

Description
Configures the shared secret string used to communicate with the TACACS+ accounting server.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the authentication string for the primary TACACS+ accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the authentication string for the secondary TACACS+ accounting server.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Indicates that the secret should be encrypted.</td>
</tr>
<tr>
<td>string</td>
<td>The string to be used for authentication.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The secret must be the same between the client switch and the TACACS+ accounting server.

If the server address is not specified, shared secret is configured for all primary and secondary TACACS+ accounting servers.

You must first configure the TACACS+ accounting server information before configuring the shared secret for a specific server.

Example
The following command configures the shared secret as “tacacsaccount” on the primary TACACS+ accounting server:

configure tacacs-accounting primary shared-secret tacacsaccount

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure tacacs-accounting timeout

configure tacacs-accounting {{primary | secondary} {server [<ipaddress>] | <hostname>}} timeout <seconds>

Description
Configures the timeout interval for TACACS+ accounting authentication requests.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Configures the timeout for the primary TACACS+ accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Configures the timeout for the secondary TACACS+ accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the TACACS+ server being configured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the TACACS+ server being configured.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds to wait before retrying accounting requests.</td>
</tr>
<tr>
<td></td>
<td>Range is 3 to 120 seconds.</td>
</tr>
</tbody>
</table>

Default
The default is 3 seconds.

Usage Guidelines
This command configures the timeout interval for TACACS+ accounting authentication requests. When the timeout has expired, another authentication attempt is made to the next alternative TACACS+ accounting server.

Examples
On an “i” series switch, the following command configures the timeout interval for TACACS+ accounting authentication to 10 seconds:

```
configure tacacs-accounting timeout 10
```

On an “e” series switch, the following command configures the timeout interval for TACACS+ accounting authentication to 10 seconds:

```
configure tacacs-accounting primary server 192.168.12.12 timeout 10
```

History
This command was first available in ExtremeWare 7.0.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure vlan access-profile

configure vlan <vlan name> access-profile [<access profile> | none]

Description
Configures a BlackDiamond 6800 series switch running ExtremeWare 4.1 to control the routing of traffic between VLANs.

NOTE
This command is available only on the BlackDiamond 6800 series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of an egress VLAN.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile that contains a list of ingress VLANs.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no access profile should be associated with this VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command configures a BlackDiamond 6800 series switch to permit or deny the routing of IP traffic from the specified list of ingress VLANs to the specified egress VLAN. If the access profile uses permit mode, only traffic from the VLANs specified in the access profile will be routed to egress VLANs configured to use that access profile.

The VLAN must already exist. The access profile must be of type VLAN (supported only in ExtremeWare releases 4.0 and earlier).

Example
Given an access profile created and configured as follows:

```
create access-profile okprofile vlan
configure access-profile okprofile mode permit
configure access-profile okprofile add vlan exec
```

The following command permits traffic from VLAN `exec` to be routed to VLAN `vlan1`:

```
configure vlan vlan1 access-profile okprofile
```

History
This command was available in ExtremeWare 4.1.

Support for this command was discontinued in ExtremeWare 6.0.
Platform Availability

This command is available on the BlackDiamond 6800 MSM32 only.
configure vlan dhcp-address-range

configure vlan <vlan-name> dhcp-address-range <start-addr> - <end-addr> {<mask>}

**Description**

Configures a set of DHCP addresses for a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be configured.</td>
</tr>
<tr>
<td>start-addr</td>
<td>Specifies the starting IP address in the configured range.</td>
</tr>
<tr>
<td>end-addr</td>
<td>Specifies the ending IP address in the configured range.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies the network mask of the range if the range specifies a remote subnet.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command configures in the switch a set of DHCP addresses for a particular VLAN. The configured address range can be for a local subnet (the range falls in one of the local subnets of the switch) or a remote subnet (the configured IP address does not fall in any of the local subnets of the switch).

To configure address ranges for a remote subnet the optional parameter `mask` must be included.

To configure address ranges for a local subnet the parameter `mask` should not be used.

You can configure a maximum of 64 local and remote address ranges.

**Example**

You can allocate IP addresses for a remote subnet (non-local subnet) using the DHCP server. The following command configures DHCP address ranges for a remote subnet using the subnet 60.0.0.x/24 in the VLAN named test:

```
configure vlan test dhcp-address-range 60.0.0.5 - 60.0.0.40 mask 255.255.255.0
```

**NOTE**

*The mask option is required when configuring the DHCP address range for the remote subnet.*

**History**

This command was first made available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

This command was modified in ExtremeWare 7.3.0 and ExtremeWare 7.3e to allow remote subnets to be configured in ExtremeWare.
Platform Availability

This command is available on all platforms.
configure vlan dhcp-lease-timer

    configure vlan <name> dhcp-lease-timer <lease-timer>

**Description**

Configures the timer value in seconds returned as part of the DHCP response.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the VLAN on whose ports netlogin should be disabled.</td>
</tr>
<tr>
<td>lease-timer</td>
<td>Specifies the timer value, in seconds.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

The timer value is specified in seconds.

The DHCP server should be used with network login and not as a stand-alone DHCP server.

**Example**

The following command configures the DHCP lease timer value for VLAN corp:

```
configure vlan corp dhcp-lease-timer <lease-timer>
```

**History**

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure vlan dhcp-options

configure vlan <vlan-name> dhcp-options [dhcp-gateway <gateway-addr> | dns-server <dns-server-ip> | wins-server <wins-server-ip>] {<start-addr>}

Description
Configures the DHCP options returned as part of the DHCP response by a switch configured as a DHCP server.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be configured.</td>
</tr>
<tr>
<td>dhcp-options</td>
<td>Specifies that DHCP options are to be configured.</td>
</tr>
<tr>
<td>dhcp-gateway</td>
<td>Specifies that the DHCP gateway option is to be configured.</td>
</tr>
<tr>
<td>gateway-addr</td>
<td>Specifies the DHCP gateway address.</td>
</tr>
<tr>
<td>dns-server</td>
<td>Specifies that the DNS server option is to be configured.</td>
</tr>
<tr>
<td>dns-server-ip</td>
<td>Specifies the DNS server IP address.</td>
</tr>
<tr>
<td>wins-server</td>
<td>Specifies that the WINS server option is to be configured.</td>
</tr>
<tr>
<td>wins-server-ip</td>
<td>Specifies the WINS server IP address.</td>
</tr>
<tr>
<td>start-addr</td>
<td>(Optional) Specifies the starting address of the range for which DHCP options are to be configured.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use the dhcp-gateway keyword to configure the DHCP gateway option for a specified DHCP address range.

Use the dns-server keyword to configure the DNS server option for a specified DHCP address range.

Use the wins-server keyword to configure the WINS server option for a given DHCP address range.

A VLAN can have multiple DHCP address ranges; therefore, the parameter start-addr identifies the DHCP address range for which this configuration is applicable.

The DHCP address range is identified as the one whose starting IP address is the same as start-addr. If start-addr is not provided, then the DHCP option will be applied for the primary DHCP address range.

To clear DHCP options for a VLAN, use the following command:
unconfigure vlan dhcp-options

Example 1
Consider a VLAN named test with a primary subnet 40.0.0.x/24 and a secondary subnet 50.0.0.x/24. Assume that for the primary subnet a DHCP address range is configured ranging from 40.0.0.5 to
40.0.0.40. Similarly, for the secondary subnet the DHCP address range is configured ranging from 50.0.0.5 to 50.0.0.40.

To configure the DHCP gateway as 40.0.0.90 for the primary subnet, use the following command:
```
configure vlan test dhcp-options dhcp-gateway 40.0.0.90
```

To configure the DHCP gateway as 50.0.0.90 for the secondary subnet use the following command:
```
configure vlan test dhcp-options dhcp-gateway 50.0.0.90 50.0.0.5
```

**NOTE**

You can configure multiple DHCP address ranges for a VLAN. The start-addr option in the command (50.0.0.5 in this example) specifies the exact DHCP address range for which the command applies. If the last option is not specified, the command is applied for the primary subnet.

**Example 2**

Consider a VLAN named test with a primary subnet 40.0.0.x/24 and a secondary subnet 50.0.0.x/24. Assume that for the primary subnet a DHCP address range is configured ranging from 40.0.0.5 to 40.0.0.40. Similarly, for the secondary subnet the DHCP address range is configured ranging from 50.0.0.5 to 50.0.0.40.

To configure the DNS server as 40.0.0.90 for the primary subnet, use the following command:
```
configure vlan test dhcp-options dns-server 40.0.0.90
```

To configure the DNS Server as 50.0.0.90 for the secondary subnet, use the following command:
```
configure vlan test dhcp-options dns-server 50.0.0.90 50.0.0.5
```

**NOTE**

You can configure multiple DHCP address ranges for a VLAN. The start-addr option in the command (50.0.0.5 in this example) specifies the exact DHCP address range for which the command applies. If the last option is not specified, the command is applied for the primary subnet.

**Example 3**

Consider a VLAN named test with a primary subnet 40.0.0.x/24 and a secondary subnet 50.0.0.x/24. Assume that for the primary subnet a DHCP address range is configured ranging from 40.0.0.5 to 40.0.0.40. Similarly, for the secondary subnet the DHCP address range is configured ranging from 50.0.0.5 to 50.0.0.40.

To configure the WINS Server as 40.0.0.90 for the primary subnet, use the following command:
```
configure vlan test dhcp-options wins-server 40.0.0.90
```

To configure the WINS Server as 50.0.0.90 for the secondary subnet, use the following command:
```
configure vlan test dhcp-options wins-server 50.0.0.90 50.0.0.5
```

**NOTE**

You can configure multiple DHCP address ranges for a VLAN. The start-addr option in the command (50.0.0.5 in this example) specifies the exact DHCP address range for which the command applies. If the last option is not specified, the command is applied for the primary subnet.
History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified so that remote or secondary subnets could be configured for DHCP options in ExtremeWare (through the addition of the parameter start-addr). This enhanced command was made available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan netlogin-lease-timer

configure vlan <vlan name> netlogin-lease-timer <seconds>

Description
Configures the timer value returned as part of the DHCP response for clients attached to
network login-enabled ports.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN to which this timer value applies.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the timer value, in seconds.</td>
</tr>
</tbody>
</table>

Default
10 seconds

Usage Guidelines
The timer value is specified in seconds.

This command applies only to the web-based authentication mode of network login.

Example
The following command sets the timer value to 15 seconds for VLAN corp:

configure vlan corp netlogin-lease-timer 15

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e

Platform Availability
This command is available on all platforms.
create access-list

create access-list <name> access-mask <access-mask name> {dest-mac <dest_mac} {source-mac <src_mac>} {vlan <name>} {ethertype [IP | ARP | <hex_value>]} {tos <ip_precedence> | code-point <code_point>} {ipproto

to protocol [tcp | udp | icmp | igmp | <prococol_num>]}} {dest-ip <dest_IP>/<mask

to length>} {dest-L4port <dest_port>} {source-ip <src_IP>/<mask length>} 

{source-L4port <src_port}> [permit (qosprofile <qosprofile>) {set code-point <code_point>} [set dot1p <dot1p_value} | permit-established | deny]{vlan-pri}{vlan-pri-2bits}

Description

Creates an access list on an “e” series switch.

NOTE

This command is available only on the “e” series switches. To create access lists for “i” series switches, use the following four commands:

create access-list icmp destination source
create access-list ip destination source ports
create access-list tcp destination source ports
create access-list udp destination source ports

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the access list.</td>
</tr>
<tr>
<td>access-mask</td>
<td>Specifies the name of the associated access mask.</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Specifies the destination MAC address.</td>
</tr>
<tr>
<td>source-mac</td>
<td>Specifies the source MAC address.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies the VLANid.</td>
</tr>
<tr>
<td>ethertype</td>
<td>Specifies the Ethernet type field.</td>
</tr>
<tr>
<td>tos</td>
<td>Specifies a 3-bit precedence field within the IP ToS field. Valid entries are from 0 to 7.</td>
</tr>
<tr>
<td>code-point</td>
<td>Specifies a 6-bit DiffServ code point. Valid entries are from 0 to 63.</td>
</tr>
<tr>
<td>ipproto</td>
<td>Specifies the IP protocol.</td>
</tr>
<tr>
<td>dest-ip</td>
<td>Specifies the destination IP address.</td>
</tr>
<tr>
<td>source-ip</td>
<td>Specifies the source IP address.</td>
</tr>
<tr>
<td>dest-L4port</td>
<td>Specifies the destination TCP/UDP port.</td>
</tr>
<tr>
<td>source-L4port</td>
<td>Specifies the source TCP/UDP port.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>Specifies the ICMP type.</td>
</tr>
<tr>
<td>icmp-code</td>
<td>Specifies the ICMP code.</td>
</tr>
<tr>
<td>egressport</td>
<td>Specifies the egress port.</td>
</tr>
<tr>
<td>ports</td>
<td>Specifies one or more ingress ports.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies to forward the packet.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies the priorities for using QoS profiles.</td>
</tr>
</tbody>
</table>
Security Commands

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>code-point</td>
<td>Specifies a 6-bit DiffServ code point. Valid entries are from 0 to 63.</td>
</tr>
<tr>
<td>dot1p</td>
<td>Specifies the priorities for 802.1p.</td>
</tr>
<tr>
<td>permit-established</td>
<td>Specifies to deny any new TCP session initiation.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies to drop the packet.</td>
</tr>
<tr>
<td>vlan-pri</td>
<td>Specifies the 802.1p priority of the VLAN tag, which is a three-bit field.</td>
</tr>
<tr>
<td>vlan-pri-2bits</td>
<td>Specifies the two most significant bits of the vlan-pri field.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

None

Example

The following access-list example performs packet filtering in the following sequence, as determined by the precedence number:

- Deny UDP port 32 and TCP port 23 traffic to the 10.2.XX network.
- All other TCP port 23 traffic destined for other 10.X.X.X networks is permitted using QoS profile Qp4.
- All remaining traffic to 10.2.0.0 uses QoS profile Qp3.

With no default rule specified, all remaining traffic is allowed using the default QoS profile.

```
create access-list deny102_32 udp dest 10.2.0.0/16 ip-port 32 source any ip-port any
deny ports any precedence 10

create access-list deny102_23 tcp dest 10.2.0.0/16 ip-port 23 source any ip-port any
deny ports any precedence 20

create access-list allow10_23 tcp dest 10.0.0.0/8 ip-port 23 source any ip-port any
permit qosprofile qp4 ports any precedence 30

create access-list allow102 ip dest 10.2.0.0/16 source 0.0.0.0/0 permit qosprofile qp3
ports any precedence 40
```

The following example shows a default entry that is used to specify an explicit deny:

```
create access-list denyall ip dest 0.0.0.0/0 source 0.0.0.0/0 deny ports any
```

History

This form of the command was available in ExtremeWare 7.1e.

Platform Availability

This command is available on the “e” series platforms only.
create access-list icmp destination source

create access-list <name> icmp destination [dest_ipaddress]/<mask> | any] source [src_ipaddress]/<source_mask> | any] type <icmp_type> code <icmp_code> [permit | deny] {<portlist>} {precedence <number>}

Description

Creates a named IP access list that applies to ICMP traffic.

NOTE

This command is available only on the “i” series switches. To create an access list for an “e” series switch, use the create access-list command.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the access list name. The access list name can be between 1 and 31 characters.</td>
</tr>
<tr>
<td>dest_ipaddress/mask</td>
<td>Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry. any specifies that any address will match.</td>
</tr>
<tr>
<td>src_ipaddress/source_mask</td>
<td>Specifies a source IP address and subnet mask. any specifies that any address will match.</td>
</tr>
<tr>
<td>icmp_type</td>
<td>Specifies the ICMP_TYPE number. The ICMP type is a number from 0 to 255.</td>
</tr>
<tr>
<td>icmp_code</td>
<td>Specifies the ICMP_CODE number. The ICMP code is a number from 0 to 255.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies that packets that match the access list description are permitted to be forward by this switch.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies that packets that match the access list description are filtered (dropped) by the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ingress port(s) on which this rule is applied.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the access list precedence number. The range is 1 to 25,600.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

The access list is applied to all ICMP ingress packets.

Example

This command creates an access list named denyping that filters out ping (ICMP echo) packets. ICMP echo packets are defined as type 8 code 0:

create access-list denyping icmp destination any source any type 8 code 0 deny ports any
Security Commands

History
This command was first available in ExtremeWare 6.0, and replaced the configure ipqos command.

Platform Availability
This command is available on the “i” series platforms only.
create access-list ip destination source ports

create access-list <name> ip destination [<dest_ipaddress>/<mask> | any] source [<src_ipaddress>/<src_mask> | any] [permit {<qosprofile>} | deny] ports [<portlist> | any] {precedence <prec_number>}

Description
Creates a named IP access list that applies to all IP traffic.

NOTE
This command is available only on the “i” series switches. To create an access list for an “e” series switch, use the create access-list command.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the access list name. The access list name can be between 1 and 31 characters.</td>
</tr>
<tr>
<td>dest_ipaddress/mask</td>
<td>Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.</td>
</tr>
<tr>
<td>any</td>
<td>specifies that any address will match.</td>
</tr>
<tr>
<td>src_ipaddress/src_mask</td>
<td>Specifies a source IP address and subnet mask.</td>
</tr>
<tr>
<td>any</td>
<td>specifies that any address will match.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies that packets that match the access list description are permitted to be forwarded by the switch.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies an optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies that packets that match the access list description are filtered (dropped) by the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ingress port(s) on which this rule is applied.</td>
</tr>
<tr>
<td>any</td>
<td>specifies that the rule will be applied to all ports.</td>
</tr>
<tr>
<td>prec_number</td>
<td>Specifies the access list precedence number. The range is 1 to 25,600.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The access list is applied to all ingress packets.

Examples
The following example defines an access list entry allow102 with precedence 40 that permits all traffic on any ingress ports to the 10.2.x.x subnet, and assigns QoS profile Qp3 to those packets:

```
create access-list allow102 ip dest 10.2.0.0/16 source 0.0.0.0/0 permit qosprofile qp3 ports any precedence 40
```
The following command defines a default entry that is used to specify an explicit deny:
create access-list denyall ip dest 0.0.0.0/0 source 0.0.0.0/0 deny ports any

**History**
This command was first available in ExtremeWare 6.0, and replaced the configure ipqos command.

**Platform Availability**
This command is available on the “i” series platforms only.
create access-list tcp destination source ports

create access-list <name> tcp destination [dest_ipaddress/mask | any] ip-port [dst_port | range dst_port_min dst_port_max | any] source [src_ipaddress/src_mask | any] ip-port [src_port | range src_port_min src_port_max | any] [permit qosprofile | permit-established | deny] ports [portlist | any] {precedence prec_number}

Description

Creates a named IP access list that applies to TCP traffic.

NOTE

This command is available only on the “i” series switches. To create an access list for an “e” series switch, use the create access-list command.

Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the access list name. The access list name can be between 1 and 31 characters.</td>
</tr>
<tr>
<td>dest_ipaddress/mask</td>
<td>Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that any address will match.</td>
</tr>
<tr>
<td>dst_port</td>
<td>Specifies a TCP layer 4 port.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that all TCP ports will match.</td>
</tr>
<tr>
<td>dst_port_min</td>
<td>Specifies the beginning of a TCP layer 4 port range.</td>
</tr>
<tr>
<td>dst_port_max</td>
<td>Specifies the end of a TCP layer 4 port range.</td>
</tr>
<tr>
<td>src_ipaddress/src_mask</td>
<td>Specifies a source IP address and subnet mask.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that any address will match.</td>
</tr>
<tr>
<td>src_port</td>
<td>Specifies a TCP layer 4 port.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that all TCP ports will match.</td>
</tr>
<tr>
<td>src_port_min</td>
<td>Specifies the beginning of a TCP layer 4 port range.</td>
</tr>
<tr>
<td>src_port_max</td>
<td>Specifies the end of a TCP layer 4 port range.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies that packets that match the access list description are permitted to be forwarded by this switch.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies an optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.</td>
</tr>
<tr>
<td>permit-established</td>
<td>Specifies that a currently-established TCP session is allowed, but TCP packets from source to destination (uni-directional) with SYN=1 and ACK=0 (to initiate a new session) will be dropped.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies that packets that match the access list description are filtered (dropped) by the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ingress port(s) on which this rule is applied.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies that the rule will be applied to all ports.</td>
</tr>
<tr>
<td>prec_number</td>
<td>Specifies the access list precedence number. The range is 1 to 25,600.</td>
</tr>
</tbody>
</table>
Default
N/A

Usage Guidelines
The access list is applied to all ingress packets.

Example
The following command defines an access-list rule named allow10_23 with precedence 30 that permits TCP port 23 traffic destined for other 10.x.x.x networks, and assigns QoS profile Qp4:
create access-list allow10_23 tcp dest 10.0.0.0/8 ip-port 23 source any ip-port any permit qosprofile qp4 ports any precedence 30

History
This command was first available in ExtremeWare 6.0, and replaced the configure ipqos command.

Platform Availability
This command is available on the “i” series platforms only.
create access-list udp destination source ports

create access-list <name> udp destination [<dest_ipaddress>/<mask> | any] ip-port [<dst_port> | range <dst_port_min> <dst_port_max> | any] source [<src_ipaddress>/<src_mask> | any] ip-port [<src_port> | range <src_port_min> <src_port_max> | any] [permit <qosprofile> | deny] ports [<portlist> | any] {precedence <prec_number>}

Description

Creates a named IP access list that applies to UDP traffic.

NOTE

This command is available only on the “i” series switches. To create an access list for an “e” series switch, use the create access-list command.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the access list name. The access list name can be between 1 and 31 characters.</td>
</tr>
<tr>
<td>dest_ipaddress/mask</td>
<td>Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry. any specifies that any address will match.</td>
</tr>
<tr>
<td>dst_port</td>
<td>Specifies a UDP layer 4 port. any specifies that all UDP ports will match.</td>
</tr>
<tr>
<td>dst_port_min</td>
<td>Specifies the beginning of a UDP layer 4 port range.</td>
</tr>
<tr>
<td>dst_port_max</td>
<td>Specifies the end of a UDP layer 4 port range.</td>
</tr>
<tr>
<td>src_ipaddress/src_mask</td>
<td>Specifies a source IP address and subnet mask. any specifies that any address will match.</td>
</tr>
<tr>
<td>src_port</td>
<td>Specifies a UDP layer 4 port. any specifies that all UDP ports will match.</td>
</tr>
<tr>
<td>src_port_min</td>
<td>Specifies the beginning of a UDP layer 4 port range.</td>
</tr>
<tr>
<td>src_port_max</td>
<td>Specifies the end of a UDP layer 4 port range.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies that packets that match the access list description are permitted to be forward by this switch.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies an optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.</td>
</tr>
<tr>
<td>deny</td>
<td>Specifies that packets that match the access list description are filtered (dropped) by the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ingress port(s) on which this rule is applied. any specifies that the rule will be applied to all ports.</td>
</tr>
<tr>
<td>prec_number</td>
<td>Specifies the access list precedence number. The range is 1 to 25,600.</td>
</tr>
</tbody>
</table>

Default

N/A
Usage Guidelines
The access list is applied to all ingress packets.

Example
The following command defines an access-list rule named allow10_35 with precedence 70 that permits udp port 35 traffic destined for other 10.X.X.X networks, and assigns QoS profile Qp2:

create access-list allow10_35 udp dest 10.0.0.0/8 ip-port 35 source any ip-port any permit qosprofile qp2 ports any precedence 70

History
This command was first available in ExtremeWare 6.0, and replaced the configure ipqos command.

Platform Availability
This command is available on the “i” series platforms only.
create access-mask

create access-mask <access-mask name> {dest-mac} {source-mac} {vlan} {tos |code-point} {ethertype} {ipprotocol} {dest-ip/<mask length>} {source-L4port | {icmp-type} {icmp-code}} {permit-established} {egressport} {ports} {precedence <number>} {vlan-pri} {vlan-pri-2bits}

**Description**

Creates an access mask.

**NOTE**

*This command is available only on the “e” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access mask name</td>
<td>Specifies the name of the access-mask.</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Specifies the destination MAC address.</td>
</tr>
<tr>
<td>source-mac</td>
<td>Specifies the source MAC address.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies the VLANid.</td>
</tr>
<tr>
<td>tos</td>
<td>Specifies a 3-bit precedence field within the IP ToS field. Valid entries are from 0 to 7.</td>
</tr>
<tr>
<td>code-point</td>
<td>Specifies a 6-bit DiffServ code point. Valid entries are from 0 to 63.</td>
</tr>
<tr>
<td>ethertype</td>
<td>Specifies the Ethernet type field.</td>
</tr>
<tr>
<td>ipprotocol</td>
<td>Specifies the IP protocol.</td>
</tr>
<tr>
<td>dest-ip</td>
<td>Specifies the destination IP address.</td>
</tr>
<tr>
<td>source-ip</td>
<td>Specifies the source IP address.</td>
</tr>
<tr>
<td>mask length</td>
<td>Specifies the IP mask length.</td>
</tr>
<tr>
<td>dest-L4port</td>
<td>Specifies the destination TCP/UDP port.</td>
</tr>
<tr>
<td>source-L4port</td>
<td>Specifies the source TCP/UDP port.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>Specifies the ICMP type.</td>
</tr>
<tr>
<td>icmp-code</td>
<td>Specifies the ICMP code.</td>
</tr>
<tr>
<td>permit-established</td>
<td>Specifies the TCP SYN and ACK bits. It is specified when IP protocol is implicit and need not be specified separately.</td>
</tr>
<tr>
<td>egressport</td>
<td>Specifies the egress port.</td>
</tr>
<tr>
<td>ports</td>
<td>Specifies one or more ingress ports.</td>
</tr>
<tr>
<td>precedence</td>
<td>Specifies the access-mask precedence, which determines the precedence of the associated access list.</td>
</tr>
<tr>
<td>vlan-pri</td>
<td>Specifies the 802.1p priority of the VLAN tag, which is a three-bit field. Valid values are 0 to 7.</td>
</tr>
<tr>
<td>vlan-pri-2bits</td>
<td>Specifies the two most significant bits of the vlan-pri field.</td>
</tr>
<tr>
<td>bgp-community</td>
<td>Specifies that the profile entries will be a list of BGP community numbers. Not supported on the Summit 400 switch.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies that the profile entries will be a list of VLANs</td>
</tr>
</tbody>
</table>
Security Commands

Default
N/A

Usage Guidelines
None

Example

The following commands create the access mask and access lists:

create access-mask ipproto_mask ipprotocol ports precedence 25000
create access-list denytcp ipproto_mask ipprotocol tcp ports 2,10 deny
create access-list denyudp ipproto_mask ipprotocol udp ports 2,10 deny

History

This form of the command was available in ExtremeWare 7.1e.

Platform Availability

This command is available on the “e” series platforms only.
create access-profile type

For the “i” series switches:

create access-profile <access profile> type [ipaddress | ipx-node | ipx-net | ipx-sap | as-path | bgp-community | vlan]

For the “e” series switches:

create access-profile <access profile> type [ipaddress | as-path]

Description

Creates an access profile.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies that the profile entries will be a list of IP address/mask pairs.</td>
</tr>
<tr>
<td>ipx-node</td>
<td>Specifies that the profile entries will be a list of IPX node addresses.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “e” series switches.</td>
</tr>
<tr>
<td>ipx-net</td>
<td>Specifies that the profile entries will be a list of IPX NetIDs.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “e” series switches.</td>
</tr>
<tr>
<td>ipx-sap</td>
<td>Specifies that the profile entries will be a list of IPX SAP advertisements.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “e” series switches.</td>
</tr>
<tr>
<td>as-path</td>
<td>Specifies that the profile entries will be a list of AS path expressions.</td>
</tr>
<tr>
<td>bgp-community</td>
<td>Specifies that the profile entries will be a list of BGP community numbers.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies that the profile entries will be a list of VLANs.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the BlackDiamond 6800 MSM32 running</td>
</tr>
<tr>
<td></td>
<td>ExtremeWare 4.1.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

You must give the access profile a unique name, in the same manner as naming a VLAN, protocol filter, or spanning tree domain.

After the access profile is created, you must configure the access profile mode. The access profile mode determines whether the items in the list are to be permitted access or denied access.

For version 4.0 (not on the Summit 400 switch):

- Only type ipaddress was supported, and the type keyword was not used.
- On BlackDiamond 6800 MSM32 running ExtremeWare 4.1, the VLAN keyword specifies that profile entries will be a list of VLANs.
Examples

The following command creates an access profile named *nosales* that will contain IP address/mask pairs:

```
create access-profile nosales type ipaddress
```

The following command creates an access profile that will contain AS path expressions:

```
create access-profile AS1 type as-path
```

History

A limited version of this command was first available in ExtremeWare 4.0.

This form of the command was available in ExtremeWare 6.1. Support for the IPX node, NetID and SAP advertisement types was added in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
create rate-limit

create rate-limit <rule_name> access-mask <access-mask name> {dest-mac <dest_mac> {source-mac <scr_mac>}} {vlan <name>} {ethertype [IP | ARP | <hex_value>]} {tos <ip_precedence> | code-point <code_point>} {ipprotocol [tcp | udp | icmp | igmp | <protocol_num>]} {dest-ip <dest_IP>/<mask length>} {dest-L4port <dest_port>} {source-ip <src_IP>/<mask length>} {source-L4port <src_port>} {permit {qosprofile <qosprofile>}} {set code-point <code_point>} {set dot1p <dot1p_value} limit <rate_in_Mbps> {exceed-action [drop | set code-point <code_point>]} {vlan-pri}{vlan-pri-2bits}

Description

Creates a rate limit rule.

NOTE

This command is available only on the “e” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rule_name</td>
<td>Specifies the name of the rate limit rule.</td>
</tr>
<tr>
<td>access-mask</td>
<td>Specifies the name of the associated access mask.</td>
</tr>
<tr>
<td>dest-mac</td>
<td>Specifies the destination MAC address.</td>
</tr>
<tr>
<td>source-mac</td>
<td>Specifies the source MAC address.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies the VLANid.</td>
</tr>
<tr>
<td>ethertype</td>
<td>Specifies the Ethernet type field.</td>
</tr>
<tr>
<td>tos</td>
<td>Specifies a 3-bit precedence field within the IP ToS field. Valid entries are from 0 to 7.</td>
</tr>
<tr>
<td>code-point</td>
<td>Specifies a 6-bit DiffServ code point. Valid entries are from 0 to 63.</td>
</tr>
<tr>
<td>ipprotocol</td>
<td>Specifies the IP protocol.</td>
</tr>
<tr>
<td>dest-ip</td>
<td>Specifies the destination IP address.</td>
</tr>
<tr>
<td>source-ip</td>
<td>Specifies the source IP address.</td>
</tr>
<tr>
<td>dest-L4port</td>
<td>Specifies the destination TCP/UDP port.</td>
</tr>
<tr>
<td>source-L4port</td>
<td>Specifies the source TCP/UDP port.</td>
</tr>
<tr>
<td>icmp-type</td>
<td>Specifies the ICMP type.</td>
</tr>
<tr>
<td>icmp-code</td>
<td>Specifies the ICMP code.</td>
</tr>
<tr>
<td>egressport</td>
<td>Specifies the egress port.</td>
</tr>
<tr>
<td>ports</td>
<td>Specifies one or more ingress ports.</td>
</tr>
<tr>
<td>permit</td>
<td>Specifies to forward the packet.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies the priorities for using QoS profiles.</td>
</tr>
<tr>
<td>code-point</td>
<td>Specifies a 6-bit DiffServ code point. Valid entries are from 0 to 63.</td>
</tr>
<tr>
<td>dot1p</td>
<td>Specifies the priorities for 802.1p.</td>
</tr>
<tr>
<td>limit</td>
<td>Specifies to limit the data rate to the specified amount in Mbps.</td>
</tr>
<tr>
<td>exceed-action</td>
<td>Specifies the action to be taken on the data traffic when it exceeds the specified amount.</td>
</tr>
<tr>
<td>vlan-pri</td>
<td>Specifies the 802.1p priority of the VLAN tag, which is a three-bit field. Valid values are 0 to 7.</td>
</tr>
<tr>
<td>vlan-pri-2bits</td>
<td>Specifies the two most significant bits of thevlan-prifield.</td>
</tr>
</tbody>
</table>

**Example**

This command creates an access list named `denyping` that filters out ping (ICMP echo) packets. ICMP echo packets are defined as type 8 code 0:

```
create access-list denyping icmp destination any source any type 8 code 0 deny ports any
```

**History**

This command was first available in ExtremeWare 7.1e.

**Platform Availability**

This command is available on the “e” series platforms only.
create route-map

create route-map <name>

Description
Creates a route map statement.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies a route map name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Route maps are a mechanism that can be used to conditionally control the redistribution of routes between two routing domains, and to modify the routing information that is redistributed.

Route maps are used in conjunction with the match and set operations. A match operation specifies a criteria that must be matched. A set operation specifies a change that is made to the route when the match operation is successful.

After a route map statement has been created, you must add entries to the route map, and then add statements to the route map entries.

Example
The following command creates a route map named bgp-out:
create route-map bgp-out

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on the “i” series platforms only.
create security-profile

```
create security-profile <name> {copy <existing_profile>}
```

**Description**

Creates a new security profile.

**NOTE**

This command is available on Summit 300 and Alpine 3800 series switches only.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the security profile being created.</td>
</tr>
<tr>
<td>existing_profile</td>
<td>Specifies the name of an existing profile from which the system copies the initial values.</td>
</tr>
</tbody>
</table>

**Default**

Unsecure profile is the default, and it is applied to all wireless ports.

**Usage Guidelines**

Use this command to create a new profile or to copy an existing profile using a new name.

**Example**

The following example creates a new security-profile called `wep-secure` using an existing profile called `unsecure`:

```
create security-profile wep-secure copy unsecure
```

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

**Platform Availability**

This command is available only on Summit 300 and Alpine 3800 series switches.
create trusted-mac-address

For the "i" switches:

```text
create trusted-mac-address {mac-address} <xx:yy:zz:aa:bb:cc> {mask <dd:ee:ff:gg:hh:kk>} vlan <vlan-name | all> {port <portlist>} {protocol[DHCP|ARP]}
```

For the "e" switches:

```text
create trusted-mac-address mac-address <mac_address> [mask <mask>] vlan <vlan_name>| all [ports <portlist>] [protocol {DHCP|ARP}]
```

**Description**

Configures a trusted media access control (MAC) address with mask for each VLAN or all VLANs for the ARP or DHCP protocols.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">xx:yy:zz:aa:bb:cc</a> or mac_address</td>
<td>Specifies the MAC address for enabling the trusted-MAC feature. The format for either is xx:yy:zz:aa:bb:cc.</td>
</tr>
<tr>
<td>mask <a href="">dd:ee:ff:gg:hh:kk</a> or mask</td>
<td>Specifies the MAC address mask value. If a mask is not specified, the default mask of ff:ff:ff:ff:ff:ff is used.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be configured. If the all keyword is specified.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all VLANs are configured for trusted-MAC.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6:2:8.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Specifies DHCP for the protocol type. DHCP is the default protocol type.</td>
</tr>
<tr>
<td>ARP</td>
<td>Specifies ARP for the protocol type.</td>
</tr>
</tbody>
</table>

**Default**

Protocol type is DHCP if the protocol option is omitted.

If the port list is not specified, the trusted MAC is applied to all ports in the selected VLAN.

**Usage Guidelines**

Use this command to configure a trusted MAC address. The mask keyword is optional. If you do not specify a mask, the default mask of ff:ff:ff:ff:ff:ff is used. This command is equivalent to configuring an individual MAC address.

If you do not specify a port list, the trusted MAC is applied to all the ports in the VLAN. Devices matching a created trusted-OUI list are allowed to bypass network login using a specified protocol.

ExtremeWare performs an AND operation between the source MAC address of the incoming packet and its mask. It then compares that result with the result of the AND operation between the configured address and the mask. If the results are the same, the address is trusted and the packet is forwarded independent of the port authentication state.
Use the following command to delete a trusted MAC address:

```
delete trusted-mac-address [mac-address <mac_address> {mask <mask>} <vlan_name>] | all [ports <portlist>] [protocol [DHCP|ARP]]
```

**Example**

The following command creates a trusted MAC address of 00:e0:18:01:32:1f for all ports in the VLAN named vlan1:

```
create trusted-mac-address 00:e0:18:01:32:1f vlan1
```

The following example creates a trusted MAC address on all ports in the VLAN bldg5 allowing the use of the DHCP protocol.

```
create trusted-mac-address mac-address 00:07:40:79:58:EB bldg5 protocol dhcp
```

**History**

This command was first available in ExtremeWare 7.3.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
delete access-list

For the “i” switches:
   delete access-list [<name> | all]

For the “i” switches:
   delete access-list <name>

Description
Deletes an access list.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the access list to be deleted.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all access lists should be deleted.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This option is available only on the “I” series switches.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command deletes access list allow102:
   delete access-list allow102

History
This command was first available in ExtremeWare 6.0.
The command was modified in ExtremeWare 6.2.1 to provide the all option.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
delete access-mask

   delete access-mask <name>

Description
Deletes the named access-mask.

NOTE
This command is available only on the “e” series switches.

Syntax Description

| name | Specifies the name of the access list to be deleted. |

Usage Guidelines
None

Example
The following command disables statistics collection for access list allow102:

   delete access-list allow102

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is available only on the “e” series platforms.
delete access-profile

   delete access-profile <access profile>

Description
Deletes an access profile.

Syntax Description

| access profile | Specifies the access profile name to be deleted. |

Default
N/A

Usage Guidelines
None

Example
The following command deletes an access profile named nosales:

   delete access-profile nosales

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
delete rate-limit

    delete rate-limit <name>

Description
Deletes a rate limit rule.

NOTE
This command is available only on the “e” series switches.

Syntax Description

| name | Specifies the name of the rate limit rule. |

Usage Guidelines
None

Example
The following command deletes a rate limit rule named throttle2:

delete access-profile throttle2

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is available on the “e” series platforms only.
delete route-map

   delete route-map <route map>

Description
Deletes a route map statement from the route map.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route map</td>
<td>Specifies a route map name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command deletes a route-map named bgp-out:

delete route-map bgp-out

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on the “i” series platforms only.
delete security-profile

    delete security-profile <name>

**Description**
Deletes the named security profile.

**Syntax Description**

| name  | Specifies the name of an existing security profile to be deleted. |

**Default**
N/A

**Usage Guidelines**
Use this command to delete the named security profile. The named profile cannot be attached to any active ports before deletion.

**Example**
The following command deletes the security profile named wep_secure:

```
delete security-profile wep_secure
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e and to the “i” series in 7.3.0.

**Platform Availability**
This command is available on Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
delete trusted-mac-address

delete trusted-mac-address [mac-address <mac_address> {mask <mask>}{vlan_name}] | all [ports <portlist>] [protocol [DHCP|ARP]]

**Description**

Deletes a trusted MAC address.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="">xx:yy:zz:aa:bb:cc</a> or mac_address</td>
<td>Specifies the MAC address of the enabled trusted-MAC. Either is specified in the form xx:yy:zz:aa:bb:cc.</td>
</tr>
<tr>
<td>mask <a href="">dd:ee:ff:gg:hh:kk</a> or mask</td>
<td>Specifies a mask for the MAC address. If a mask is not specified, the default mask of ff:ff:ff:ff:ff:ff is used.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be configured.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>DHCP</td>
<td>Specifies DHCP for the protocol type. DHCP is the default protocol type.</td>
</tr>
<tr>
<td>ARP</td>
<td>Specifies ARP for the protocol type.</td>
</tr>
</tbody>
</table>

**Default**

If you do not specify the MAC address to be deleted, the trusted-mac entries for all the configured MAC addresses will be deleted.

**Usage Guidelines**

Use this command to delete a trusted MAC address. If you do not specify the MAC address to be deleted, all the MAC addresses in the VLAN are deleted.

Use the following command to create a trusted MAC address:

```
create trusted-mac-address (mac-address) <xx:yy:zz:aa:bb:cc> {mask <dd:ee:ff:gg:hh:kk>} vlan <vlan-name | all> (port <portlist>) [protocol{DHCP|ARP}]
```

**Examples**

The following command deletes a MAC address from a VLAN named corp:

```
delete trusted-mac-address mac-address 00:04:0D:23:45:C2 corp
```

**History**

This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.
Platform Availability

This command is available on all platforms.
disable access-list

disable access-list <name> [counter | log]

Description
Disables message logging or the collection of access-list statistics.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of the access list.</td>
</tr>
<tr>
<td>counter</td>
<td>Specifies that access-list statistics collection should be disabled.</td>
</tr>
<tr>
<td>log</td>
<td>Specifies that message logging to the Syslog facility for each packet that matches the access-list description should be disabled.</td>
</tr>
</tbody>
</table>

Default
Counting is on; logging is off.

Usage Guidelines
None

Example
The following command disables statistics collection for access list allow102:
disable access-list allow102 counter

History
This command was first available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
disable arp-learning

disable arp-learning

Description
Disables the ARP-learning feature on the switch.

Syntax Description
This command has no arguments or variables.

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
disable arp-learning ports

disable arp-learning ports <portlist>

**Description**
Disables the ARP-learning feature on a port or ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies the ingress port(s) on which this rule is applied.</th>
</tr>
</thead>
<tbody>
<tr>
<td>any</td>
<td>specifies that the rule will be applied to all ports.</td>
</tr>
</tbody>
</table>

**Default**
By default, ARP learning is enabled.

**Usage Guidelines**
None

**Example**
N/A

**History**
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
disable arp-learning vlan

disable arp-learning vlan <vlan name>

Description
Disables the ARP-learning feature on a specified VLAN.

Syntax Description

| vlan name | Specifies the vlan to which the rule applies. |

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
disable arp-learning vlan ports

    disable arp-learning vlan <vlan name> port <portlist>

Description
Disables the ARP-learning feature on a port in the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the vlan to which the rule applies.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports to which the rule applies.</td>
</tr>
</tbody>
</table>

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
disable cpu-dos-protect

disable cpu-dos-protect

Description
Disables denial of service protection.

Syntax Description
There are no arguments or variables for this command.

Default
The default is disabled.

Usage Guidelines
None

Example
The following command disables denial of service protection.

disable cpu-dos-protect

History
This command was first available in ExtremeWare 6.2.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable dhcp ports vlan

   disable dhcp ports <portlist> vlan <vlan name>

Description
Disables DHCP on a specified port in a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports for which DHCP should be disabled.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN on whose ports DHCP should be disabled.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The DHCP server should be used with network login and not as a stand-alone DHCP server.

Example
The following command disables DHCP for port 9 in VLAN corp:

disable dhcp ports 9 vlan corp

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable enhanced-dos-protect

disable enhanced-dos-protect {rate-limit | ipfdb} {ports [<portlist> | all]}

Description
Disables enhanced denial of service protection globally or for selected ports.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit</td>
<td>Disables software rate limiting.</td>
</tr>
<tr>
<td>ipfdb</td>
<td>Disables the IPFDB learning qualifier.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
The default is disabled.

Usage Guidelines
Use the rate-limit keyword in this command to disable the lowering of the percentage of slow path traffic being sent to the CPU. Verify the disabled status by using the show enhanced-dos-protect rate-limit command. To globally disable rate limiting, omit the ports keyword and qualifier.

Use the ipfdb keyword in this command to disable the IPFDB learning qualifier. Verify the disabled status by using the show enhanced-dos-protect ipfdb command. To globally disable the IPFDB learning qualifier, omit the ports keyword and qualifier.

Examples
The following command disables enhanced denial of service protection rate limiting for all ports.

disable enhanced-dos-protect rate-limit ports all

The following command globally disables the enhanced denial of service protection IPFDB learning qualifier.

disable enhanced-dos-protect ipfdb

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
disable ip-subnet-lookup

Description
Disables the IPDA subnet lookup feature in a switch.

Syntax Description
There are no arguments or variables for this command.

Default
The default is disabled.

Usage Guidelines
On the “i” series switches, system rebooting is needed for a new setting to be effective.
On the “e” series switches, rebooting is not required.

Example
The following command disables IPDA lookup:

disable ip-subnet-lookup

History
This command was first available in ExtremeWare 7.3.0.
This command was added to the “e” series switches in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
disable mac-lockdown-timeout ports

disable mac-lockdown-timeout ports [<portlist> | all]

Description
This command disables the MAC address lockdown timeout feature for the specified port or group of ports or for all ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*; 2:5, 2:6-2:8. |
|-----------|
| all | Specifies all ports. |

Default
By default, the MAC address lockdown timeout feature is disabled.

Usage Guidelines
If you disable the MAC lockdown timer on a port with a configured MAC address learning limit, the limit continues to apply to the port.

When you disable the MAC lockdown timer on a port, existing MAC address entries for the port will time out based on the FDB aging period.

Example
The following example disables the MAC address lockdown timeout set for ports 3, and 5.
disable mac-lockdown-timeout ports 3,5

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
disable netlogin

disable netlogin [web-based | dot1x | mac]

Description
Disables network login modes.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-based</td>
<td>Specifies web-based authentication.</td>
</tr>
<tr>
<td>dot1x</td>
<td>Specifies 802.1x authenticating.</td>
</tr>
<tr>
<td>mac</td>
<td>Specifies MAC-based RADIUS authentication.</td>
</tr>
</tbody>
</table>

Default
Web-based and 802.1x authentication are enabled by default.

MAC-based authentication is disabled by default.

Usage Guidelines
All types, any combination of types, or no type of authentication can be enabled on the same switch. To enable an authentication mode, use the following command:

enable netlogin [web-based | dot1x | mac]

This command was first introduced as disable netlogin, which disabled the initial version of network login, the web-based mode. The original command was subsequently deprecated when the 802.1x mode of network login was introduced in ExtremeWare 7.1.0. The deprecated version of the command is temporarily supported in configurations. During an upgrade, the deprecated command disable netlogin will be interpreted as:

disable netlogin web-based
disable netlogin dot1x

Example
The following command disables web-based authentication for network login:

disable netlogin web-based

The following command globally disables MAC-based RADIUS authentication for network login:

disable netlogin mac

History
This command was first available in ExtremeWare 7.0.0.
The web-based and dot1x keywords were added in ExtremeWare 7.1.0, and the initial version of the command (without the new keywords) was deprecated.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
The `mac` keyword was added in Extremeware 7.4.

**Platform Availability**

This command is available on all platforms.
disable netlogin logout-privilege

disable netlogin logout-privilege

Description
Disables the network login logout window pop-up.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
This command controls the logout window pop-up on the web-based network client. This command applies only to the web-based authentication mode of network login. When disabled, the logout window pop-up no longer opens.

Example
The following command disables the network login logout pop-up window:
disable netlogin logout-privilege

History
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable netlogin ports

disable netlogin ports <portlist> vlan <vlan name>

Description
Disables network login on a specified port in a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports for which netlogin should be disabled.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN on whose ports netlogin should be disabled.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Network login must be disabled on a port before you can delete a VLAN that contains that port.

This command applies to both the web-based and 802.1x mode of network login. To control which authentication mode is used by network login, use the following commands:

```
enable netlogin [web-based | dot1x]
disable netlogin [web-based | dot1x]
```

Example
The following command disables network login on port 9 in the VLAN called corp:

disable netlogin ports 9 vlan corp

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable netlogin ports mac

disable netlogin ports <portlist> mac

**Description**
Disables MAC-based network login on specified ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies the ports for which MAC-based network login should be disabled.</th>
</tr>
</thead>
</table>

**Default**
By default, MAC-based network login is disabled.

**Usage Guidelines**
None

**Example**
The following command disables network login on all ports:
disable netlogin ports 9 mac

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on all platforms.
disable netlogin session-refresh

disable netlogin session-refresh

Description

Disables network login session refresh.

Syntax Description

This command has no arguments or variables.

Default

Disabled

Usage Guidelines

Network login sessions can refresh themselves after a configured timeout. After the user has been logged in successfully, a logout window opens which can be used to close the connection by clicking on the LogOut link. Any abnormal closing of this window is detected on the switch and the user is logged out after a time interval as configured for session refresh. The session refresh is enabled and set to five minutes by default.

This command applies only to the web-based authentication mode of network login.

Example

The following command disables network login session refresh:

disable netlogin session-refresh

History

This command was first available in ExtremeWare 7.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
disable radius

disable radius

Description
Disables the RADIUS client.

Syntax Description
This command has no arguments or variables.

Default
RADIUS authentication is disabled by default.

Usage Guidelines
None

Example
The following command disables RADIUS authentication for the switch:

disable radius

History
This command was first available in ExtremeWare 4.1.
The command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable radius-accounting

disable radius-accounting

Description
Disables RADIUS accounting.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command disables RADIUS accounting for the switch:

disable radius-accounting

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable source-ip-lockdown ports

    disable source-ip-lockdown ports [all | <portlist>]

Description
Disables the source IP lockdown feature on one or more ports.

Syntax Description

<table>
<thead>
<tr>
<th>port-list</th>
<th>Specifies the ports to which the command applies.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
By default source IP lockdown is disabled.

Usage Guidelines

Example

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms
disable ssh2

Description
Disables the SSH2 server for incoming SSH2 sessions to the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
SSH2 session options (access profile and non-default port setting) are not saved when SSH2 is disabled.

To view the status of SSH2 telnet sessions on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for SSH2 telnet sessions.

SSH2 client connections can still be initiated from the switch when the SSH2 server is disabled.

Example
The following command disables the SSH2 server:

disable ssh2

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable tacacs

disable tacacs

Description
Disables TACACS+ authentication.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command disables TACACS+ authentication for the switch:
disable tacacs

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable tacacs-accounting

disable tacacs-accounting

Description
Disables TACACS+ accounting.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command disables TACACS+ accounting:

disable tacacs-accounting

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable tacacs-authorization

Description
Disables TACACS+ authorization.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command disables CLI command authorization but leaves user authentication enabled.

Example
The following command disables TACACS+ CLI command authorization:

disable tacacs-authorization

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable trusted-mac-address

disable trusted-mac-address (vlan <vlan-name>)

Description
Disables trusted Organizational Unique Identifier (OUI) or MAC addresses for port-specific configurations.

Syntax Description

| vlan name | Specifies the VLAN on whose ports trusted-MAC feature should be disabled. |

Default
Disabled

Usage Guidelines
Use this command to disable OUI or MAC addresses for port-specific configurations. Disabling this feature does not remove the previous port-specific configurations. The system default is disable trusted-mac-address.

To disable the feature globally, use disable trusted-mac-address.

To disable the feature on a VLAN, use disable trusted-mac-address vlan <vlan-name>

Use the following command to enable a trusted MAC address:

enable trusted-mac-address

Example
The following command disables trusted MAC addresses on the VLAN named corp:

disable trusted-mac-address vlan corp

History
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
disable web

Description
Disables both HTTP access and secure HTTP access (HTTPS) to the switch.

NOTE
This command is available only for the Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
Enabled

Usage Guidelines
Use this command to prevent web access.

Example
The following command disables HTTP and HTTPS:

disable web

History
This command was first available in ExtremeWare 6.2a.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on the Summit 300 series only.
disable web http

disable web http

Description
Disables HTTP access to the switch on the default HTTP port (80).

NOTE
This command is available only on the Alpine 3800 and Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
Enabled

Usage Guidelines
Use this command to disallow users from connecting with HTTP. Disabling HTTP access forces users to use a secured HTTPS connection if web HTTPS is enabled.

Use the following command to enable web HTTPS:

enable web https

Example
The following command disables HTTP on the default port:

disable web http

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300 and Alpine 3800 series only.
disable web https

disable web https

Description
Disables secured HTTP access (HTTPS) to the switch on the default HTTPS port (443).

\[\text{NOTE}\]
This command is available only on the Alpine 3800 and Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
Enabled

Usage Guidelines
Use this command to disable HTTPS before changing the certificate or private key.

Example
The following command disables HTTPS on the default port:

disable web https

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300 and Alpine 3800 series only.
download ssl certificate

download ssl <ip address> certificate <cert file>

Description
Permits downloading of a certificate key from files stored in a TFTP server.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the TFTP server.</td>
</tr>
<tr>
<td>cert file</td>
<td>Specifies the name of certificate key.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If the download operation is successful, any existing certificate is overwritten. Following successful download, a check is performed to find out whether the public key in the certificate matches the private key stored. If the private and public keys do not match, a warning message is displayed (“Warning: The Private Key does not match with the Public Key in the certificate.”). This warning is a reminder to the user to download the private key also.

The certificate and private key file should be in PEM format and generated using RSA as the cryptography algorithm.

Example
The following example downloads a certificate from IP address 166.81.0.14:

download ssl 166.81.0.14 certificate goethner1

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
Beginning with ExtremeWare 7.4, this command is available in all platforms using SSH image except for the Summit “i” platform switches using SSH Base image (.SBxtr).
download ssl privkey

download ssl <ip address> privkey <key file>

Description
Permits downloading of a private key from files in a TFTP server.

NOTE
This command is available only for the Alpine 3800 and Summit 300 switches.

Syntax Description

| ip address | Specifies the IP address of the TFTP server. |
| key file   | Specifies the name of private key file.      |

Default
N/A

Usage Guidelines
When this command is executed, if the private key is encrypted, the user is prompted to enter the passphrase that was used to encrypt the private key when the private key was generated. Only DES and 3DES encryption mechanisms are supported for private key encryption. If the download operation is successful the existing private key is overwritten.

After the download is successful, a check is performed to find out whether the private key downloaded matches the public key stored in the certificate. If they do not match, a warning message is displayed (“Warning: The Private Key does not match with the Public Key in the certificate.”). This warning is a reminder to the user to download the corresponding certificate.

The certificate and private key file should be in PEM format and generated using RSA as the cryptography algorithm.

Example
The following command enables downloading of a private key from a TFTP server:

download ssl 166.81.0.14 privkey t00Ts1e

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.
Platform Availability

Beginning with ExtremeWare 7.4, this command is available in all platforms using SSH image except for the Summit “i” platform switches using SSH Base image (.SBxtr).
enable access-list

    enable access-list <name> [counter | log]

**Description**
Enables message logging or the collection of access-list statistics.

⚠️ **NOTE**
*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of the access list.</th>
</tr>
</thead>
<tbody>
<tr>
<td>counter</td>
<td>Specifies that access-list statistics should be collected.</td>
</tr>
<tr>
<td>log</td>
<td>Specifies that a message should be logged to the Syslog facility for each packet that matches the access-list description. The message details the properties of the packet.</td>
</tr>
</tbody>
</table>

**Default**
Counting is on; logging is off.

**Usage Guidelines**
None

**Example**
The following command enables statistics collection for access list *allow102*:

```
enable access-list allow102 counter
```

The following command enables logging of packets for access list *allow102*:

```
enable access-list allow102 log
```

**History**
This command was first available in ExtremeWare 6.0.

**Platform Availability**
This command is available on the “i” series platforms only.
enable arp-learning

enable arp-learning

Description
Enables the ARP-learning feature on the switch.

Syntax Description
This command has no arguments or variables.

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
enable arp-learning ports

    enable arp-learning ports <portlist>

Description
Enables the ARP-learning feature on a port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ingress port(s) on which this rule is applied.</td>
</tr>
<tr>
<td>any</td>
<td>specifies that the rule will be applied to all ports.</td>
</tr>
</tbody>
</table>

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
enable arp-learning vlan

   enable arp-learning vlan <vlan name>

Description
Enables the ARP-learning feature on a vlan.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the vlan to which the rule applies.</td>
</tr>
</tbody>
</table>

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on the “i” series platforms only.
enable arp-learning vlan ports

    enable arp-learning vlan <vlan name> port <portlist>

Description
Enables the ARP-learning feature on a port in the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the vlan to which the rule applies.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports to which the rule applies.</td>
</tr>
</tbody>
</table>

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
N/A

History
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
enable cpu-dos-protect

enable cpu-dos-protect

Description
Enables denial of service protection.

Syntax Description
There are no arguments or variables for this command.

Default
The default is disabled.

Usage Guidelines
None

Example
The following command enables denial of service protection.

```
enable cpu-dos-protect
```

History
This command was first available in ExtremeWare 6.2.2.

This command was added to the Summit “e’’ series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable cpu-dos-protect simulated

enable cpu-dos-protect simulated

Description
Enables simulated denial of service protection.

Syntax Description
There are no arguments or variables for this command.

Default
The default is disabled.

Usage Guidelines
When simulated denial of service protection is enabled, no ACLs are created. This mode is useful to gather information about normal traffic levels on a switch. This will assist in configuring denial of service protection so that legitimate traffic is not blocked.

Example
The following command enables simulated denial of service protection.

enable cpu-dos-protect simulated

History
This command was first available in ExtremeWare 6.2.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
enable dhcp ports vlan

    enable dhcp ports <portlist> vlan <vlan name>

**Description**

Enables DHCP on a specified port in a VLAN.

**NOTE**

This command is available only on the “e” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports for which DHCP should be disabled.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN on whose ports DHCP should be disabled.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

The DHCP server should be used with network login and not as a stand-alone DHCP server.

**Example**

The following command enables DHCP for port 9 in VLAN corp:

```bash
enable dhcp ports 9 vlan corp
```

**History**

This command was first available in ExtremeWare 7.1e.

**Platform Availability**

This command is available on the “e” series platforms only.
enable enhanced-dos-protect

enable enhanced-dos-protect {rate-limit | ipfdb} {ports [<portlist> | all]}

Description
Enables enhanced denial of service protection globally or for selected ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit</td>
<td>Enables software rate limiting.</td>
</tr>
<tr>
<td>ipfdb</td>
<td>Enables the IPFDB learning qualifier, resulting in reduction of IPFDB thrashing.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*; 1:5, 1:6-1:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Use the rate-limit keyword in this command to lower the percentage of slow path traffic being sent to the CPU. Verify the enabled/disabled status by using the show enhanced-dos-protect rate-limit command.

Use the ipfdb keyword in this command to prevent IPFDB thrashing. Verify the enabled/disabled status by using the show enhanced-dos-protect ipfdb command.

Examples
The following command enables enhanced denial of service protection rate limiting for all ports.

```
enable enhanced-dos-protect rate-limit ports all
```

The following command globally enables the enhanced denial of service protection IPFDB learning qualifier.

```
enable enhanced-dos-protect ipfdb
```

History
This command was first available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
enable ip-subnet-lookup

enable ip-subnet-lookup

Description
Enables IPDA subnet lookup feature in a switch.

Syntax Description
There are no arguments or variables for this command.

Default
Disabled

Usage Guidelines
For a new setting to be effective in the “i” series switches, system rebooting is needed. Rebooting is not needed for the “e” series switches.

On the “i” series switches, if IPDA subnet lookup is enabled for the first time, the IPDA subnet lookup mask length is 24 (255.255.255.0).

Example

enable ip-subnet-lookup
To be effective, system rebooting is needed
# show ipc
IP Routing : Enabled
....
MPLS : Disabled

In default status, IPDA SUBNET lookup feature is disabled.
# show ipc
IP Routing : Enabled
....
MPLS : Disabled

If flow redirections, IPDA QOS, or FDB ACL is configured, operation is aborted with error message
# enable ip-subnet-lookup
ERROR: Flow Redirection is already configured. Remove flow redirection configuration at first.

History
This command was first available in ExtremeWare 7.3.0.

This command was added to the “e” series switches in ExtremeWare 7.5.
Platform Availability
This command is available on all platforms.
enable mac-lockdown-timeout ports

enable mac-lockdown-timeout ports [<portlist> | all]

Description
This command enables the MAC address lockdown timeout feature for the specified port or group of
ports or for all ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
By default, the MAC address lockdown timeout feature is disabled.

Usage Guidelines
You cannot enable the MAC lockdown timer on a port that also has the lock learning feature enabled.
For more information about MAC lock learning (MAC address lockdown), see “MAC Address
Lockdown” on page 242.

Example
The following example enables the MAC address lockdown timeout set for ports 3 and 5.

```
enable mac-lockdown-timeout ports 3,5
```

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
enable netlogin

enable netlogin [web-based | dot1x | mac]

Description
Enables network login authentication modes.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>web-based</td>
<td>Specifies web-based authentication.</td>
</tr>
<tr>
<td>dot1x</td>
<td>Specifies 802.1x authentication.</td>
</tr>
</tbody>
</table>
| mac      | Specifies MAC-based RADIUS authentica
tion. |

Default
Web-based and 802.1x authentication are enabled by default.
MAC-based authentication is disabled by default.

Usage Guidelines
All types, any combination of types, or no type of authentication can be enabled on the same switch. To disable an authentication mode, use the following command:

disable netlogin [web-based | dot1x | mac]

This command was first introduced as enable netlogin, which enabled the initial version of network login, the web-based mode. The original command was subsequently deprecated when the 802.1x mode of network login was introduced in ExtremeWare 7.1.0. The deprecated version of the command is temporarily supported in configurations. During an upgrade, the deprecated command enable netlogin will be interpreted as:

enable netlogin web-based
enable netlogin dot1x

Example
The following command enables web-based network login:

enable netlogin web-based

The following command globally enables MAC-based network login:

enable netlogin mac

History
This command was first available in ExtremeWare 7.0.0.
The web-based and dot1x keywords were added in ExtremeWare 7.1.0, and the initial version of the command (without the new keywords) was deprecated.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
The `mac` keyword was added in ExtremeWare 7.4.

**Platform Availability**

This command is available on all platforms.
enable netlogin logout-privilege

Description
Enables the network login logout pop-up window.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
This command controls the logout window pop-up on the web-based network client. This command applies only to the web-based authentication mode of network login.

Example
The following command enables the network login logout pop-up window:

```
enable netlogin logout-privilege
```

History
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable netlogin ports

   enable netlogin ports <portlist> vlan <vlan name>

**Description**
Enables network login on a specified port in a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports for which network login should be enabled.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN on whose ports network login should be enabled.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The VLAN you specify must exist and include the specified ports prior to enabling network login. Only untagged ports are allowed to be configured for network login.

For campus mode login with web-based clients, the following conditions must be met:

- A DHCP server must be available, and a DHCP range must be configured for the port or ports in the VLAN on which you want to enable network login.
- The switch must be configured as a RADIUS client, and the RADIUS server must be configured to enable the Extreme network login capability.

For ISP mode login, no special conditions are required. A RADIUS server must be used for authentication.

Network login is used on a per-port, per-VLAN basis. **On the “i” series switches**, a port that is tagged can belong to more than one VLAN. In this case, network login can be enabled on one port for each VLAN.

Windows authentication is not supported via network login.

**Example**
The following command configures network login on port 9 in VLAN corp:

```
enable netlogin ports 9 vlan corp
```

**History**
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
enable netlogin ports mac

    enable netlogin ports <portlist> mac

Description
Enables MAC-based authentication for network login on the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the ports for which MAC-based network login should be enabled.</td>
</tr>
</tbody>
</table>

Default
By default, MAC-based authentication for network login is disabled.

Usage Guidelines
MAC-based RADIUS authentication uses the MAC address of the client for authentication. This feature is useful for devices that cannot function as 802.1x supplicants, such as IP phones. RADIUS is used as the transport protocol for authentication.

Before MAC-based RADIUS authentication is enabled, the RADIUS server must be populated with the MAC addresses of all clients or with a MAC address and a mask. To add MAC address/mask pairs to the table used for MAC-based network login authentication, use the following command:

configure netlogin mac-address

When a new MAC address is detected on a port that is enabled for MAC-based network login, the RADIUS client sends an authentication message (RADIUS access-request) to the RADIUS server for validation. The RADIUS client tries the configured maximum number of retries to validate the supplicant. To configure the maximum number of retries, use the following command:

configure netlogin mac auth-retry-count

While a port is in an authenticated state, the reauthentication mechanism periodically sends a RADIUS Access-Request message to the RADIUS server to reauthenticate the port. To specify the number of seconds between successive reauthentication messages, use the following command:

configure netlogin mac reauth-period

Example
The following command enables MAC-based network login on port 9:

enable netlogin ports 9 mac

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
enable netlogin session-refresh

    enable netlogin session-refresh {<minutes>}

Description
Disables network login session refresh.

Syntax Description

| minutes | Specifies the session refresh time for network login in minutes. |

Default
Disabled, with a value of three minutes for session refresh.

Usage Guidelines
Network login sessions can refresh themselves after a configured timeout. After the user has been logged in successfully, a logout window opens which can be used to close the connection by clicking on the LogOut link. Any abnormal closing of this window is detected on the switch and the user is logged out after a time interval as configured for session refresh. The session refresh is enabled and set to three minutes by default. The value can range from 1 to 255 minutes. When you configure the network login session refresh for the logout window, ensure that the FDB aging timer is greater than the network login session refresh timer.

This command applies only to the web-based authentication mode of network login.

enable netlogin session-refresh enables the session-refresh option only if this option was disabled earlier using the disable netlogin session-refresh command. It doesn’t reset the refresh minutes to default value.

Example
The following command enables network login session refresh and sets the refresh time to ten minutes:

```
enable netlogin session-refresh 10
```

History
This command was first available in ExtremeWare 7.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable radius

enable radius

Description
Enables the RADIUS client on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
When enabled, all web and CLI logins are sent to the RADIUS servers for authentication. When used with a RADIUS server that supports ExtremeWare CLI authorization, each CLI command is sent to the RADIUS server for authorization before it is executed.

Example
The following command enables RADIUS authentication for the switch:

```
enable radius
```

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable radius-accounting

enable radius-accounting

Description
Enables RADIUS accounting.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
The RADIUS client must also be enabled.

Example
The following command enables RADIUS accounting for the switch:

enable radius-accounting

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable source-ip-lockdown ports

   enable source-ip-lockdown ports [all | <portlist>]

Description
Enables the source IP lockdown feature.

Syntax Description

| port-list | Specifies one or more ports for which source IP lockdown should be enabled. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:* , 1:5, 1:6-1:8. |
| all | Specifies all ports. |

Default
By default source IP lockdown is disabled.

Usage Guidelines
This feature applies only to the Layer 3 environment. The switch allows only those hosts whose IP addresses are assigned by the locally configured DHCP server (switch acting as a DHCP server) or assigned by an external DHCP server. In the latter case, the switch should be configured as a bootp relay. For statically configured IP ARP entries, the MAC address (specified during the addition of a IP ARP entry) should already exist in the FDB. Before enabling source IP lockdown on a port, the switch should be configured either as a DHCP Server or a BOOTP Relay.

Example
The following command enables source IP lockdown on ports 3 and 5

enable source-ip-lockdown ports 3,5

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms
enable ssh2

    enable ssh2 {access-profile [<access profile> | none]} {port <tcp_port_number>}

Description
Enables the SSH2 server to accept incoming sessions from SSH2 clients.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
<tr>
<td>none</td>
<td>Cancels a previously configured access profile.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a TCP port number. The default is port 22.</td>
</tr>
</tbody>
</table>

Default
The SSH2 feature is disabled by default.

Usage Guidelines
SSH2 enables the encryption of session data. You must be logged in as an administrator to enable SSH2, and you must obtain and enter a security license key to enable the SSH2 feature. To obtain a security license key, access the Extreme Networks website.

You can specify a list of predefined clients that are allowed SSH2 access to the switch. To do this, you must create an access profile that contains a list of allowed IP addresses. To create an access profile, use the create access-profile type command. To configure an access profile, use the configure access-profile add command.

Use the none option to cancel a previously configured access profile.

Use the port option to specify a TCP port number other than the default.

To view the status of SSH2 sessions on the switch, use the show management command. The show management command displays information about the switch including the enable/disable state for SSH2 sessions.

Example
The following command enables the SSH2 feature, with access allowed based on the access profile management:

    enable ssh2 access-profile management

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
enable tacacs

enable tacacs

Description
Enables TACACS+ authentication.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
After they have been enabled, all web and CLI logins are sent to one of the two TACACS+ servers for login name authentication and accounting.

Example
The following command enables TACACS+ user authentication:

```bash
enable tacacs
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable tacacs-accounting

enable tacacs-accounting

Description
Enables TACACS+ accounting.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
If accounting is used, the TACACS+ client must also be enabled.

Example
The following command enables TACACS+ accounting for the switch:
    enable tacacs-accounting

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable tacacs-authorization

enable tacacs-authorization

Description
Enables CLI command authorization.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
When enabled, each command is transmitted to the remote TACACS+ server for authorization before the command is executed.

Example
The following command enables TACACS+ command authorization for the switch:

```
enable tacacs-authorization
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable trusted-mac-address

    enable trusted-mac-address {vlan <vlan_name>}

**Description**

Enables the trusted-MAC feature at either the global level or a VLAN level.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_name</td>
<td>Specifies the name of a VLAN on which to enable the trusted-MAC feature.</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Usage Guidelines**

Use this command to enable the trusted-MAC feature at either the global level or a VLAN-specific level. If you specify the command without the VLAN option, the trusted-MAC feature is enabled for VLAN-specific configurations.

To enable the feature globally, enter:

    enable trusted-mac-address

To enable and activate trusted-MAC on an individual VLAN, enter:

    enable trusted-mac-address vlan <vlan name>

Use the following command to disable a trusted MAC address:

    disable trusted-mac-address

Disabling this feature does not remove the previous port-specific information.

**Example**

The following command enables the trusted-MAC feature globally on the VLAN named corp:

    enable trusted-mac-address vlan corp

**History**

This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

**Platform Availability**

This command is available on the “i” platforms and Summit 300 switches.
enable web

enable web

Description
Enables both HTTP access to the switch and HTTPS on the default ports.

NOTE
This command is available only on the Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
Enabled

Usage Guidelines
Use this command to enable HTTP and HTTPS access to the switch web pages on the default ports. The default port for HTTP is port 80 and HTTPS is port 443.

Example
The following command enables HTTP and HTTPS on the default port:

```plaintext
enable web
```

History
This command was first available in ExtremeWare 6.2a.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Summit 300 series switches.
enable web http

Description
Enables HTTP access to the switch on the default HTTP port (80).

NOTE
This command is available only on the Alpine 3800 and Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
Enabled

Usage Guidelines
Use this command to enable HTTP access to the switch web pages.

Example
The following command enables HTTP on the default port:

```
enable web http
```

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300 and Alpine 3800 series only.
enable web http access-profile

   enable web http access-profile [none | <access-profile>] port <port number>

Description
Allows HTTP access on the specified (non-default) port.

NOTE
This command is available only on the Alpine 3800 and Summit 300 series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies not to use an access profile when accessing HTTP.</td>
</tr>
<tr>
<td>access-profile</td>
<td>Specifies the name of an access profile to use when accessing HTTP.</td>
</tr>
<tr>
<td>port number</td>
<td>Specifies the port number to use to access HTTP.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to set up an access profile for a particular port number to restrict HTTP usage.

Example
The following example enables HTTP access using the access profile named open_web on port 120:

```
enable web http access-profile open_web port 120
```

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300 and Alpine 3800 series only.
enable web https

enable web https

Description
Enables secure HTTP access (HTTPS) to the switch on the default HTTPS port (443).

**NOTE**
this command is available only on the Alpine 3800 and Summit 300 series switches.

Syntax Description
This command has no parameters or variables.

Default
Enabled

Usage Guidelines
Use this command to allow users to connect using a more secure HTTPS connection.

Example
The following command enables HTTPS on the default port:

```
enable web https
```

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300 and Alpine 3800 series only.
enable web https access-profile

   enable web https access-profile [none | <access-profile>] port <port number>

Description
Allows HTTPS access on the specified (non-default) port.

NOTE
This command is available only for the Alpine 3800 and Summit 300 series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies to not to use an access profile when accessing HTTPS.</td>
</tr>
<tr>
<td>access-profile</td>
<td>Specifies the name of an access profile to use when accessing HTTPS.</td>
</tr>
<tr>
<td>port number</td>
<td>Specifies the port number to use to access HTTPS.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to set up an access profile for a particular port number to restrict HTTPS usage.

Example
The following example enables HTTPS access using the access-profile named secure_web on port 120:

   enable web https access-profile secure_web port 120

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300 and Alpine 3800 series only.
scp2

scp2 \{cipher [3des | blowfish]\} \{port <portnum>\} \{debug <debug_level>\} <user>@ [\<hostname> | \<ipaddress>\] :<remote_file> \{configuration \{incremental\} | image \{primary | secondary\} | bootrom\}

**Description**

Initiates an SCP2 client session to a remote SCP2 server and copies a file from the remote system to the switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
<td>Specifies that the 3des cipher should be used for encryption. This is the default.</td>
</tr>
<tr>
<td>blowfish</td>
<td>Specifies that the blowfish cipher should be used for encryption.</td>
</tr>
<tr>
<td>portnum</td>
<td>Specifies the TCP port number to be used for communicating with the SSH2 client. Default is port 22.</td>
</tr>
<tr>
<td>debug_level</td>
<td>Specifies a debug level. Default is 0.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies a login name for the remote host.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the name of the remote host.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the remote host.</td>
</tr>
<tr>
<td>remote file</td>
<td>Specifies the name of the remote file to be copied to the switch.</td>
</tr>
<tr>
<td>configuration</td>
<td>Specifies that the copied file is a switch configuration file. It the incremental option is not specified, it replaces the current switch configuration.</td>
</tr>
<tr>
<td>incremental</td>
<td>Specifies that the copied file should be handled like an incremental configuration download (only the commands in the file are executed).</td>
</tr>
<tr>
<td>image</td>
<td>Specifies that the copied file is an ExtremeWare image.</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies that the image should be placed in the primary image area.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies that the image should be placed in the secondary image area.</td>
</tr>
<tr>
<td>bootrom</td>
<td>Specifies that the copied file is a bootrom image.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

You must be running a security-enabled version of ExtremeWare 6.2.1 or later (which is under Export Control) in order to use the SCP2 command.

SSH2 does not need to be enabled on the switch in order to use this command.

This command logs into the remote host as `<user>` and accesses the file `<remote_file>`. You will be prompted for a password from the remote host, if required.
CAUTION

You can download a configuration to an Extreme Networks switch using SCP. If you do this, you cannot save this configuration. If you save this configuration and reboot the switch, the configuration will be corrupted.

Example

The following command copies a configuration file from the file \texttt{configpart1.save} on host \texttt{system1} to the switch as an incremental configuration:

\texttt{scp2 admin@system1:configpart1.save configuration incremental}

History

This command was first available in ExtremeWare 6.2.1

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
scp2 configuration

scp2 {cipher [3des | blowfish]} {port <portnum>} {debug <debug_level>} configuration <user>@ [<hostname> | <ipaddress>]:<remote_file>

Description
Copies the configuration file from the switch to a remote system using SCP2.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
<td>Specifies that the 3des cipher should be used for encryption. This is the default.</td>
</tr>
<tr>
<td>blowfish</td>
<td>Specifies that the blowfish cipher should be used for encryption.</td>
</tr>
<tr>
<td>portnum</td>
<td>Specifies the TCP port number to be used for communicating with the SSH2 client. Default is port 22.</td>
</tr>
<tr>
<td>debug_level</td>
<td>Specifies a debug level. Default is 0.</td>
</tr>
<tr>
<td>user</td>
<td>Specifies a login name for the remote host.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the name of the remote host.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the remote host.</td>
</tr>
<tr>
<td>remote_file</td>
<td>Specifies the name of the file to be created on the remote host.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You must be running a security-enabled version of ExtremeWare 6.2.1 or later (which is under Export Control) in order to use the SCP2 command.

SSH2 does not need to be enabled on the switch in order to use this command. (SSH2 is enabled by default if you are running a security-enabled version of ExtremeWare).

This command logs into the remote host as <user> and creates the file <remote_file>.

Example
The following command copies the switch configuration and saves it as file config1.save on host system1:
scp2 configuration admin@system1:config1.save

History
This command was first available in ExtremeWare 6.2.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show access-list

    show access-list {<name> | port <portlist>}

Description
Displays access list information and real-time statistics.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an access list to be displayed.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Shows information for all access lists.

Usage Guidelines
To verify access list settings, you can view the access list configuration and see real-time statistics on which access list entries are being accessed when processing traffic.

Example
The following command shows information on all current access lists:

show access-list

It produces output similar to the following:

<table>
<thead>
<tr>
<th>Rule</th>
<th>Dest/mask:L4DP</th>
<th>Src/mask:L4SP</th>
<th>Flags</th>
<th>Hits</th>
</tr>
</thead>
<tbody>
<tr>
<td>test1</td>
<td>0.0.0.0/ 0: 0</td>
<td>0.0.0.0/ 0: 0</td>
<td>I-P-X</td>
<td>1531</td>
</tr>
</tbody>
</table>

Flags: I=IP, T=TCP, U=UDP, E=Established, M=ICMP
  P=Permit Rule, D=Deny Rule
  N=Port Specific Rule, X=Any Port

The following command shows information on all current access lists:

show access-list a1

It produces output similar to the following:

#show access-list a1

Access-list with name "a1" created by user

Access-mask:  "f1"
show access-list

MAC:
  IP/mask:L4port: dest-ip=11.11.11.0/24:---- source-ip=none/--:----
Layer 2:
  Layer 3/4:
Egress Port:
  Ingress Ports:  2 3 4 5
  In Profile:     permit QOS=QP5
#show access-list port 2
Access-list "a1"
  Access-mask:    "f1"
MAC:
  IP/mask:L4port: dest-ip=11.11.11.0/24:---- source-ip=none/--:----
Layer 2:
  Layer 3/4:
Egress Port:
  Ingress Ports:  2 3 4 5
  In Profile:     permit QOS=QP5

The following command shows real-time access list statistics for ingress ports 5-7:
show access-list port 5-7

The following command shows information for access list test1:
show access-list test1

The command generates output similar to the following:
test1
  Protocol: ip    Action: permit qp1
  Destination: 0.0.0.0/0 any
  Source: any    any
  Precedence: 0
  Rule Number: 0
  Hit Count: 4566 Flags: ac
  Ports:
    any

The following example shows output of the command on an “e” series switch:

Summit200-48:12 # show access-list acl1
Access-list "acl1"
  Access-mask:    "mask1"
MAC:
  IP/mask:L4port: dest-ip=none/--:---- source-ip=10.0.0.1/32:----
Layer 2:
  Layer 3/4:
Egress Port:
  Ingress Ports:  all
  In Profile:     deny

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
show access-list source-ip-lockdown

Description
Displays the ACLs created for the source IP lockdown feature.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines

Example
The following command displays the ACLs created for the source IP lockdown feature:
show access-list source-ip-lockdown

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms
show access-list-fdb

Description
Displays the hardware access control list mapping.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command displays the hardware access control list mapping:
show access-list-fdb

History
This command was first available in ExtremeWare 6.0.

Platform Availability
This command is available on the “i” series platforms only.
show access-list-monitor

Description
Initiates the access-list information display, and refreshes it until discontinued.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command initiates a display of real-time access list information. Use the keys as shown in Table 17 to change the view of the data. The [Esc] or [Return] keys discontinue the display.

Table 17: Monitoring Display Keys

<table>
<thead>
<tr>
<th>Key(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>U</td>
<td>Displays the previous page of ports.</td>
</tr>
<tr>
<td>D</td>
<td>Displays the next page of ports.</td>
</tr>
<tr>
<td>[Esc] or [Return]</td>
<td>Exits from the screen.</td>
</tr>
<tr>
<td>0</td>
<td>Clears all counters.</td>
</tr>
</tbody>
</table>

Example
The following command initiates the access-list information display:

```
show access-list-monitor
```

The command displays output similar to the following:

```
Access List | Proto | Destination | Source | Hit Count
-------------|-------|-------------|--------|-----------
test1        | ip    | 0.0.0.0/0   | 0.0.0.0/0 | 1922      
```

The Hit Count continues to be updated until you exit from the display or enter “0” to reset the count to zero.

History
This command was first available in ExtremeWare 6.0.
Platform Availability
This command is available on the “i” series platforms only.
show access-mask

    show access-mask {<name>}

Description
Displays information about a specific access mask or all access masks.

NOTE
This command is available only on the “e” series switches.

Syntax Description

| name        | Specifies an access mask name. |

Default
N/A

Usage Guidelines
None

Example
The following command shows information about the access mask called MyIpMask.

    show MyIpMask

The command generates output similar to the following:

    Access-mask with name “MyIpMask” created by user
    MAC:
    IP/mask:L4port:
    Layer 2:
    Layer 3/4:
    Ports:
    Precedence:
    ACL/Rate-limit:

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is available on the “e” series platforms only.
show access-profile

    show access-profile {<access profile>}

Description
Displays access-profile related information for the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Access profile</th>
<th>Specifies an access profile.</th>
</tr>
</thead>
</table>

Default
Shows all access profile information for the switch.

Usage Guidelines
None

Example
The following command displays access-profile related information for access profile called nosales:

    show access-profile nosales

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show arp-learning vlan

    show arp-learning vlan <vlan name>

Description
Displays the ARP-learning feature on a port in the given vlan.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the vlan to which the rule applies.</td>
</tr>
</tbody>
</table>

Default
By default, ARP learning is enabled.

Usage Guidelines
None

Example
The following command shows that ARP learning is enabled on the management VLAN:

```
# show arp-learning vlan mgmt
Arp Learning Enabled on vlan Mgmt
          (Vlan,Port)-Arp Learning                  (Port)-Arp learning
            --------------------------                  ------------------------
            [Mgmt      ,Mgmt]- Enabled                       [Mgmt]-Enabled
```

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show arp-learning vlan ports

    show arp-learning vlan <vlan name> ports <portlist>

**Description**
Displays the ARP-learning configuration for a port in the given vlan.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the vlan to which the rule applies.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports to which the rule applies.</td>
</tr>
</tbody>
</table>

**Default**
By default, ARP learning is enabled.

**Usage Guidelines**
The first column of the show output displays the configuration of the VLAN and port. The second column of the output display the ARP learning configuration on that port.

**Example**
The following example displays the arp-learning configuration on the VLAN called vlan1:

* Summit400-48t:55 #show arp-learning vlan1 ports all

The command generates output similar to the following:

```
(Vlan,Port)-Arp Learning       (Port)-Arp learning
--------------------------      ------------------------
[vlan1     ,3   ]-Enabled       [3   ]-Enabled
```

**History**
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
show auth

Description
Displays the current authentication and accounting servers configured for management and netlogin sessions.

Syntax Description
There are no arguments or variables for this command.

Default
Shows all authentication server information for the switch.

Usage Guidelines
The output from this command displays the information about the type of authentication and accounting used by the primary and secondary servers that are configured for that particular type of session.

Example
The following example displays the authentication information:

```
show auth
```

The output of the command is similar to:

```
Session Type : mgmt-access
   Authentication Server Type : Radius
   Primary Authentication Server : 12.16.1.2
   Secondary Authentication Server : None
   Primary Accounting Server : None
   Secondary Accounting Server : None

Default configuration :
   Using Radius servers for Authentication/Accounting
   Primary Authentication Server : 172.16.1.2
```

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show cpu-dos-protect

For the “i” switches:
   show cpu-dos-protect

For the “e” switches:
   show cpu-dos-protect [ports <portnumber>]

Description
Displays the status of denial of service protection for the entire switch or for a particular port (on the “e” series switches).

Syntax Description
There are no arguments or variables for this command in the “i” switches.

On the “e” switches, the syntax is:

| portnumber | Specifies one or more port numbers. May be in the form 1, 2, 3-5. |

Default
The output of this command has valid values only when denial of service protection is enabled.

Usage Guidelines
None

Examples
The following command displays the status of denial of service protection on an “i” series switch.

show cpu-dos-protect

Following is the output from this command:

Denial-of-service protection to CPU is ENABLED
Notice level:  4000 new packets/second (level for logging)
Alert level:  4000 new packets/second (level for ACL creation)
Filter types: destination
ACL timeout:  15 seconds
ACL rule precedence: 10
Messages are ON
Trusted Ports:  none
ACL is active ports 48 to 192.168.3.1 proto all precedence 10
ACL should expire in 13 seconds

The following command displays the status of denial of service protection on port 1.

show cpu-dos-protect ports 1
Following is the output from this command:

```
Cpu dos protect: enabled

Port L3Miss L3Err Bcast IpUnkMcast Learn Curr Int Cfg Thr Cfg Int Pass
1   150   150   150   150   150   1   150 1   3
```

Trusted ports: none

The output of this show command displays the following information, which can help you analyze the type of activity coming across the port to the CPU:

- The status of DoS Protection on the port
- Layer 3 miss to the CPU
  These are packets that do not have corresponding IPFDB entries on VLANs, which are enabled for IP forwarding. Packets that are unicast to the CPU IP are also considered in this category.
- Layer 3 error
  These are IP packets with options, IPMC packets (but not class D address) with checksum errors, and non-IP packets.
- Broadcast traffic
- IP multicast unknown
  These are IPMC packets that do not have corresponding IPMC FDB entries.
- Learning packets
  These are packets that do not have a corresponding FDB entries.
- Current interval
  The current time interval, less than or equal to the configured interval.
- Configured alert threshold
  The maximum number of packets that can be sent to the CPU. This variable is equal to the `configured interval` parameter in seconds for each traffic category.
- Configured interval
- Free pass indicator (Zero in this field indicates a free pass for three intervals after the port comes up.)
- Trusted port status

**History**

This command was first available in ExtremeWare 6.2.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show enhanced-dos-protect

show enhanced-dos-protect [rate-limit | ipfdb] ports [<portlist> | all]

Description
Displays the status of the enhanced denial of service protection feature.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-limit</td>
<td>Displays rate limiting configuration.</td>
</tr>
<tr>
<td>ipfdb</td>
<td>Displays IPFDB learning qualifier configuration.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The output from this command displays status of the following enhanced denial of service protection conditions:

- Enabled/Disabled
- Max. entries
- Current entries
- List of trusted/untrusted ports
- Rate limiting configuration
- Packet filtering statistics

Example
The following command shows global enhanced denial of service protection rate limit information:

```
show enhanced-dos-protect rate-limit
```

<table>
<thead>
<tr>
<th>PortNum</th>
<th>Status</th>
<th>Trusted</th>
<th>Proto</th>
<th>Threshold</th>
<th>Learn-Window</th>
<th>Drop-Prob</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>PktsDrop</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4:4</td>
<td>Enabled</td>
<td>Trusted</td>
<td>icmp</td>
<td>100</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>50</td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enhanced DOS Protect Rate Limit Global Configuration
Global Status : Enabled
History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show ip-subnet-lookup fdb

    show ip-subnet-lookup fdb {<ipaddress> | <ipaddress><netmask>}

Description
Displays the contents of the IP FDB subnet forwarding table. If no option is specified, all IP FDB subnet entries are displayed.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP subnet address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
The default is to show all IP subnet FDB entries.

Usage Guidelines
None

Example
The following command displays the IP subnet forwarding entries:

    show ip-subnet-lookup

This command generates output similar to the following:

<table>
<thead>
<tr>
<th>Dest IP Addr</th>
<th>TblIdx</th>
<th>MacIdx</th>
<th>Flag Flow</th>
<th>MAC Address</th>
<th>VLAN Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>20.2.0.0</td>
<td>11402.0</td>
<td>CCFA.0</td>
<td>00000</td>
<td>0000:00:00:00:00:04</td>
<td>4091 4:3</td>
</tr>
<tr>
<td>20.3.0.0</td>
<td>11403.0</td>
<td>CCFA.0</td>
<td>00000</td>
<td>0000:00:00:00:00:04</td>
<td>4091 4:3</td>
</tr>
<tr>
<td>20.4.0.0</td>
<td>11404.0</td>
<td>CCFA.0</td>
<td>00000</td>
<td>0000:00:00:00:00:04</td>
<td>4091 4:3</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>20.10.128.0</td>
<td>1940A.0</td>
<td>CCFA.0</td>
<td>00000</td>
<td>0000:00:00:00:00:04</td>
<td>4091 4:3</td>
</tr>
</tbody>
</table>

Total number of entries = 61
IPFDB SUBNET Lookup Maskbits: [18]

History
This command was first available in ExtremeWare 7.3.0.
This command was added to the “e” series platforms in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
show mac-lockdown-timeout ports

show mac-lockdown-timeout ports [<portlist> | all]

Description
This command shows information about the MAC address lockdown timeout feature for the specified port or group of ports or for all ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The information generated by this command includes whether or not the feature is enabled and the timeout value set for the specified ports.

Example
The following example shows information about the MAC address lockdown timeout settings for ports 21, 22, 24, and 25.

```
show mac-lockdown-timeout ports 21,22,24,25
```

The command generates output similar to the following:

<table>
<thead>
<tr>
<th>Port</th>
<th>Mac lockdown timeout</th>
<th>Timeout (in secs)</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>Enabled</td>
<td>2000</td>
</tr>
<tr>
<td>22</td>
<td>Enabled</td>
<td>3000</td>
</tr>
<tr>
<td>24</td>
<td>Disabled</td>
<td>200</td>
</tr>
<tr>
<td>25</td>
<td>Disabled</td>
<td>15</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
show mac-lockdown-timeout fdb ports

    show mac-lockdown-timeout fdb ports [<portlist> | all]

Description
This command displays the MAC entries that are learned on the specified port or set of ports, along with the aging time of each port.

Syntax Description

|     | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots
|-----------|------------------------------------------------|
| portlist  | and ports. On a stand-alone switch, can be one or
|           | more port numbers. May be in the form 1, 2, 3-5, 2:*,
| all       | Specifies all ports.

Default
N/A

Usage Guidelines
If a port is down, this command displays all the MAC entries that are maintained locally in the software.

The MAC entries learned on the specified port will be displayed only if the MAC lockdown timeout feature is enabled on the port. If you specify a port on which this feature is disabled, the MAC entries learned on that port will not be displayed.

Example
The following example shows information about the MAC entries for ports 21 and 22.

    show mac-lockdown-timeout fdb ports 21,22

The command generates output similar to the following:

<table>
<thead>
<tr>
<th>Mac</th>
<th>Vlan</th>
<th>Age</th>
<th>Use</th>
<th>Port</th>
<th>Flags</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:00:01:02:03:04</td>
<td>v1(4094) 0010 0000</td>
<td>21</td>
<td>F</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:01:02:03:02</td>
<td>v1(4094) 0030 0000</td>
<td>21</td>
<td>FB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:0A:02:03:04</td>
<td>v2(4093) 0050 0000</td>
<td>22</td>
<td>L</td>
<td></td>
<td></td>
</tr>
<tr>
<td>00:00:0B:02:03:04</td>
<td>v2(4093) 0090 0000</td>
<td>22</td>
<td>F</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Flags: (F) Entry as in h/w FDB (L) Entry in s/w and not in h/w (B) Egress Blackhole,
       (b) Ingress Blackhole

Total: 4, Entries in FDB: 3, Entries in s/w: 1

History
This command was first available in ExtremeWare 7.5.
Platform Availability

This command is available on all platforms.
show netlogin

    show netlogin {port <portlist> vlan <vlan name>}

Description
Shows status information for network login.

Syntax Description

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The information reported by this command is the following:
- Whether network login is enabled or disabled
- The base-URL
- The default redirect page
- The logout privileges setting
- The netlogin session-refresh setting and time
- The MAC and IP address of supplicants
- The type of authentication, 802.1x or HTTP (web-based)

Examples
The following command shows the summary network login information:

```
show netlogin
```

The command generates output similar to the following:

```
Netlogin Authentication Mode :  web-based ENABLED ;   802.1x ENABLED
-----------------------------------------------
Web-based Mode Global Configuration
-----------------------------------------------
Base-URL                              :  "network-access.net"
Default-Redirect-Page                 :  "http://www.extremenetworks.com"
Logout-privilege                      :   YES
Netlogin Session-Refresh              :   DISABLED ; 3 minutes
-----------------------------------------------
802.1x Mode Global Configuration
-----------------------------------------------
```
Quiet Period                        :  60      secs
Client Response Timeout             :  30      secs
Default Reauthentication Timeout    :  3600    secs
Max. Number Authentication Failure  :  3
Periodic Reauthentication           :  ENABLED
---------------------------------

Port: 1:13,   Vlan: Default,  State: Unauthenticated
MAC                IP address      Auth   Type      ReAuth-Timer User
00:B0:D0:90:2F:72  0.0.0.0         No     802.1x    12           Unknown
-------------------------------
Total Number of Authenticated MACs : 0

The following command shows the detailed network login information for the port 1:13 in the VLAN named Default:
show netlogin ports 1:13 "Default"

Following is the output from this command before authentication:
Port: 1:13      Vlan: Default
Port State:     Unauthenticated
DHCP:           Not Enabled
MAC               IP address    Auth  Type   ReAuth-Timer User
------------------------------------------------------------------
00:B0:D0:90:2F:72    0.0.0.0     No   802.1x  30           Unknown
------------------------------------------------------------------
Quiet Period Timer            :  0      Num. Authentication Failed    :  1
------------------------------------------------------------------
Following is the output from this same command after authentication:
Port: 1:13      Vlan: Default
Port State:     Unauthenticated
DHCP:           Not Enabled
MAC               IP address    Auth  Type   ReAuth-Timer User
------------------------------------------------------------------
00:B0:D0:90:2F:72    0.0.0.0     Yes  802.1x  3600        auto20@dot1x.net
------------------------------------------------------------------
Quiet Period Timer            :  0      Num. Authentication Failed    :  0
------------------------------------------------------------------

History
This command was first available in ExtremeWare 6.2.
This command was modified to show the authentication type in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show netlogin mac

Description
Displays the list of MAC address/mask pairs used for MAC-based RADIUS authentication.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
For MAC-based RADIUS authentication, the RADIUS server must be populated with the MAC addresses of the clients, or with MAC addresses plus a mask. This command displays the list of MAC addresses or MAC address/mask pairs used for authentication.

Example
The following command displays the MAC address list for RADIUS authentication:

```
show netlogin mac
```

<table>
<thead>
<tr>
<th>Mac Addr</th>
<th>Mac Mask</th>
<th>Password</th>
</tr>
</thead>
</table>

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
show radius

    show radius {<ipaddress> | <hostname>}

**Description**
Displays the current RADIUS client configuration and statistics.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the RADIUS server for which information is being displayed (optional).</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the name of the host for which RADIUS server information is being displayed.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The output from this command displays the status of the RADIUS and RADIUS accounting (enabled or disabled) and the primary and secondary servers for RADIUS and RADIUS accounting.

If you specify the `ipaddress` option, configuration and statistics for that server are displayed.

**Example**
The following command displays the current RADIUS client configuration and statistics:

```
show radius
```

Following is the output from this command:

Radius: enabled
Radius Accounting: enabled
Radius Server Connect Timeout sec: 3

Primary radius server:
Server name: 172.17.1.123
IP address: 172.17.1.123
Server IP Port: 1645
Client address: 172.17.1.221
Shared secret:
Access Requests:0 Access Accepts:0 Access Rejects:0
Access Challenges:0 Access Retransmits:0 Client timeouts:0
Bad authenticators:0 Unknown types:0 Round Trip Time:0 sec(s)

Secondary radius server:
Server name: 172.17.1.123
IP address: 172.17.1.123
Server IP Port: 1645
Client address: 172.17.1.221
Shared secret:
Access Requests:3 Access Accepts:0 Access Rejects:0
Access Challenges:0 Access Retransmits:2 Client timeouts:0
Bad authenticators:0 Unknown types:0 Round Trip Time:0
Radius Acct Server Connect Timeout sec: 3
Primary radius accounting server:
  Server name:    172.17.1.104
  Client address: 172.17.1.221
  Shared secret:  lf|nki
Secondary radius accounting server:
  Server name:    172.17.1.123
  Client address: 172.17.1.221
  Shared secret:  lf|nki

The following is an example of output from this command where RADIUS is not configured on the switch:
Radius: disabled
Radius Accounting: disabled

Primary radius server:  Not configured
Secondary radius server:  Not configured
Primary radius accounting server:  Not configured
Secondary radius accounting server:  Not configured

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show radius-accounting

    show radius-accounting [{<ipaddress> | <hostname>}]

Description
Displays the current RADIUS accounting client configuration and statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the RADIUS server for which information is being displayed (optional).</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the name of the host for which RADIUS server information is being displayed.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The output from this command displays:

- The status of the RADIUS accounting (enabled or disabled).
- The statistics for the configured primary and secondary servers.

If you specify the ipaddress option, configuration and statistics for that server are displayed.

Example
The following command displays RADIUS accounting client configuration and statistics:

```
show radius-accounting
```

Following is the output from this command:

```
Radius Accounting: enabled
Radius Acct Server Connect Timeout sec: 3
Primary radius accounting server:
    Server name: 172.17.1.104
    IP address: 172.17.1.104
    Server IP Port: 1646
    Client address: 172.17.1.221
    Shared secret: lf|nki
    Acct Requests:0  Acct Responses:0  Acct Retransmits:0  Timeouts:0
Secondary radius accounting server:
    Server name: 172.17.1.123
    IP address: 172.17.1.123
    Server IP Port: 1646
    Client address: 172.17.1.221
    Shared secret: lf|nki
    Acct Requests:0  Acct Responses:0  Acct Retransmits:0  Timeouts:0
```

The following is an example of output from this command:

```
Radius Accounting: disabled
```
Primary radius accounting server:  
   Not configured  
Secondary radius accounting server:  
   Not configured  

**History**  
This command was first available in ExtremeWare 4.1.  
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.  

**Platform Availability**  
This command is available on all platforms.
show rate-limit

    show rate-limit {<name> | ports <portlist>}

**Description**

Displays information for a specific rate limit rule or for all rate limit rules.

**NOTE**

*This command is available only on the “e” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of a rate limit rule.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

If you do not specify a rate limit name, information is displayed for all the rate limit rules.

**Examples**

The following command displays all rate limit information configured for the switch:

```
#show rate-limit
```

Output from this command is similar to the following:

```
Rate-limit   Access-mask  Vlan         QoS Limit Port Flags
r1           f1                     10    5 DI-IP-P-EC
r2           f3                      3    3 IP-P-ED
```

Flags: DM=Dest MAC, SM=Source MAC, ET=Ether Type,
T=TOS, C=Code Point, I=IP Protocol
DI=Dest IP, SI=Src IP, D4=Dest L4 Port, S4=Src L4 Port
MT=ICMP Type, MC=ICMP Code, EP=Egress Port
P=Permit, Q=Qosprofile, SC=Set Code-Point, SD=Set Dot.1p
ED=Exceed Drop, EC=Exceed Set Code-Point

The next example shows information for the r1 rate limit:

```
#show rate-limit r1
Rate-Limit with name "r1" created by user
Access-mask:  "f1"
MAC:
Layer 2:
Layer 3/4:
```
Egress Port:
Ingress Ports:  5
In Profile:     permit
Rate Limit:     10 Mbps
Out Profile:    set code-point=0x2c

The following example shows information for the rate limit configured on port 5:

#show rate-limit port 5
Rate-Limit "r1"
  Access-mask:    "f1"
  MAC:
  Layer 2:
  Layer 3/4:
  Egress Port:
  Ingress Ports:  5
  In Profile:     permit
  Rate Limit:     10 Mbps
  Out Profile:    set code-point=0x2c

History
This command was first available in ExtremeWare 7.1e.

Platform Availability
This command is available on the “e” series platforms only.
show route-map

show route-map <route map>

**Description**
Displays route map information.

**NOTE**
This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route map</td>
<td>Specifies a route map name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
If you do not specify a route map name, information is displayed for all the route maps.

**Example**
The following command displays the route-map named bgp-out:

```
show route-map bgp-out
```

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on the “i” series platforms only.
show security-profile

    show security-profile {<name>}

Description
Displays the configured parameters of the security profile.

Syntax Description

| name | Specifies the name of an existing security profile whose parameters need to be displayed. |

Default
All

Usage Guidelines
Use this command to show security profiles currently configured on the platform and all values associated with each security profile. If no security profile name is entered, configuration parameters are displayed for all security profiles.

Examples
The following command displays the security profile configuration for all profiles:

    show security-profile

The output of the command is similar to:

    Profile Name: Unsecure
    ESS Name: fz-unsecure
    Dot11 Authentication: open
    Network Authentication: none
    Encryption: none
    User VLAN: Default
    Use Dynamic VLAN: yes
    SSID in Beacon: on
    Interfaces: 180
                1:1:2, 1:2:2, 1:3:2, 1:4:1, 1:4:2,
                1:4:2, 1:5:1, 1:5:2, 1:5:2, 1:6:1,
                1:6:2, 1:6:2, 1:7:1, 1:7:2, 1:7:2,
                1:8:1, 1:8:2, 1:8:2, 1:9:1, 1:9:2,
                1:9:2, 1:10:1, 1:10:2, 1:10:2, 1:11:1,
                1:11:2, 1:11:2, 1:12:1, 1:12:2, 1:12:2,
                1:13:1, 1:13:2, 1:13:2, 1:14:1, 1:14:2,
                1:14:2, 1:15:1, 1:15:2, 1:15:2, 1:16:1,
                1:16:2, 1:16:2, 1:17:1, 1:17:2, 1:17:2,
                1:18:1, 1:18:2, 1:18:2, 1:19:1, 1:19:2,
                1:19:2, 1:20:1, 1:20:2, 1:20:2, 1:21:1,
                1:23:1, 1:23:2, 1:23:2, 1:24:1, 1:24:2,
                1:24:2, 1:25:1, 1:25:2, 1:25:2, 1:26:1,
Profile Name: open64wep
  ESSID Name: fz-open-wep-64
  Dot11 Authentication: open
  Network Authentication: none
  Encryption: wep64
  User VLAN: SKSPVlan
  Use Dynamic VLAN: no
  WEP Key 0: 3>:>?75<;5
  Default WEP Key: 0
  SSID in Beacon: on
  Interfaces: 2
    1:3:2, 2:5:1,

Profile Name: open128wep
  ESSID Name: fz-open-wep-128
  Dot11 Authentication: open
  Network Authentication: none
  Encryption: wep128
  User VLAN: SKSPVlan
  Use Dynamic VLAN: no
  WEP Key 0: 3>:>?75<;50>?=6343:2=;9>44
  Default WEP Key: 0
  SSID in Beacon: on
No interfaces bound to this security profile

Profile Name: shared64wep
  ESSID Name: fz-shared-wep-64
  Dot11 Authentication: shared
  Network Authentication: none
Encryption: wep64
User VLAN: VSA-DKSP
Use Dynamic VLAN: yes
WEP Key 0: 3>:?>75<;5
Default WEP Key: 0
SSID in Beacon: on
Interfaces: 1
1:2:1,

Profile Name: shared128wep
ESS Name: fz-shared-wep-128
Dot11 Authentication: shared
Network Authentication: none
Encryption: wep128
User VLAN: VSA-DKSP
Use Dynamic VLAN: yes
WEP Key 0: 3>:?>75<;50>?:=6343:2=:;9>44
Default WEP Key: 0
SSID in Beacon: on

No interfaces bound to this security profile.

History
This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability
This command is available on Summit 300-48, Summit 300-24, Summit 400-24p and Alpine 3800 switches.
show source-ip-lockdown ports

    show source-ip-lockdown ports

Description
Displays the configuration of the source IP lockdown feature.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines

Example
The following command displays the configuration of the source IP lockdown feature:
show source-ip-lockdown ports

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms
show ssl

    show ssl {detail}

Description
Displays the Secure Sockets Layer (SSL) configuration.

Syntax Description

| detail | Specifies to display the information in detailed format. |

Default
N/A

Usage Guidelines
This command displays the following information:

- HTTPS port configured. This is the port on which the clients will connect.
- Result of a check to see whether the private key matches with the public key stored in the certificate.
- Length of RSA key (number of bits used to generate the private key).
- Basic information about the stored certificate

The optional keyword `detail` provides the same output as the `show ssl` command, plus the complete certificate. Private key (in PEM format) is displayed for users with administration privileges.

Examples
The following command displays the SSL configuration:

```plaintext
show ssl
```

The output of the command is similar to:

```
HTTPS Port Number: 443
Private Key matches the Certificate's public key.
RSA Key Length: 1026
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: md5WithRSAEncryption
        Issuer: C=us, O=93673, CN=extr
        Validity
             Not Before: Jul 23 14:00:07 2004 GMT
             Not After : Jul 23 14:00:07 2005 GMT
        Subject: C=us, O=93673, CN=extr
```
The following command displays the SSL configuration with the complete certificate.

```
show ssl
```

The output of the command is similar to:

```
HTTPS Port Number: 443
Private Key matches the Certificate's public key.
RSA Key Length: 1026
Certificate:
  Data:
    Version: 3 (0x2)
    Serial Number: 0 (0x0)
    Signature Algorithm: md5WithRSAEncryption
    Issuer: C=us, O=93673, CN=extr
    Validity
      Not Before: Jul 23 14:00:07 2004 GMT
      Not After : Jul 23 14:00:07 2005 GMT
    Subject: C=us, O=93673, CN=extr
    Subject Public Key Info:
      Public Key Algorithm: rsaEncryption
      RSA Public Key: (1026 bit)
      Modulus (1026 bit):
      Exponent: 65537 (0x10001)
      X509v3 extensions:
        X509v3 Basic Constraints: critical
        CA:TRUE
      Signature Algorithm: md5WithRSAEncryption
      af:3d:4c
    RSA Private key:
      -----BEGIN RSA PRIVATE KEY-----
      MIICXwIBAAKBgQOeadUPLzJVuMK0vRSNq1FDZ4VRuwPK1esd/HgqoHNKq/ILLJy5
      pvswa1W5V5p+b076H1Rh1PrIVjCS5x0uL5zcBn3qZ60ifqzd38N0V8SfqSvJP
      wxN/vp7Y+Sx4LahuUqeMgtA2KP8yUY8E80uxVM+CEuStkLW90cXzoWkIaQAB
      AoGBAIU0ryAX4aKXVkJdV5bOMCUIwKTqrbPqlpTazNKwVLrn5g5nJ3qj4DPMLLN
      /FIRCI07NYKw+3DPpLkAuuuzB0wWFvCHqfXw/7XOgeaifwEE0eZcYQOEtE+j+8d0sw
      sfuzrdMMLCJRZwAAVtv+a0oOSAPZ4HCthaiHwyk27aJY+bsJAkEB7osCIDLxCs+9
      jhG4/aSU5hEytDXgRrmhHVoveLeTJ0ssxK5xQf91WgmXewaj2zrK6G3yaHmT5d
      Re4A4V9PnBwfrd5d+0u+TzZNCaHSjSmey+ynXK/xZBLC8p16Vd/2d9kk4ykYjRQT
      wjWDZv2ogK1w8U38qKJe7wO2v5A16D9d2OCQPOQHq8mePP5tC/fx8acqppKxqgF4
      071Nvi9RQZ4R+3yL3zcPwyczOcvla6WHgU56eaXt:9ge+m/PHg08c4vpiCMBAxK4A
      -----END RSA PRIVATE KEY-----
```

ExtremeWare 7.5 Command Reference Guide 1059
History

This command was first available in ExtremeWare 6.2a.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e; it was added to the “i” series of switches in ExtremeWare 7.3.0.

Platform Availability

Beginning with ExtremeWare 7.4, this command is available in all platforms using SSH image except for the Summit “i” platform switches using SSH Base image (.SBxtr)
show tacacs

show tacacs {<ipaddress> | <hostname>}

Description
Displays the current TACACS+ configuration and statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the TACACS+ server for which information will be displayed (optional).</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name for the TACACS+ server for which information will be displayed.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The output from this command displays:
- The status of the TACACS+ authentication and accounting servers.
- The statistics for the configured primary and secondary servers.

If you specify the ipaddress option, configuration and statistics for that server are displayed.

Example
The following command displays TACACS+ client configuration and statistics:

```
show tacacs
```

The output from this command is similar to:

```
TACACS+: enabled
TACACS+ Authorization: enabled
TACACS+ Accounting: enabled
TACACS+ Server Connect Timeout sec: 3

Primary TACACS+ Server:
    Server name: 172.17.1.104
    IP address: 172.17.1.104
    Server IP Port: 49
    Client address: 172.17.1.220
    Shared secret: lf|nki

Secondary TACACS+ Server:
    Server name: 172.17.1.123
    IP address: 172.17.1.123
    Server IP Port: 49
    Client address: 172.17.1.220
    Shared secret: lf|nki

TACACS+ Acct Server Connect Timeout sec: 3
Primary TACACS+ Accounting Server:
```
Server name: 172.17.1.104
Client address: 172.17.1.220
Shared secret: lf\nki

Secondary TACACS+ Accounting Server:
Server name: 172.17.1.123
Client address: 172.17.1.220
Shared secret: lf\nki

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show tacacs-accounting

    show tacacs-accounting {{<ipaddress> | <hostname>}}

**Description**
Displays the current TACACS+ accounting client configuration and statistics.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the TACACS+ server for which accounting information will be displayed (optional).</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name for the TACACS+ server for which accounting information will be displayed.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The output from this command displays:
- The status of the TACACS+ accounting servers.
- The statistics for the configured primary and secondary servers.

If you specify the ipaddress option, configuration and statistics are displayed for that server.

**Example**
The following command displays TACACS+ accounting client configuration and statistics:
show tacacs-accounting

Following is the output from this command:

TACACS+ Accounting: enabled
TACACS+ Acct Server Connect Timeout sec: 3

Primary TACACS+ Accounting Server:
    Server name: 172.17.1.104
    IP address: 172.17.1.104
    Server IP Port: 49
    Client address: 172.17.1.220
    Shared secret: lf|nki

Secondary TACACS+ Accounting Server:
    Server name: 172.17.1.123
    IP address: 172.17.1.123
    Server IP Port: 49
    Client address: 172.17.1.220
    Shared secret: lf|nki
Security Commands

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show trusted-mac-address

show trusted-mac-address {vlan <vlan-name>} {port <portlist>}

Description
Displays the status of the enable and disable keywords before displaying all the configured trusted MAC addresses.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*?, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to display the status of the enabled and disabled keywords before displaying all of the configured trusted-MAC addresses.

Examples
The following command displays the status of the enable/disable keywords and then displays all of the configured trusted MAC addresses for all VLANs:

```plaintext
show trusted-mac-address
```

The following command displays trusted-MAC address information for the VLAN named corp:

```plaintext
show trusted-mac-address vlan corp
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show vlan security

    show vlan <vlan_name> security

Description
Displays information about dynamic MAC addresses on a VLAN.

NOTE
This command is available only on the “e” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_name</td>
<td>Specifies the name of the VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following example shows the security settings for a VLAN named vsa-dksp.

* S24-FZ:6 # show vlan vsa-dksp security
Port  Limit     State    Appeared Learnt Blackholed Locked
1     Unlimited Unlocked 7        7      0          0
2     Unlimited Unlocked 4        4      0          0
3     Unlimited Unlocked 0        0      0          0
4     Unlimited Unlocked 2        2      0          0
5     Unlimited Unlocked 0        0      0          0
6     Unlimited Unlocked 4        4      0          0
25    Unlimited Unlocked 13       13     0          0
26    Unlimited Unlocked 0        0      0          0
* S24-FZ:7 #

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the “e” series platforms only.
ssh2

ssh2 {cipher [3des | blowfish]} {port <portnum>} {compression [on | off]} {user <username>} {debug <debug_level>} {<username>@} [<host> | <ipaddress>] {<remote command>}

**Description**

Initiates an SSH2 client session to a remote SSH2 server.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3des</td>
<td>Specifies that the 3des cipher should be used for encryption. This is the default.</td>
</tr>
<tr>
<td>blowfish</td>
<td>Specifies that the blowfish cipher should be used for encryption.</td>
</tr>
<tr>
<td>portnum</td>
<td>Specifies the TCP port number to be used for communicating with the SSH2 client. Default is port 22.</td>
</tr>
<tr>
<td>compression</td>
<td>on specifies that data is to be compressed.</td>
</tr>
<tr>
<td></td>
<td>off specifies that compression is not to be used. Default is off.</td>
</tr>
<tr>
<td>username</td>
<td>Specifies a login name for the remote host, as an alternate to the user@host parameter.</td>
</tr>
<tr>
<td>debug_level</td>
<td>Specifies a debug level. Default is 0.</td>
</tr>
<tr>
<td>host</td>
<td>Specifies the name of the remote host.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the remote host.</td>
</tr>
<tr>
<td>remote command</td>
<td>Specifies a command to be passed to the remote system for execution. Remote commands are not supported on switches. This option is only valid if the remote system is a system, such as a UNIX workstation, that can accept remote commands.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

You must be running a security-enabled version of ExtremeWare 6.2.1 or later (which is under Export Control) in order to use the SSH2 client command.

SSH2 does not need to be enabled on the switch in order to use this command.

Typically this command is used to establish a secure session to a remote switch. You will be prompted for your password. Once you have logged in successfully, all ExtremeWare commands you enter will be executed on the remote switch. When you terminate the remote session, commands will then resume being executed on the original switch.

The remote command option cannot be used with Extreme Networks switches. If you include a remote command, you will receive an error message.

The default settings for SSH2 parameters are as follows:

- cipher—3DES
- port—22
Security Commands

- compression—off
- debug—0 (zero)

**Examples**

The following command establishes an SSH2 session on switch engineering1:

```
ssh2 admin@engineering1
```

The following command establishes an SSH2 session with the switch summit48i over TCP port 2050 with compression enabled:

```
ssh2 port 2050 compression on admin@summit48i
```

**History**

This command was first available in ExtremeWare 6.2.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
unconfigure auth mgmt-access

unconfigure auth mgmt-access

Description
Disables the remote authentication for management sessions.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
N/A

Example
unconfigure auth mgmt-access

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure auth netlogin

unconfigure auth netlogin

Description
Disables the remote authentication for netlogin sessions.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
N/A

Example
unconfigure auth netlogin

History
This command was first available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure cpu-dos-protect

**Description**
Resets the denial of service protection configuration to default parameter values.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A

**Usage Guidelines**
This command does not change whether denial of service protection is enabled or disabled. To enable or disable denial of service protection, use the following commands:

```
enable cpu-dos-protect
disable cpu-dos-protect
```

The default values for the denial of service protection parameters are as follows:

- alert-threshold—4000 packets per second
- notice-threshold—4000 packets per second
- timeout—15 seconds
- messages—on (messages are sent to syslog)
- filter-precedence—10

**Example**
The following command resets the denial of service protection configuration to the default values:

```
unconfigure cpu-dos-protect
```

**History**
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
unconfigure enhanced-dos-protect ipfdb agingtime

unconfigure enhanced-dos-protect ipfdb agingtime ports <portlist>

Description
Resets aging time configuration for enhanced denial of service protection to default values for the selected ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:, 2:5, 2:6-2:8. |

Default
The default aging time is 30 seconds.

Usage Guidelines
Use this command to reset aging time to default values for selected untrusted ports. To verify configuration, use the show enhanced-dos-protect ipfdb ports <portlist> command and view data in the Aging column.

Example
The following command resets the aging time on port 2 to the default value, 30 seconds:

unconfigure enhanced-dos-protect ipfdb agingtime ports 2

History
This command was first available in ExtremeWare 7.3.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure enhanced-dos-protect ipfdb cache-size

Description
Resets the cache size for enhanced denial of service protection to default parameter values.

Syntax Description
This command has no arguments or variables.

Default
The default cache size value is 256 (in kilobytes).

Usage Guidelines
Enhanced denial of service protection maintains the number of IPFDB entries according to the cache-size limit. Use this command to reset the cache size to the default of 256K.

Use the following command to set the cache-size to something other than the 256K default value:

```configure enhanced-dos-protect ipfdb cache-size```

Example
The following command resets the cache size to the 256K default value:

```unconfigure enhanced-dos-protect ipfdb cache-size```

History
This command was first available in ExtremeWare 7.3.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure enhanced-dos-protect ipfdb learn-limit

unconfigure enhanced-dos-protect ipfdb learn-limit ports <portlist>

Description
Resets the learning limit for enhanced denial of service protection to default parameter values for the selected ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8. |

Default
The default learn-limit on Fast Ethernet ports is 100 pkts/learn window. The default learn-limit on Gigabyte ports is 100 pkts/learn window.

Usage Guidelines
Use this command to reset to default the learning limit value that defines the number of packets to be counted before ExtremeWare can create an IPFDB entry in the hardware.

To configure the learning limit on untrusted ports for enhanced denial of service protection, use the following command:

configure enhanced-dos-protect ipfdb learn-limit

Usage Guidelines
Use this command to reset the learning limit value to the default number of packets being counted before the software can create an entry in hardware.

Example
The following command resets the learn limit on Fast Ethernet port 3 to 100 packets within the learning window before an IPFDB entry can be created:

unconfigure enhanced-dos-protect ipfdb learn-limit ports 3

History
This command was first available in ExtremeWare 7.3.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure enhanced-dos-protect ipfdb learn-window

unconfigure enhanced-dos-protect ipfdb learn-window ports <portlist>

Description
Resets the learning window on untrusted ports for the enhanced denial of service protection IPFDB learning qualifier to default values for the selected ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8. |

Default
The default learning window is 10 seconds.

Usage Guidelines
Use this command to reset the IPFDB learning window values for selected untrusted ports to the default value of 10 seconds. To verify configuration, use the show enhanced-dos-protect ipfdb ports <portlist> command.

Example
The following command resets the learning window on port 2 to the default value, 10 seconds:

unconfigure enhanced-dos-protect ipfdb learn-window ports 2

History
This command was first available in ExtremeWare 7.3.0.
This command was added to the Summit "e" series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure enhanced-dos-protect ports

unconfigure enhanced-dos-protect ports <portlist>

Description
 Resets the enhanced denial of service protection to the default trusted value for selected ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8. |

Default
 By default, ports are trusted.

Usage Guidelines
 Use this command to reset the enhanced denial of service protection to the default value for selected ports. The default value is trusted.

You can configure each port as trusted or untrusted by using the `configure enhanced-dos-protect ports` command. A trusted port behaves as a normal port. An untrusted port behaves according to the configuration parameter used in IPFDB thrashing.

Verify the status of each port by using the `show enhanced-dos-protect ports <portlist>` command.

Example
 The following command resets a range of ports to trusted, so that enhanced denial of service protection is not applied to ports 2 through 4:

```
unconfigure enhanced-dos-protect ports 2-4
```

History
 This command was first available in ExtremeWare 7.3.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
 This command is available on all platforms.
unconfigure enhanced-dos-protect rate-limit

unconfigure enhanced-dos-protect rate-limit [threshold | drop-probability | learn-window | protocol] ports <portlist>

Description
Removes ports from rate limiting or resets the rate limiting configuration for enhanced denial of service protection to default parameter values for the selected ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>Resets to the default value the number of packets allowed on a given port within the learning window before the rate limit is applied. The default on Fast Ethernet ports is 100 pkts/learn window. The default on Gigabyte ports is 100 pkts/learn window.</td>
</tr>
</tbody>
</table>
| drop-probability        | Resets to the default value the percentage of slow-path traffic to be dropped per port. The default value is 50 percent. |}
| learn-window            | Resets to the default value the number of seconds for the learning window per port. This value is the duration of time to be considered to reach the rate limit threshold. The default value is 10 seconds. |
| protocol [all | icmp] | Resets to the default value the protocol packets to which rate limiting is applied. By default, rate limiting is applied to Internet Control Message Protocol (ICMP) packets. |
| portlist                | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8. |

Default
Rate limiting is applied by default to ICMP packets.

Usage Guidelines
Use this command to remove ports from rate limiting, or reset the rate-limit threshold, drop probability, learning window, or packet protocol. To verify settings, use the show enhanced-dos-protect rate-limit command.

The default values for enhanced DoS protection rate limiting are as follows:

- threshold on Fast Ethernet ports—100 pkts/learn window
- threshold on Gigabyte ports—100 pkts/learn window
- drop-probability—50 percent
- learn-window—10 seconds

Examples
The following command resets the rate limiting threshold on Fast Ethernet port 3 to the default value, 100 packets:

unconfigure enhanced-dos-protect rate-limit threshold ports 3
The following command resets the rate limiting drop probability on port 4 to the default value, 50 percent:

```
unconfigure enhanced-dos-protect rate-limit drop-probability ports 4
```

The following command resets the rate limiting learn window on ports 2 and 3 to the default value, 10 seconds:

```
unconfigure enhanced-dos-protect rate-limit learn-window ports 2,3
```

The following command resets the rate limiting protocol to the default value, ICMP packet types, on ports 1 through 3:

```
unconfigure enhanced-dos-protect rate-limit protocol ports 1-3
```

The following command removes ports 1 through 4 from rate limiting:

```
unconfigure enhanced-dos-protect rate-limit ports 1-4
```

**History**

This command was first available in ExtremeWare 7.3.0.

This command was added to the Summit “e” series of switches in 7.3e.

**Platform Availability**

This command is available on all platforms.
unconfigure netlogin mac-address

unconfigure netlogin mac-address [<mac address> |default] mask <mask>

Description

Deletes MAC address/mask pairs from the table that is used for authentication in MAC-based network login.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>Used as the default entry password the supplicant's mac-address does not match any of the entries in the table.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies the network mask.</td>
</tr>
</tbody>
</table>

Default

By default, MAC-based authentication for network login is disabled.

Usage Guidelines

MAC-based RADIUS authentication uses the MAC address of the client for authentication. This feature is useful for devices that cannot function as 802.1x supplicants, such as IP phones. RADIUS is used as the transport protocol for authentication.

Only one default entry can be configured; this will be used if none of the configured entries match.

If a password is not configured locally, the MAC address is used as the password

Example

The following example deletes a MAC address/ mask pair from the table used for authentication:


History

This command was first available in ExtremeWare 740.

Platform Availability

This command is available on all platforms.
unconfigure netlogin mac auth-retry-count

Description
Returns the reauthentication retry count to the default value of 3.

Syntax Description
This command has no arguments or variables.

Default
The default number of retries is three.

Usage Guidelines
When a new MAC address is detected on a port enabled for MAC-based network login, an authentication message (RADIUS Access-Request message) is sent from the RADIUS client to the RADIUS server for validation. By default, the RADIUS client tries again a maximum of three times if the validation request fails. After the third retry, the authentication attempt times out. This command returns the retry count to its default value.

To set the authentication retry count to a number besides 3, use the following command

`configure netlogin mac auth-retry-count`

Example
The following command sets the retry count to its default value:

`unconfigure netlogin mac auth-retry-count`

History
This command was first available in ExtremeWare 740.

Platform Availability
This command is available on all platforms.
unconfigure netlogin mac reauth-period

Description
Returns the reauthentication interval for ports using MAC-based RADIUS authentication to the default value.

Syntax Description
This command has no arguments or variables.

Default
The default length of the reauthentication interval is 1800 seconds.

Usage Guidelines
While a port is in an authenticated state, the reauthentication mechanism periodically sends a RADIUS Access-Request message to the RADIUS server to reauthenticate the port. You can specify an interval in seconds between successive reauthentication messages. This command returns the interval to the default value of 1800 seconds.

Example
The following example sets the reauthentication period to 1800 seconds (the default):

unconfigure netlogin mac reauth-period

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
unconfigure radius

    unconfigure radius {server [primary | secondary] {<host name> | <ipaddress>}}

Description
Removes the RADIUS client configuration.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Unconfigures the primary RADIUS server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Unconfigures the secondary RADIUS server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the server being unconfigured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the server being unconfigured.</td>
</tr>
</tbody>
</table>

Default
Unconfigures both the primary and secondary authentication servers.

Usage Guidelines
None

Example
The following command unconfigures the secondary RADIUS server for the client:

    unconfigure radius server secondary

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure radius-accounting

unconfigure radius-accounting {server [primary | secondary] {[<host name> | <ipaddress>]]}

Description
Removes the RADIUS accounting client configuration.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Unconfigures the primary RADIUS accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Unconfigures the secondary RADIUS accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the server being unconfigured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the server being unconfigured.</td>
</tr>
</tbody>
</table>

Default
Unconfigures both the primary and secondary accounting servers.

Usage Guidelines
None

Example
The following command unconfigures the secondary RADIUS accounting server for the client:

unconfigure radius-accounting server secondary

History
This command was first available in ExtremeWare 4.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure tacacs

For the “i” switches:

unconfigure tacacs {server [primary | secondary]}

For the “e” switches:

unconfigure tacacs {
[primary | secondary] {server [<ipaddress> | <hostname>]} }

Description
Removes the TACACS+ client configuration.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Unconfigures the primary TACACS+ server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Unconfigures the secondary TACACS+ server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the server being unconfigured.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “e” series switches.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the server being unconfigured.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “e” series switches.</td>
</tr>
</tbody>
</table>

Default
Unconfigures both the primary and secondary TACACS+ servers.

Usage Guidelines
None

Example
The following command unconfigures all TACACS+ servers for the client:

unconfigure tacacs

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure tacacs-accounting

For the “i” switches:

    unconfigure tacacs-accounting {server [primary | secondary]}

For the “e” switches:

    unconfigure tacacs-accounting {[primary | secondary] server {<ipaddress> | <hostname>}}

**Description**

Removes the TACACS+ accounting client configuration.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Unconfigures the primary TACACS+ accounting server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Unconfigures the secondary TACACS+ accounting server.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the server being unconfigured.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the server being unconfigured.</td>
</tr>
<tr>
<td>NOTE:</td>
<td>This option is available only on the “e” series switches.</td>
</tr>
</tbody>
</table>

**Default**

Unconfigures both the primary and secondary TACACS+ accounting servers.

**Usage Guidelines**

None

**Example**

The following command unconfigures all TACACS+ accounting servers for the client:

    unconfigure tacacs-accounting

**History**

This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
unconfigure vlan dhcp-address-range

unconfigure vlan <vlan-name> dhcp-address-range {<start-addr>}

Description
Clears the specified DHCP address range in a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be unconfigured.</td>
</tr>
<tr>
<td>dhcp-address-range</td>
<td>Specifies that DHCP address range to be unconfigured.</td>
</tr>
<tr>
<td>start-addr</td>
<td>(Optional) Specifies the starting address of the DHCP address range to be unconfigured.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to unconfigure, or clear, the specified DHCP address in a VLAN.

A VLAN can have multiple DHCP address ranges; therefore, the start-addr parameter identifies the DHCP address range for which the clearing needs to be done.

The DHCP address range is identified as the one whose starting IP address is the same as start-addr. If start-addr is not provided, then the primary DHCP address range will be unconfigured.

Examples
Consider a VLAN named test with a primary subnet 40.0.0.x/24 and a secondary subnet 50.0.0.x/24. Assume that for the primary subnet a DHCP address range is configured ranging from 40.0.0.5 to 40.0.0.40. Similarly, for the secondary subnet the DHCP address range is configured ranging from 50.0.0.5 to 50.0.0.40.

To unconfigure the DHCP address range of the primary subnet, use the following command:
unconfigure vlan test dhcp-address-range

To unconfigure the DHCP address range with the start-addr as 50.0.0.5, use the following command
unconfigure vlan test dhcp-address-range 50.0.0.5

NOTE
You can configure multiple DHCP address ranges for a VLAN. The start-addr option in the command (50.0.0.5 in this example) specifies the exact DHCP address range for which the command applies. If the last option is not specified, the command is applied for the primary subnet.
History
This command has been modified so that clearing of the secondary or remote address ranges is possible (through the addition of the parameter `start-addr`). This enhanced command was made available in ExtremeWare 7.3.0. and ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure vlan dhcp-options

   unconfigure vlan <vlan-name> dhcp-options {<start-addr>}

Description
Clears the DHCP options for the specified address range in a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN to be unconfigured.</td>
</tr>
<tr>
<td>dhcp-options</td>
<td>Specifies that DHCP options are to be unconfigured.</td>
</tr>
<tr>
<td>start-addr</td>
<td>(Optional) Specifies the starting address of the range for which DHCP options are to be unconfigured.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to unconfigure, or clear, the DHCP options for the specified address range in a VLAN.

A VLAN can have multiple DHCP address ranges; therefore, the start-addr parameter identifies the DHCP address range that requires clearing of DHCP options.

The DHCP address range is identified as the range whose starting IP address is the same as start-addr. If start-addr is not provided, then the DHCP options for the primary address range will be cleared.

To configure DHCP options for the specified address range in a VLAN, use the following command:
configure vlan dhcp-options

Examples
Consider a VLAN named test with a primary subnet 40.0.0.x/24 and a secondary subnet 50.0.0.x/24. Assume that for the primary subnet a DHCP address range is configured ranging from 40.0.0.5 to 40.0.0.40.

Similarly, for the secondary subnet the DHCP address range is configured ranging from 50.0.0.5 to 50.0.0.40. Assume that for the DHCP Address range 40.0.0.5 to 40.0.0.40 the DHCP gateway is configured as 40.0.0.90. Similarly, assume that for the DHCP address range 50.0.0.5 to 50.0.0.40 the DHCP gateway is configured as 50.0.0.90.

To unconfigure the DHCP options for the primary subnet, use the following command:
unconfigure vlan test dhcp-options

To unconfigure the DHCP options for the DHCP address range starting from 50.0.0.5, use the following command:
unconfigure vlan test dhcp-options 50.0.0.5
**NOTE**

You can configure multiple DHCP address ranges for a VLAN. The `start-addr` option in the command (50.0.0.5 in this example) specifies the exact DHCP address range for which the command applies. If the last option is not specified, the command is applied for the primary subnet.

**History**

This command has been modified so that clearing the DHCP options for secondary or remote subnets is possible (through the addition of the parameter `start-addr`). This enhanced command was made available in ExtremeWare 7.3.0 and ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
This chapter describes the following commands:

- Commands related to downloading and using a new switch software image
- Commands related to saving, uploading, and downloading switch configuration information
- Commands related to the BootROM and switch rebooting
- Commands related to downloading and using a new Altitude 300 Access Point software image

The switch software image file contains the executable code that runs on the switch. An image comes preinstalled from the factory. The image can be upgraded by downloading a new version from a Trivial File Transfer Protocol (TFTP) server on the network.

A switch can store up to two images, a primary and a secondary image. You can download a new image into either one of these areas, and you can select which image will load on the next switch reboot.

The configuration is the customized set of parameters that you have selected to run on the switch. As you make configuration changes, the new settings are stored in run-time memory. To retain the settings, and have them load when you reboot the switch, you must save the configuration to nonvolatile storage.

A switch can store two different configurations, a primary and a secondary configuration. You can select the configuration area to which you want the changes saved, and which configuration will be used on the next switch reboot.

The BootROM initializes certain important switch variables during the switch boot process. In specific situations, the BootROM can be upgraded by download from a TFTP server on the network.

The Altitude 300 Access Point (AP) is shipped with installed bootstrap and boot loader images. When it is installed, it obtains its runtime image from the switch or from a TFTP server.
configure configuration-mode

configure configuration-mode <standard | enhanced>

Description
Configures the default startup configuration for the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>standard</td>
<td>Specifies the standard default configuration mode, in which ExtremeWare starts the switch with all ports in forwarding mode. The default configuration mode is the standard mode.</td>
</tr>
<tr>
<td>enhanced</td>
<td>Specifies the enhanced default configuration mode, in which ExtremeWare starts the switch with all ports disabled. The default configuration mode is the standard mode.</td>
</tr>
</tbody>
</table>

Default
The standard mode is the default configuration mode.

Usage Guidelines
This command configures the default startup configuration for the switch. To remove an enhanced mode configuration and reset the configuration to the default standard configuration mode, use the unconfigure configuration-mode command.

Example
The following command sets the default startup configuration for the switch to enhanced mode, in which the switch will start up with all ports disabled:

```
configure configuration-mode enhanced
```

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on all platforms.
configure download server

configure download server [primary | secondary] [<ip address> | <hostname>] <filename>

Description
Configures the TFTP server(s) used by a scheduled incremental configuration download.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Specifies that the following parameters refer to the primary TFTP server.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies that the following parameters refer to the secondary TFTP server.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the TFTP server from which the configuration should be obtained.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the hostname of the TFTP server from which the configuration should be obtained.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the filename on the server that contains the configuration to be downloaded.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command must be executed before scheduled configuration downloads can be performed.

Use of the hostname parameter requires that DNS be enabled.

A secondary TFTP server is only used as a back up server when the primary server fails.

Example
The following command specifies that scheduled incremental downloads into the primary configuration space be done from the server named tftphost, from the ASCII file primeconfig.txt (residing in directory \configs\archive on the server).

```
configure download server primary tftphost \configs\archive\prime_config.txt
```

History
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure switch

configure switch {auto | extended | standard}

Description

Configures the mode of switch operation for the Alpine 3802 switch.

NOTE

This command is available only on the Alpine 3802 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Specifies the mode of switch operation to be auto mode.</td>
</tr>
<tr>
<td>extended</td>
<td>Specifies the mode of switch operation to be extended mode.</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies the mode of switch operation to be standard mode</td>
</tr>
</tbody>
</table>

Default

Auto mode

Usage Guidelines

The Alpine 3802 switch supports all existing Alpine I/O modules; however, there are limitations to the number and type of I/O modules supported, based upon the mode of switch operation.

The Alpine 3802 has three modes of switch operation:

- Extended—In extended mode, all slots (slots 1, 2, and 3) are enabled. Slot 1 supports all existing Alpine I/O modules: Alpine Ethernet I/O modules (modules with a green stripe on the front of the module) and Alpine Access I/O modules (modules with a silver stripe on the front of the module). Slots 2 and 3 support only Alpine Access I/O modules (silver stripe).
  The Extended mode LED lights when the switch is in extended mode.

- Standard—In standard mode, only slots 1 and 2 are enabled. Slot 3 is disabled. Slots 1 and 2 support all existing Alpine I/O modules: Alpine Ethernet I/O modules (green stripe) and Alpine Access I/O modules (silver stripe).
  The Standard mode LED lights when the switch is in extended mode.

- Auto—In auto mode, the switch determines if it is in standard or extended mode depending upon the type of modules installed in the chassis or the slot preconfigurations. If an Alpine I/O module with a green stripe (for example, an FM-32Ti module) is installed or preconfigured in slot 2, the switch operates in standard mode. If an Alpine I/O module with a silver stripe (for example, a WM-4Ti module) is installed or preconfigured in slots 2 or 3, the switch operates in extended mode.

Slot 3 can accept only Alpine Access I/O modules (silver stripe). You cannot insert an Alpine Ethernet I/O module (green stripe) into slot 3.

If you insert a module into the Alpine 3802 that is not allowed in a particular slot, the switch logs an error to the syslog. For example, if you insert a GM-WDMi module into slot 3, a module type not supported in slot 3, the switch logs an error.
**Example**

The following command specifies that the Alpine 3802 operates in standard mode.
```
configure switch standard
```

**History**

This command was first available in ExtremeWare 6.1.8.

**Platform Availability**

This command is available on the Alpine 3802 switch only.
configure wireless ports image

configure wireless ports [<portlist> | all] image [bootstrap | bootloader | runtime] [<ip address> | <hostname>] [<hostname/ip address> <filename>]

Description
Use this command to configure the image location for a wireless port.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| all      | Specifies all ports. |
| bootstrap | Specifies the bootstrap image. |
| bootloader | Specifies the bootloader image |
| runtime | Specifies the runtime image |
| ip address | Specifies the IP address of the TFTP server. |
| hostname | Specifies the hostname of the TFTP server. |
| hostname/filename | Specifies the path for the file on the server that contains the specified image. |
| filename | Specifies the name of the file on the server that contains the specified image. |

Default
By default the image location and path information are set to null.

Usage Guidelines
To configure Direct Connect ports, use the IP address of the wireless management VLAN for Direct Connect ports.

To configure Remote Connect ports, use the IP address of the VLAN that the Remote Connect APs are members of. This may not be the same as the wireless management VLAN.

A wireless port cannot be enabled if you have not configured runtime parameters for it.

Example
The following example configures a wireless port to download its image files from the TFTP server called tftphost at IP address 10.12.123.1:

```plaintext
configure wireless ports 1:1 image bootstrap tftphost/10.12.123.1 ABS-1_8_0.bin
configure wireless ports 1:1 image bootloader tftphost/10.12.123.1 ABL-1_11_2.bin
configure wireless ports 1:1 image runtime tftphost/10.12.123.1 ART-7_5_8.bin
```

History
This command was first available in ExtremeWare 7.5.
Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine switches.
download bootrom

For the “i” switches:
   download bootrom [<ip address> | <hostname>] <filename> {slot <slot>}

For the “e” switches:
   download bootrom [<ip address> | <hostname>] <filename>

Description
Downloads a BootROM image from a TFTP server after the switch has booted. The downloaded image replaces the BootROM in the onboard FLASH memory.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the TFTP server.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the hostname of the TFTP server.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies name of the file on the server that contains the bootROM image.</td>
</tr>
<tr>
<td>slot</td>
<td>Specifies the slot where a PoS or MPLS module is installed.</td>
</tr>
</tbody>
</table>

**NOTE:** This option is available only on the “i” series of switches.

Default
N/A

Usage Guidelines
Upgrade the BootROM only when asked to do so by an Extreme Networks technical representative.

If this command does not complete successfully it could prevent the switch from booting. In the event the switch does not boot properly, some boot option functions can be accessed through a special BootROM menu (see Chapter 12, “Configuration and Image Commands” in the ExtremeWare Software User Guide.

Use of the hostname parameter requires that DNS be enabled.

Example
The following command downloads a bootROM image from the tftp server called tftphost from the file bootimages (residing in directory \images on the server):

download bootrom tftphost \images\bootimage

History
This command was first available in ExtremeWare 4.0.
This command was modified in the ExtremeWare IP Services Technology Release based on 6.1.8b12 to support download to a PoS or MPLS module.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
download configuration

download configuration [<ip address> | <hostname>] <filename> {incremental}

Description
Downloads a previously saved ASCII configuration file from a specific TFTP server host.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the TFTP server from which the configuration should be obtained.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the hostname of the TFTP server from which the configuration should be obtained.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the path and filename of a saved ASCII configuration.</td>
</tr>
<tr>
<td>incremental</td>
<td>Specifies an incremental configuration download (v 6.0 or later).</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Unless you specify the incremental keyword, this command does a complete download, resetting the current switch configuration and replacing it with the new downloaded configuration. You will be prompted to reboot the switch after the download is complete. If you do not reboot when prompted, the switch views the configuration file as corrupted and the next time you reboot the switch prompts you to reset to the factory defaults.

The new configuration information is stored in switch run-time memory, and is not retained if the switch has a power failure. After the switch has rebooted, you should save the configuration to the primary or secondary configuration area to retain it through a power cycle. You can include a save command at the end of the configuration file to have the save done at the end of the download.

The file on the server is assumed to be located relative to the TFTP server base directory. You can specify a path as part of the file name.

Use of the hostname parameter requires that DNS be enabled.

Use the incremental keyword to specify an incremental or partial configuration download. In this case, the commands specified in the incremental download file are executed, but configuration settings not specified in the file are left intact. No reboot is required.

Examples
The following command clears the current switch configuration, and downloads a new full configuration from the TFTP server called tftphost. It uses the configuration from the file stdconfig.txt residing in the subdirectory configs\archive of the TFTP server base directory on the server:

download configuration tftphost configs\archive\stdconfig.txt

The following command downloads a partial configuration from the TFTP server called tftphost from the file modifyconfig.txt (residing in the subdirectory configs\archive on the server):

download configuration tftphost configs\archive\modifyconfig.txt incremental
download configuration

**History**
This command was first available in ExtremeWare 2.0.

Support for the `hostname` parameter was introduced in ExtremeWare 4.0.

Support for incremental downloads was introduced in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
download configuration cancel

download configuration cancel

Description
Cancels a scheduled incremental configuration download.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command cancels the scheduled download command completely, not just the next scheduled daily download. The download configuration every <hour> command must be issued again to resume automatic downloads.

If no downloads are scheduled, this command has no effect.

Example
The following command cancels a previously scheduled download:

download configuration cancel

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
download configuration every

    download configuration every <time>

**Description**
Automatically does an incremental configuration download every day at the specified time, or immediately after switch bootup, based on the parameters specified in the `configure download server` command.

**Syntax Description**

| time          | The time of day in the format <hour (0-23)>:<minutes (0-59)>.

**Default**
N/A

**Usage Guidelines**
You must run the `configure download server` command before using this command, to specify:

- The TFTP server and the configuration file from which the downloaded configuration will be obtained.
- Whether this TFTP server is the primary server or the secondary (backup) TFTP server.

**Example**
The following commands set up a scheduled incremental download of the file `config_info.txt`, to be done from the TFTP server named `tftphost` into the primary configuration area, every day at 10:00 pm:

```
configure download server primary tftphost config_info.txt
download configuration every 22:00
```

**History**
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
download file-name

download file-name <ipaddress/hostname> <filename>

Description
Downloads a new Altitude 300 access point image file to a switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress/hostname</td>
<td>Specifies the IP address and host name of the server that contains the image.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the path and name of the file on the server that contains the image.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Image software for the Altitude 300 access point consists of bootstrap, boot loader, and runtime image files. Current bootstrap and boot loader files are installed on the AP before it is shipped.

To upgrade Remote Connect APs, download the new AP image files to the switch being used as the attachment switch for the APs.

To upgrade Direct Connect APs, download the new AP image files to the switch with the physical connection to the APs.

Examples
The following command downloads the AP image file ABS-1_8_0.bin from the TFTP server named tftphost at IP address 10.12.123.1:

download file-name 10.12.123.1/tftphost ABS-1_8_0.bin

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
download image

```
download image [<hostname> | <ipaddress>] <filename> {primary | secondary}
```

**Description**
Downloads a new version of the ExtremeWare software image.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Specifies the hostname of the TFTP server from which the image should be obtained.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of TFTP server from which the image should be obtained.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies the filename of the new image.</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies that the new image should be stored as the primary image.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies that the new image should be stored as the secondary image.</td>
</tr>
</tbody>
</table>

**Default**
Stores the downloaded image in the current location (the location used for the last reboot).

**Usage Guidelines**
Before downloading an image, you must place the new image in a file on a TFTP server on your network. Unless you include a path with the filename, this command assumes that the file resides in the same directory as the TFTP server itself.

The switch can store up to two images: a primary image and a secondary image. When you download a new image, you must select the image space (primary or secondary) into which you want the new image to be placed. If no parameters are defined, the software image is saved to the selected image, that is, the next boot-up image.

Use of the `hostname` parameter requires that DNS be enabled.

For ExtremeWare 7.1.0 and higher, the following features are available on the Alpine and BlackDiamond chassis:

- You can update the operational images for all installed modules that run a software image. All of the operational image files must be located in the same directory on the TFTP server and they must have the same filename prefix.

- The main ExtremeWare image always downloads first.

  The download image process proceeds with each slot starting at slot 1.
  - If the main ExtremeWare image cannot be found, the download image process is discontinued.
  - If a specific image file is not found for a specific module, an error is displayed and the download process continues to the next module.

- Slots with modules that do not support separate operational images (for example, the G8Xi or the GM-4Ti module) are skipped.

Table 18 lists the modules and operational images supported in ExtremeWare 7.1.0.
Examples

The following command downloads the switch software image from the TFTP server named tftphost, from the file named s4119b2.xtr, to the secondary image store:

download image tftphost s4119b2.xtr secondary

The following example assumes that you have a modular chassis with modules installed. This command downloads the switch and module software images from the TFTP server named tftphost from the filename prefix named v710b35, to the primary image store:

download image tftphost all-images v710b35 primary

The following sample log is displayed:

MSM A Primary bank:  Downloading image v710b35.xtr
.................................................................
Verifying the image...
Done!
Slot 2 Primary bank:  Downloading image v710b35.oc3
.................................................................
Download to slot 2 successful.
Slot 3 Primary bank:  Downloading image v710b35.mpls
.................................................................
Download to slot 3 successful.
Slot 4 Primary bank:  Downloading image v710b35.oc3
.................................................................
Download to slot 4 successful.
Slot 7 Primary bank:  Downloading image v710b35.atm3

Table 18:  Supported modules and operational images

<table>
<thead>
<tr>
<th>Module Name</th>
<th>Image Extension</th>
<th>Image Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MSM, SMMi</td>
<td>xtr</td>
<td>ExtremeWare image</td>
</tr>
<tr>
<td>MSM</td>
<td>Gxtr</td>
<td>6816 ExtremeWare image</td>
</tr>
<tr>
<td>MSM, SMMi</td>
<td>Sxtr</td>
<td>SSH ExtremeWare image</td>
</tr>
<tr>
<td>MSM</td>
<td>SGxtr</td>
<td>SSH 6816 ExtremeWare image</td>
</tr>
<tr>
<td>ARM</td>
<td>arm</td>
<td>ARM image</td>
</tr>
<tr>
<td>A3cSi</td>
<td>atm3</td>
<td>ATM OC-3 image</td>
</tr>
<tr>
<td>P3cSi, P3cMi</td>
<td>oc3</td>
<td>PoS OC-3 image</td>
</tr>
<tr>
<td>P12cSi, P12cMi</td>
<td>oc12</td>
<td>PoS OC-12 image</td>
</tr>
<tr>
<td>MPLS</td>
<td>mpls</td>
<td>MPLS image</td>
</tr>
<tr>
<td>WM-4E1i</td>
<td>e1</td>
<td>E1 WAN image</td>
</tr>
<tr>
<td>WM-4T1i</td>
<td>t1</td>
<td>T1 WAN image</td>
</tr>
<tr>
<td>WM-1T3i</td>
<td>t3</td>
<td>T3 WAN image</td>
</tr>
</tbody>
</table>
Download to slot 7 successful.

The following example assumes that you have a modular chassis with modules installed. This command downloads the security switch and module software images from the TFTP server named tftphost from the filename prefix named v700b68, to the secondary image store:

download image tftphost all-images v700b68 image-type ssh secondary

The following sample log is displayed:

MSM  A  Secondary bank:  Downloading image v700b68.xtr

Download to slot 2 successful.

Slot 2  Secondary bank:  Downloading image v700b68.oc3

Download to slot 3 successful.

Slot 3  Primary   bank:  Downloading image v700b68.mpls

Download to slot 4 successful.

Slot 4  Secondary bank:  Downloading image v700b68.oc3

Download to slot 7 successful.

History
This command was available in ExtremeWare 2.0.

Support for the hostname parameter was introduced in ExtremeWare 4.0.

Support for the slot parameter was introduced in ExtremeWare 7.0.0.

Support for the filename_prefix parameter was introduced in ExtremeWare 7.1.0.

Support for the non-ssh and ssh keywords was introduced in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
**download image hostname filename**

`download image hostname filename {primary | secondary} [slot <slot-id-list>]`

**Description**
Downloads a new version of the ExtremeWare software image.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Specifies that the new image should be stored as the primary image.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies that the new image should be stored as the secondary image.</td>
</tr>
<tr>
<td>slot-id-list</td>
<td>Specifies that the new image should be stored on one or more switches in a stack. The slot ID is the number of the switch in the stack.</td>
</tr>
</tbody>
</table>

**Default**
Stores the downloaded image in the current location (the location used for the last reboot).

**Usage Guidelines**
This command downloads images to the appropriate slot. If the primary or secondary information is not given, then the image is downloaded to the applicable slots or active partition.

Use the `show slot` command to find the discovered members, their operational and configured platform-types and the ports that are active or inactive on them.

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
save configuration

save configuration {primary | secondary} [slot <slot-id-list> | all ]

Description

Saves the run-time configuration of the specified devices to an area in non-volatile memory.

Syntax Description

| primary  | Specifies the primary saved configuration of a switch. If this switch is a stack, it is the configuration of the current slot. |
| secondary| Specifies the secondary saved configuration. |
| slot-id-list | Stack-enabled switches only |
| all      | Stack-enabled switches only |

Specifies to save the run-time configuration of one or more switches in a stack. The slot ID is the number of the switch in the stack.

Specifies to save all configurations (stack manager and all stack members).

Default

Saves the current configuration to the location used on the last reboot. If the switch is a member of a stack, the default is all.

Usage Guidelines

Use this command to save the run time configuration of the specified switch to non-volatile memory.

Because of differences in the CPU, the Summit 200 series switches take longer than other Extreme switches to save configuration data.

Stacked Switches Only.  In a stacked configuration, you can save the configuration of the members, the stack manager only, or of all the members and the stack manager. The configuration takes effect on the next reboot.

Example

The following command saves the current switch configuration in the secondary configuration area:

```
save configuration secondary
```

This command saves the run-time configuration of an entire stack in the primary configuration area:

```
save configuration primary all
```

The following command saves the current switch configuration in the primary configuration area of a manager on a stack of switches:

```
save configuration primary
```

This command saves the current switch configuration in the primary configuration area for a stack member:
save configuration slot 4 primary

**History**

This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.4 to support stacking.
Support for the all and slot keywords was added in ExtremeWare 7.4.

**Platform Availability**

This command is available on all platforms. The slot, master, and all parameters are only supported on the Summit 200, Summit 300-24, and Summit 400 switches for stacking.
show configuration

    show configuration [detail]

Description
Displays the currently active configuration to the terminal.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to show all configuration statements including default commands.</td>
</tr>
</tbody>
</table>

Usage Guidelines
If the output scrolls off the top of the screen, you can use the `enable clipaging` command to pause the display when the output fills the screen. The default for clipaging is enabled.

**NOTE**

After you use the `unconfigure switch all` command, the `show configuration` output displays the VLAN default without any ports assigned. The ports still belong to the VLAN default, as the `show vlan` output correctly displays.

Example
This command shows the current configuration active in the switch:

```
show configuration detail
```

History
This command was available in ExtremeWare 2.0.

This command was modified to show the auto-negotiation status of Gigabit Ethernet ports in ExtremeWare 6.2.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

The command was modified in ExtremeWare 7.2e to support the `detail` keyword.

Platform Availability
This command is available on all platforms.
show wireless ports img-configuration

    show wireless ports [ <portlist> | all] img-configuration

Description
This command shows the image configuration details for the specified wireless ports.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use this command to show the image configuration details for the specified wireless ports.

Examples
The following example displays the image configuration information for all the wireless ports:

    show wireless ports all img-configuration

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
synchronize

Description
Replicates all saved images and configurations from the master MSM to the slave MSM on the BlackDiamond switch.

NOTE
This command is available only on the BlackDiamond switch.

Syntax Description
This command has no arguments or variables.

Usage Guidelines
This command does the following:
1. Copies both the primary and secondary software images
2. Copies both the primary and secondary configurations
3. Copies the BootROM
4. Reboots the slave MSM

When you install a slave MSM, you are not prompted to synchronize the images and the configurations from the master. If not synchronized, the slave uses its image and the master’s configuration. This image/configuration mismatch will likely cause the switch to operate differently after failover. Use the synchronize command to replicate all saved images and configurations from the master to the slave. However, if one of the configurations on the master MSM is empty, the sync process will not overwrite the corresponding configuration on the slave. If the configuration on the slave MSM is an older configuration, this can cause problems if the switch is rebooted using the outdated configuration.

This command does not replicate the run-time configuration. You must use the save command to store the run-time configuration first.

Example
The following command replicates all saved images and configurations from the master MSM to the slave MSM:
synchronize

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on the BlackDiamond switch only.
unconfigure configuration-mode

unconfigure configuration-mode

Description
Removes the effect of the default startup configuration currently defined for the switch, resetting the configuration mode to the standard configuration mode.

Syntax Description
This command has no arguments or variables.

Default
The standard mode is the default configuration mode.

Usage Guidelines
Use this command on “i” series switches to remove an enhanced mode configuration and reset the configuration to the default standard configuration mode.

To configure the default startup configuration for the switch, use the configure configuration-mode command.

Example
The following command removes the effect of the default startup configuration currently defined for the switch, resetting the configuration mode to the standard configuration mode:

unconfigure configuration-mode

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on all platforms.
unconfigure switch

On the “i” series switches:

    unconfigure switch {all} {enhanced}

On the “e” series switches:

    unconfigure switch {all}

Description

Returns the switch configuration to its factory default settings.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies that the entire current configuration should be erased, and the switch rebooted.</td>
</tr>
</tbody>
</table>
| enhanced  | Specifies that the entire current configuration should be erased with the exception of the default configuration mode, which will be set to enhanced. In enhanced mode, the switch boots with all ports disabled. 

NOTE: This option applies only to the “i” series switches.

Default

Resets configuration to factory defaults without reboot.

Usage Guidelines

Use the unconfigure switch command to reset the configuration to factory defaults, but without erasing the configuration and rebooting. This preserves user account information such as date and time settings.

Include the parameter all to clear the entire current configuration, including all switch parameters, and reboot using the last used image and configuration.

On the “i” series switches, include the parameter enhanced to clear the entire current configuration, with the exception of the default configuration mode, which will be set to enhanced. In enhanced mode, the switch boots with all ports disabled. If the enhanced parameter is not entered, the default configuration mode will be reset to the standard mode, in which the switch boots with all ports in forwarding mode. To configure the default startup configuration for the switch, use the configure configuration-mode command.

NOTE

After using the unconfigure switch all command, the show configuration output displays the VLAN default without any ports assigned. The ports still belong to the VLAN default, as the show vlan output correctly displays.

Example

The following command erases the entire current configuration, resets to factory defaults, and reboots the switch using the last specified saved image and saved configuration:

    unconfigure switch all
History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
This command was modified to include the enhanced parameter in ExtremeWare 7.3.0.

Platform Availability
This command is available on all platforms.
unconfigure wireless ports image-configuration

unconfigure wireless ports <portlist | all> img-configuration [bootstrap } bootloader | runtime | all]

Description
This command unconfigures the image configuration for the specified wireless port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports, an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>bootstrap</td>
<td>Specifies the bootstrap image file.</td>
</tr>
<tr>
<td>bootloader</td>
<td>Specifies the bootloader image file.</td>
</tr>
<tr>
<td>runtime</td>
<td>Specifies the runtime image file.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all image files.</td>
</tr>
</tbody>
</table>

Usage Guidelines
Use this command to unconfigure one or all image files for the specified wireless port or ports.

You cannot unconfigure the runtime configuration of a wireless port that is enabled. You must disable the port first.

Examples
The following command unconfigures the bootloader image for port 1:18 on the Summit 300-48:

unconfigure wireless ports 1:18 img-configuration bootloader

History
This command was introduced in ExtremeWare 7.5.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
upload configuration

    upload configuration [<ip address> | <hostname>] <filename> {every <time>}

Description

Uploads the current configuration to a TFTP server on your network.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the TFTP server.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the hostname of the TFTP server.</td>
</tr>
<tr>
<td>filename</td>
<td>Specifies a name for the file where the configuration is to be saved.</td>
</tr>
<tr>
<td>time</td>
<td>The time of day in the format &lt;hour (0-23)&gt;:&lt;minutes (0-59)}.</td>
</tr>
</tbody>
</table>

Default

Uploads the current configuration immediately.

Usage Guidelines

The filename can be up to 255 characters long, and cannot include any spaces, commas, quotation marks, or special characters. Unless you include a path with the filename, this command places the file in the same directory as the TFTP server itself.

The uploaded ASCII file retains the command-line interface (CLI) format. This allows you to do the following:

- Modify the configuration using a text editor, and later download a copy of the file to the same switch, or to one or more different switches.
- Send a copy of the configuration file to Extreme Networks Technical Support for problem-solving purposes.

If every <time> is specified, the switch automatically saves the configuration to the server once per day, at the specified time. Because the filename is not changed, the configured file stored in the TFTP server is overwritten every day.

For version 4.0:

- The keyword every is not supported. Specify the time immediately after the filename.

For version 6.0 or later:

- The keyword every is required if a time is specified.

To cancel automatic upload, use the cancel option. If no options are specified, the current configuration is uploaded immediately.

Use of the hostname parameter requires that DNS be enabled.
Example
The following command uploads the current configuration to the file configbackup.txt on the TFTP server named tftphost, every night at 10:15 p.m.:

upload configuration tftphost configbackup.txt every 22:15

History
This command was available in ExtremeWare 2.0.
Support for the <hostname> parameter was introduced in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
upload configuration cancel

    upload configuration cancel

Description
Cancels a previously scheduled configuration upload.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command cancels the scheduled upload command completely, not just the next scheduled daily upload. You must re-issue the `upload configuration every <hour>` command to resume automatic uploads.

If no uploads are scheduled, this command has no effect.

Example
The following command cancels the current automatic upload schedule:

    upload configuration cancel

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
use configuration

use configuration [primary | secondary]

Description
Configures the switch to use a previously saved configuration on the next reboot.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Specifies the primary saved configuration.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies the secondary saved configuration.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The keyword configuration can be abbreviated to config.

Example
The following command specifies that the next reboot should use the primary saved configuration:

use configuration primary

History
This command was available in ExtremeWare 2.0.

Support for the slot parameter was introduced in ExtremeWare 7.0.0. The <slot> parameter is applicable to the Alpine and BlackDiamond chassis.

Support for the all keyword was introduced in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Support for the slot and all keywords was removed in ExtremeWare 7.4.

Platform Availability
This command is available on all platforms.
use image

use image [primary | secondary]

Description
Configures the switch to use a saved image on the next reboot.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>primary</td>
<td>Specifies the primary saved software image.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies the secondary saved software image.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you issue the unconfigure switch all command, you will still have the last configured value of the use image command; it can be either a primary or secondary image.

Example
The following command configures the switch to use the primary image on the next reboot:

use image primary

History
This command was first available in ExtremeWare 2.0.
Support for the slot parameter was introduced in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
If you encounter problems when using your switch, ExtremeWare troubleshooting commands can help identify and solve the problem. Use these commands only under the guidance of Extreme Networks technical personnel.

You can contact Extreme Networks technical support at (800) 998-2408 or (408) 579-2826.

The Event Management System (EMS), introduced in ExtremeWare 7.1.0, provides enhanced features to filter and capture information generated on a switch. The various systems in ExtremeWare are being converted to EMS components. As a system is converted, the corresponding debug trace command is no longer available. Details of using EMS are discussed in the ExtremeWare User Guide, in the chapter “Status Monitoring and Statistics”, and the commands used for EMS are detailed in this document in Chapter 10, “Commands for Status Monitoring and Statistics”.

Until all the systems in ExtremeWare are converted, you may need to use a mix of EMS and debug trace commands under the guidance of Extreme Networks technical personnel.

Included in this chapter, as well as in Chapter 10, are the EMS commands to enable and disable debug mode for EMS components.

The debug trace commands require the CPU; therefore, if CPU utilization is high, use these commands sparingly. Disable any external syslog before you configure a debug trace, because the debug trace utility can send large amounts of information to the syslog, and if your syslog is external, that information travels over your network. Alternatively, you can configure a filter to select only the most necessary information.

Configure a debug trace at lower levels first, and look for obvious problems. Higher levels typically record so much information that they record enough information within a few seconds.
clear debug-trace

Description
Resets the debug-trace levels to the factory settings of level 0.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command resets the debug-trace levels to level 0:

clear debug-trace

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace accounting

configure debug-trace accounting <debug level>

Description
This command provides system-level debug tracing for the accounting subsystem.

NOTE
This command is available on the ARM and MPLS modules on the BlackDiamond switches and on the "e" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records critical error messages, such as memory allocation errors. Indicates a severe event that can terminate or corrupt accounting.</td>
</tr>
<tr>
<td>1</td>
<td>Records warning messages for various non-critical error conditions.</td>
</tr>
<tr>
<td>2</td>
<td>Records various informational messages.</td>
</tr>
<tr>
<td>3</td>
<td>Records debug information, such as message and event processing. Provides additional information to support engineers for the purpose of diagnosing network problems.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for accounting to 3:

```
configure debug-trace accounting 3
```

Following is the log output at this level for switches in the “i” series:

```
<DBG:NPAPI> Slot6 NP_KRT_GET_DSB_COUNTS responses from both NPs
<DBG:NPAPI> Slot6 genpipe: received DSA message GET_COUNTS
<DBG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DBG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB) (Accounting)
<DBG:DSA> Vlan vlan1 Vlan ID 4091
<DBG:DSA> processDSBMessage: rsp type 2 from slot 6
<DBG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DBG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB) (Accounting)
<DBG:DSA> Vlan vlan0 Vlan ID 4092
<DBG:DSA> processDSBMessage: rsp type 2 from slot 6
```
<DEBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DEBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DEBUG:DSA> Vlan Mgmt Vlan ID 4094
<DEBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DEBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DEBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DEBUG:DSA> Vlan MacVlanDiscover Vlan ID 4095
<DEBUG:DSA> processDSBMessage: rsp type 2 from slot 6
<DEBUG:DSA> (npGenPipe)sendMsg: 0x8093f70c sends to slot 5, len=68
<DEBUG:DSA> npGenPipeAllocTCB: TCB allocated by Accounting (DSB)(Accounting)
<DEBUG:DSA> Vlan Default Vlan ID 1
<DEBUG:DSA> All Vlan

History
This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on the ARM and MPLS modules on the BlackDiamond platform and on the “e” series platforms.
configure debug-trace bootprelay

configure debug-trace bootprelay <debug level> vlan <vlan name>

**Description**
This command records debug information to the syslog.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug level</td>
<td>Specifies a debug level:</td>
</tr>
<tr>
<td>0</td>
<td>None.</td>
</tr>
<tr>
<td>1</td>
<td>Records error messages and tracks BOOTP messages relayed.</td>
</tr>
<tr>
<td>2</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>3</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
The default level is 0.

**Usage Guidelines**
The **debug level** range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

**Example**
The following command sets the reporting level for BOOTP relay errors to 3:

```bash
configure debug-trace bootprelay 3
```

**History**
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure debug-trace card-state-change

configure debug-trace card-state-change <debug level>

Description
This command is not currently supported.

Syntax Description
<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>1</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>2</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>3</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>4</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>5</td>
<td>Not currently supported.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
This command is not currently supported.

Example
This command is not currently supported.

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace debug-link

configure debug-trace debug-link <debug level>

Description
This command records debug information to the syslog.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disables debug tracing for debug link and stops recording information to the syslog.</td>
</tr>
<tr>
<td>1</td>
<td>Enables debug tracing for debug link and records information to the syslog.</td>
</tr>
<tr>
<td>2</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>3</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Level 0 disables the debug-trace for link detection, and level 1 enables debug-trace for link detection.

For levels 2 through 5, no additional information is recorded.

Example
The following command enables debug-trace for link detection:

```
configure debug-trace debug-link 1
```

The following command disables debug-trace for link detection:

```
configure debug-trace debug-link 0
```

History
This command was first available in ExtremeWare 6.2.2b108.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace dvmrp-cache

configure debug-trace dvmrp-cache <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

vlan name Specifies a VLAN name.

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Use this command to trace the detailed process of adding, deleting, and modifying a multicast cache. The IP multicast cache is a hardware forwarding entry identified by a ptag index number. The following command displays the cache entries:

```
show ipmc cache [detail] <IP multicast group>
```

The trace is based on the ingress VLAN of a cache. Use this tool if the egress list of a cache is incorrect, if there are missing cache entries, or if the DVMRP task has been intermittently suspended.

Example
The following command sets the reporting level for DVMRP cache errors to 3:

```
configure debug-trace dvmrp-cache 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-cache 4 vlan v49
<DEBUG:DVMR> dvcareq.c 698: Remove Cache for (192.168.3.0,224.2.127.254)
<DEBUG:DVMR> dvcareq.c 698: Remove Cache for (192.168.3.0,239.1.1.1)
```
configure debug-trace dvmrp-cache

<DBG:DVMR> dvcareq.c 213: Build Cache for (192.168.3.10,239.1.1.1)
<DBG:DVMR> dvcareq.c 213: Build Cache for (192.168.3.10,224.2.127.254)
<DBG:DVMR> dvcareq.c 596: dvmrp mask del interface 6 in 239.1.1.1/192.168.3.0/255.255.255.0
<DBG:DVMR> dvcareq.c 213: Build Cache for (192.168.3.10,224.10.253.4)

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on “i” platforms only.
configure debug-trace dvmrp-hello

configure debug-trace dvmrp-hello <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

| vlan name   | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all DVMRP probe messages coming into a VLAN. Use this command if switches connected to a common network have problems establishing or maintaining normal neighbor relationships.

Example
The following command sets the reporting level for DVMRP hello errors to 3:
configure debug-trace dvmrp-hello 3 vlan v49

Following is the log output at this level:

<INFO:SYST> serial admin: configure debug-trace dvmrp-hello 4 vlan v49
<DEBUG:DVMR> dvr.x.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DEBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49). Len=16, nbr=1.
<DEBUG:DVMR> dvr.x.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DEBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49). Len=16, nbr=1.
<DEBUG:DVMR> dvr.x.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
<DEBUG:DVMR> dvnbr.c 612: Tx Hello on Vlan(v49). Len=16, nbr=1.
<DEBUG:DVMR> dvr.x.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)
configure debug-trace dvmrp-hello

DBUG:DVMR> dvmbr.c 612: Tx Hello on Vlan(v49). Len=16, nbr=1.
DBUG:DVMR> dvrx.c 151: Rx Hello from 192.168.200.2 on VLAN(v49)

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on "i" platforms only.
configure debug-trace dvmrp-message

configure debug-trace dvmrp-message <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

vlan name Specifies a VLAN name.

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the DVMRP system messages (prune, graft, and graft acknowledgement) coming into a VLAN. Use this command if a multicast stream cannot be stopped, or does not come down to the receiver after the IGMP snooping entry is verified.

Example
The following command sets the reporting level for DVMRP message errors to 3:

configure debug-trace dvmrp-message 3 vlan v49

Following is the log output at this level:

<INFO:SYST> last message repeated 2 times
<INFO:SYST> serial admin: disable dvmrp
<DEBUG:DVMR> DVMRP task stopped.

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on "i" platforms only.
configure debug-trace dvmrp-neighbor

configure debug-trace dvmrp-neighbor <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

default level | Specifies a debug level:

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — Records error messages.</td>
<td></td>
</tr>
<tr>
<td>1 — Records warnings.</td>
<td></td>
</tr>
<tr>
<td>2 — Records verbose warnings.</td>
<td></td>
</tr>
<tr>
<td>3 — Displays a dump of each packet.</td>
<td></td>
</tr>
<tr>
<td>4 — No additional information recorded.</td>
<td></td>
</tr>
<tr>
<td>5 — No additional information recorded.</td>
<td></td>
</tr>
</tbody>
</table>

vlan name | Specifies a VLAN name.

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record
the messages recorded at lower levels.

This command traces the state of all DVMRP neighbors on a common VLAN to monitor when a
neighbor is added or deleted.

Example
The following command sets the reporting level for DVMRP neighbor errors to 3:

configure debug-trace dvmrp-neighbor 3 vlan v49

Following is the log output at this level:

<INFO:SYST> serial admin: enable dvmrp
<DEBUG:DVMR> dvmbr.c 149: Add new Nbr 192.168.200.2 on Vlan (v49). Len=16

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on "i" platforms only.
configure debug-trace dvmrp-route

configure debug-trace dvmrp-route <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

| vlan name | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command records all DVMRP route report messages coming into a VLAN. Use this command if the DVMRP routing table is incorrect or unstable.

Example
The following command sets the reporting level for DVMRP route errors to 3:

```
configure debug-trace dvmrp-route 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-route 3 vlan v49
<DEBUG:DVMR> dvr.x.c 159: Rx Report from 192.168.200.2 in VLAN(v49)
<DEBUG:DVMR> dvr.x.c 298: Rx route 10.1.2.0/24 Metric 0.1 from 192.168.200.2
<DEBUG:DVMR> dvr.trx.c 330: Replace RT (10.1.2.0/24 Metrix=1). Flag=01/4
<DEBUG:DVMR> dvr.x.c 298: Rx route 192.168.3.0/24 Metric 1.1 from 192.168.200.2
<DEBUG:DVMR> dvr.trx.c 330: Replace RT (192.168.3.0/24 Metrix=1). Flag=01/4
<DEBUG:DVMR> dvr.x.c 298: Rx route 192.168.1.3/32 Metric 1.1 from 192.168.200.2
<DEBUG:DVMR> dvr.trx.c 330: Replace RT (192.168.1.3/32 Metrix=1). Flag=01/4
```
<DBUG:DVMR> dvrttx.c 339: Trigger RT(10.1.2.0/24 metric=34) to Vlan(v49).
<DBUG:DVMR> dvrttx.c 339: Trigger RT(192.168.3.0/24 metric=34) to Vlan(v49).
<DBUG:DVMR> dvrttx.c 339: Trigger RT(192.168.1.3/32 metric=34) to Vlan(v49).
<DBUG:DVMR> dvrttx.c 496: Tx trigger report on VLAN(v49). Len=27
<DBUG:DVMR> dvrx.c 159: Rx Report from 192.168.200.2 in VLAN(v49)
<DBUG:DVMR> dvrx.c 298: Rx route 10.1.2.0/24 Metric 0.1 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.3.0/24 Metric 1.1 from 192.168.200.2
<DBUG:DVMR> dvrx.c 330: Replace RT (10.1.2.0/24 Metric=0). Flag=00/0
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.1.3/32 Metric 1.1 from 192.168.200.2
<DBUG:DVMR> dvrx.c 330: Replace RT (192.168.1.3/32 Metric=1). Flag=00/0
<DBUG:DVMR> dvrttx.c 492: Tx periodic report on VLAN(v49). Len=49
<DBUG:DVMR> dvrx.c 159: Rx Report from 192.168.200.2 in VLAN(v49)
<DBUG:DVMR> dvrx.c 298: Rx route 172.17.1.0/24 Metric 1.34 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.2.0/30 Metric 0.34 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.100.0/30 Metric 1.34 from 192.168.200.2
<DBUG:DVMR> dvrx.c 298: Rx route 192.168.1.1/32 Metric 1.34 from 192.168.200.2

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on "i" platforms only.
configure debug-trace dvmrp-timer

configure debug-trace dvmrp-timer <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

| vlan name | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for DVMRP timer errors to 3:

```
configure debug-trace dvmrp-timer 3 vlan v49
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace dvmrp-timer 3 v49
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace eaps-system

configure debug-trace eaps-system <debug level>

**Description**
This command records debug information to the syslog.

**NOTE**
*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug level</td>
<td>Specifies a debug level:</td>
</tr>
<tr>
<td>0 —</td>
<td>Records software bugs and severe errors.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warning messages.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records changes in state, such as a failure, and changes in port status, such as a port going down.</td>
</tr>
<tr>
<td>3 —</td>
<td>Records events that do not cause a state change and basic debug information, such as failed PDU transmission, disabled or unconfigured ports, or inactive links.</td>
</tr>
<tr>
<td>4 —</td>
<td>Records frequently occurring events, such as timers expiring, and detailed debug information, such as sending or receiving PDUs, VLAN ID and EAPS domain of each PDU, and configuration values.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
The default level is 0.

**Usage Guidelines**
The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

**Example**
The following command sets the reporting level for EAPS errors to 3:

```bash
configure debug-trace eaps-system 3
```

Following is the log output at this level:

```
<INFO:SYST> serial admin: configure debug-trace eaps-system 0
<DEBUG:EAPS> eaps_runtime.c 1673: Complete state unchanged, EAPS="man1"
<DEBUG:EAPS> eaps_runtime.c 931: Pdu="Health-Pdu", EAPS="man1" [MAC=00:01:33:14:00], RcvdSeq#=14851, CurrSeq#
<DEBUG:EAPS> eaps_runtime.c 852: pdu="Health-Pdu"
<DEBUG:EAPS> eaps_runtime.c 843: [DEBUG] vlanId=10, eapsdInst=0
<DEBUG:EAPS> eaps.c 520: [DEBUG] Found Control Vlan. EapsInst=0
<DEBUG:EAPS> eaps.c 368: [DEBUG] Wowie!! Received EAPS_PDU_MSG
```
Troubleshooting Commands

This command was first available in ExtremeWare 6.1.9.

Platform Availability
This command is available on“i” platforms only.
configure debug-trace flow-redirect

configure debug-trace flow-redirect <debug level>

Description
This command records debug information to the syslog.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>None.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records configuration changes and unexpected code states.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records next-hop resources becoming active or inactive.</td>
</tr>
<tr>
<td>3 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for flow redirect errors to 2:

```
configure debug-trace flow-redirect 2
```

Following is the log output at this level:

```
<INFO:IPRT> redirect next hop http1 30.0.0.9 changed to up
<DBG:SYST> i=1 Changing Nexthop fg=fffc Source=24.3.89.150 Nexthop=30.0.0.6 Nfg=fffb
<DBG:SYST> i=0 Changing Nexthop fg=fffc Source=24.3.89.149 Nexthop=30.0.0.5 Nfg=ffffa
<DBG:SYST> i=4 Changing Nexthop fg=fffc Source=24.3.89.148 Nexthop=30.0.0.9 Nfg=ffff
<DBG:SYST> i=3 Changing Nexthop fg=fffc Source=24.3.89.147 Nexthop=30.0.0.8 Nfg=fffe
<DBG:SYST> i=2 Changing Nexthop fg=fffc Source=24.3.89.146 Nexthop=30.0.0.7 Nfg=ffffd
<DBG:SYST> i=1 Changing Nexthop fg=fffc Source=24.3.89.145 Nexthop=30.0.0.6 Nfg=ffffb
<DBG:SYST> i=0 Changing Nexthop fg=fffc Source=24.3.89.144 Nexthop=30.0.0.5 Nfg=ffffa
<DBG:SYST> Sag=fffc
<DBG:SYST> Grps0 = fffa fffbf fffdf ffef ffff 0 0 0
<DBG:SYST> rLBS inst=0 inUse=1 SA=24.3.89.144 sMask=ffffffff 8 dPort=50
<DBG:SYST> Looking for entries to balance in redirect 3
<DBG:SYST> Looking for entries to balance in redirect 2
<DBG:SYST> Looking for entries to balance in redirect 1
<DBG:SYST> Looking for entries to balance in redirect 0
<INFO:IPRT> redirect next hop http1 30.0.0.8 changed to up <DBG:SYST> Balancing group ffff
```
Troubleshooting Commands

This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace flowstats

configure debug-trace flowstats <debug level>

Description
This command records debug information to the system log.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages, such as cannot open a socket, cannot bind a socket, or cannot add or remove a flow from health-check.</td>
</tr>
<tr>
<td>1 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>2 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>3 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>Displays informational messages, such as adding or deleting a flow collector.</td>
</tr>
<tr>
<td>6 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>7 —</td>
<td>Displays debug messages such as enabling and disabling ping-check, IP address of flow collector, and port, flow collector, and flow group information for each packet, as well as a packet dump.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for flowstats errors to 3:

```
configure debug-trace flowstats 3
```

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is available on”i” platforms only.
configure debug-trace health-check

configure debug-trace health-check [<debug level> | {filter [real | virtual] <ip address> | ftp | http | https | imap4 | ldap | nntp | pop3 | smtp | socks | telnet | tftp | web | wildcard | www | <tcp port number>}]}

**Description**

This command records debug information to the syslog.

**NOTE**

This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>filter</th>
<th>Specifies a filter.</th>
</tr>
</thead>
<tbody>
<tr>
<td>real</td>
<td>Specifies a real IP address.</td>
</tr>
<tr>
<td>virtual</td>
<td>Specifies a virtual IP address.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address.</td>
</tr>
<tr>
<td>ftp</td>
<td>Specifies FTP messages.</td>
</tr>
<tr>
<td>http</td>
<td>Specifies HTTP messages.</td>
</tr>
<tr>
<td>https</td>
<td>Specifies HTTPS messages.</td>
</tr>
<tr>
<td>imap4</td>
<td>Specifies IMAP4 messages.</td>
</tr>
<tr>
<td>ldap</td>
<td>Specifies LDAP messages.</td>
</tr>
<tr>
<td>nntp</td>
<td>Specifies NNTP messages.</td>
</tr>
<tr>
<td>pop3</td>
<td>Specifies POP3 messages.</td>
</tr>
<tr>
<td>smtp</td>
<td>Specifies SMTP messages.</td>
</tr>
<tr>
<td>socks</td>
<td>Specifies SOCKS messages.</td>
</tr>
<tr>
<td>telnet</td>
<td>Specifies Telnet messages.</td>
</tr>
<tr>
<td>tftp</td>
<td>Specifies TFTP messages.</td>
</tr>
<tr>
<td>web</td>
<td>Specifies HTTP messages.</td>
</tr>
<tr>
<td>wildcard</td>
<td>Specifies messages from all services.</td>
</tr>
<tr>
<td>www</td>
<td>Specifies HTTP messages.</td>
</tr>
<tr>
<td>debug level</td>
<td>Specifies a debug level:</td>
</tr>
<tr>
<td>0</td>
<td>Records unable to initialize or add a health check due to unavailable internal resources (memory, tasks, sockets, timers, or queues).</td>
</tr>
<tr>
<td>1</td>
<td>Records resources becoming active or inactive, unexpected code states, and internal resources unavailable.</td>
</tr>
<tr>
<td>2</td>
<td>Records resources added to or removed from health-check, configuration parameters updated, and individual health-check activity.</td>
</tr>
<tr>
<td>3</td>
<td>Records more verbose health-check activity and debug messages.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>
Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Health-check debug messages apply to all resources tracked by health-check. The messages recorded are in addition to messages you have configured for other features.

You can define a filter to limit the debug messages logged. Before you define a filter, you must configure the debug level. To define a filter, you must do the following:

1. Specify a real or virtual IP address. You can specify both a real and virtual IP address in the same command line. An IP address of 0.0.0.0 will match any IP address. Messages without associated IP addresses are logged regardless of the filters you define.

2. Specify a port or service. A service of wildcard or a port of 0 will match any service or port number.

The filter limits the recorded messages to those concerning the IP addresses and services you specify. If you do not configure a filter, debug-trace records messages at the debug level you specify for every service on every IP address.

When you save your configuration, you also save your configured filter values.

Example
The following command enables level 2 debug-tracing:

```
configure debug-trace health-check 2
```

The following command then configures a filter for a specific server and service:

```
configure debug-trace health-check filter real 1.2.3.4 : http
```

This configuration logs health-check debug messages at levels 0, 1, and 2 for the following:

- Generic health-check messages
- ping-check for IP address 1.2.3.4
- tcp-port-check for IP 1.2.3.4 port 80 (HTTP)
- service-check for IP 1.2.3.4 port 80 (including any virtual servers that use SLB pool member 1.2.3.4 port 80)

Alternate Example
The following command enables level 2 debug-tracing:

```
configure debug-trace health-check 2
```

The following command configures a filter that provides all of the information in the preceding example, and also logs service-checks specifically for the SLB virtual server (5.6.7.8 port 80) that references SLB pool member 1.2.3.4 port 80:

```
configure debug-trace health-check filter real 1.2.3.4 : http virtual 5.6.7.8 : http
```
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on "i" platforms only.
configure debug-trace iparp

configure debug-trace iparp <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

Syntax Description

<table>
<thead>
<tr>
<th>debug</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records IP and ARP conflicts, and duplicate IP addresses.</td>
</tr>
<tr>
<td>1</td>
<td>Records the following errors:</td>
</tr>
<tr>
<td></td>
<td>• ARP interface down</td>
</tr>
<tr>
<td></td>
<td>• No bridge for router interface</td>
</tr>
<tr>
<td></td>
<td>• No free new entry</td>
</tr>
<tr>
<td></td>
<td>• Filter out multicast and broadcast source address</td>
</tr>
<tr>
<td></td>
<td>• Header too short</td>
</tr>
<tr>
<td></td>
<td>• ARP Ethernet/IP</td>
</tr>
<tr>
<td></td>
<td>• Invalid hw/prot length</td>
</tr>
<tr>
<td></td>
<td>• Wrong length</td>
</tr>
<tr>
<td>2</td>
<td>Records the following errors:</td>
</tr>
<tr>
<td></td>
<td>• Router interface down</td>
</tr>
<tr>
<td></td>
<td>• Bad IP destination</td>
</tr>
<tr>
<td></td>
<td>• No mbuf available</td>
</tr>
<tr>
<td></td>
<td>• Failed to ARP</td>
</tr>
<tr>
<td></td>
<td>• SubVLAN proxy ARP disabled, replied, or ARPing</td>
</tr>
<tr>
<td></td>
<td>NOTE: This error is supported only on the “I” series switches.)</td>
</tr>
<tr>
<td></td>
<td>• No bridge available</td>
</tr>
<tr>
<td></td>
<td>• No ARP available</td>
</tr>
<tr>
<td></td>
<td>• No router interface in ARPT</td>
</tr>
<tr>
<td></td>
<td>• Loopback entry created</td>
</tr>
<tr>
<td></td>
<td>• Suppressed re-ARP</td>
</tr>
<tr>
<td></td>
<td>• New ARP entry for IP/MAC address</td>
</tr>
<tr>
<td></td>
<td>• Filtering own ARP</td>
</tr>
<tr>
<td></td>
<td>• Target matched primary, secondary, or backup</td>
</tr>
<tr>
<td>3</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

vlan name  Specifies a VLAN name.

Default
The default level is 0.
Usage Guidelines

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example

The following command sets the reporting level for IP ARP errors to 3:

```
configure debug-trace iparp 3
```

Following is the log output at this level:

```
<DBG:SYS> arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBG:SYS> arpresolve: START ac=0x82f3d6e0 m=0x849a6800 IP=192.168.192.12
<DBG:SYS> arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBG:SYS> arpresolve: START ac=0x82f3d6e0 m=0x849a6c00 IP=192.168.192.12
<DBG:SYS> arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBG:SYS> arpresolve: START ac=0x82f3d6e0 m=0x849a6c00 IP=192.168.192.12
<DBG:SYS> arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<DBG:SYS> arpresolve: START ac=0x82f3d6e0 m=0x849a6800 IP=192.168.192.12
<DBG:SYS> arpresolve: Filled entry for (192.168.192.12,00:00:86:54:7f:2a)
<INFO:SYST> serial admin: configure debug-trace iparp 3 t2
<INFO:SYST> Port 2:1 link active 100Mbs FULL duplex
<INFO:SYST> serial admin: configure t2 add ports 2 : 1
<INFO:SYST> serial admin: configure t2 delete ports 1 : 1
<INFO:SYST> serial admin: enable ipforwarding t2
<INFO:SYST> serial admin: configure t2 ipaddress 192.168.192.1 / 24
<INFO:SYST> serial admin: configure t2 add ports 1 : 1
```

History

This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
configure debug-trace ipxgns-message

configure debug-trace ipxgns-message <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — None.</td>
<td></td>
</tr>
<tr>
<td>1 — None.</td>
<td></td>
</tr>
<tr>
<td>2 — Verifies that IPX GNS messages are being sent and received.</td>
<td></td>
</tr>
<tr>
<td>3 — Verifies the contents of the messages.</td>
<td></td>
</tr>
<tr>
<td>4 — No additional information recorded.</td>
<td></td>
</tr>
<tr>
<td>5 — No additional information recorded.</td>
<td></td>
</tr>
</tbody>
</table>

| vlan name | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for IPX GNS message errors to 3:

```
configure debug-trace ipxgns-message 3
```

Following is the log output at this level:

```
<DBUG:XAP> SAP Traverse: Stuffing entry into packet
<DBUG:XAP> SAP Traverse: Ignoring type 0278
<DBUG:XAP> SAP Traverse: Ignoring type 026b
<DBUG:XAP> SAP Traverse: Ignoring type 0640
<DBUG:XAP> SAP Traverse: Ignoring type 0278
<DBUG:XAP> SAP Traverse: Ignoring type 026b
<DBUG:XAP> SAP Traverse: Ignoring type 0640
<DBUG:XAP> type 0004 net: 3646f895 mac: 00:90:27:a1:44:3c socket: 1105
<DBUG:XAP> SAP Traverse: Stuffing entry into packet
<DBUG:XAP> last message repeated 9 times
<DBUG:XAP> Rcv bcast GNS type(3) from f0003606, 00:a0:c9:59:a4:5e for service=0x4
```
History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace ipxrip-message

configure debug-trace ipxrip-message <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

dep level  Specifies a debug level:
0 — None.
1 — None.
2 — Verifies that ipxrip messages are being sent and received.
3 — Verifies the contents of the messages.
4 — Displays a dump of each packet.
5 — No additional information recorded.

vlan name  Specifies a VLAN name.

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for IPX RIP message errors to 4:
configure debug-trace ipxrip-message 4

Following is the log output at this level:

<INFO:SYST> serial admin: configure debug-trace ipxrip-message 4 ipxvlan
<INFO:SYST> Log cleared
<INFO:SYST> serial admin: clear log
<DBG:KERN> 0x0881347d82: 00 03
<DBG:KERN> 0x0881347d72: 00 02 00 00 36 12 00 01 00 01 00 00 10 69 00 02
*****6********i**
<DBG:XRIP> Sending Rsp msg to f0001964:ff:ff:ff:ff:ff len 18
<DBG:XRIP> Added entry net 1069 hops 2 ticks 3 to rsp
<DBG:XRIP> Added entry net 3612 hops 1 ticks 1 to rsp
<INFO:EAPS> eaps_runtime.c 1426: State Change, Failed -> Complete, EAPS="man1"
<INFO:EAPS> eaps_runtime.c 277: Primary Port Change, Down -> Up
Troubleshooting Commands

INFO:SYST> Port 1:2 link active 1000Mbs FULL duplex
DEBUG:KERN> 0x0881347d82: 00 03
DEBUG:KERN> 0x0881347d72: 00 02 00 00 36 12 00 01 00 01 00 00 10 69 00 02
*****6************i**
DEBUG:X RIP> Sending Rsp msg to f0001964:ff:ff:ff:ff:ff:len 18
DEBUG:X RIP> Added entry net 1069 hops 2 ticks 3 to rsp
DEBUG:X RIP> Added entry net 3612 hops 1 ticks 1 to rsp
INFO:EAPS> eaps_runtime.c 1449: State Change, Complete -> Failed, EAPS="man1"
INFO:EAPS> eaps_runtime.c 1018: Pdu="Link-Down-Pdu", EAPS="man1"
[MAC=00:01:30:32:ef:00]
INFO:EAPS> eaps_runtime.c 303: Primary Port Change, Up -> Down
INFO:SYST> Port 1:2 link down

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on "i" platforms only.
configure debug-trace ipxrip-route

configure debug-trace ipxrip-route <debug level>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None.</td>
</tr>
<tr>
<td>1</td>
<td>None.</td>
</tr>
<tr>
<td>2</td>
<td>Displays route additions and deletions.</td>
</tr>
<tr>
<td>3</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for IPX RIP route errors to 2:
configure debug-trace ipxrip-route 2

Following is the log output at this level:

<DEBUG:XRIP> Added route to net f0220666 g/w f001964:00:01:30:32:8d:00, hops 2, tics 2
<INFO:SYST> Log cleared

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace ipxsap-entry

configure debug-trace ipxsap-entry <debug level>

Description
This command is not currently supported.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>1</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>2</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>3</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>4</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>5</td>
<td>Not currently supported.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
This command is not currently supported.

Example
This command is not currently supported.

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace ipxsap-message

configure debug-trace ipxsap-message <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug level</td>
<td>Specifies a debug level:</td>
</tr>
<tr>
<td></td>
<td>0 — None.</td>
</tr>
<tr>
<td></td>
<td>1 — None.</td>
</tr>
<tr>
<td></td>
<td>2 — Verifies that IPX SAP messages are being sent and received.</td>
</tr>
<tr>
<td></td>
<td>3 — Verifies the contents of the messages.</td>
</tr>
<tr>
<td></td>
<td>4 — Displays a dump of each packet.</td>
</tr>
<tr>
<td></td>
<td>5 — No additional information recorded.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for IPX SAP message errors to 3:

```
configure debug-trace ipxsap-message 3
```

Following is the log output at this level:

```
<INFO:USER> admin logged in through console
<DBG:XSAP> Generating SAP query (opcode=0001, svc type=ffff)
<INFO:SYST> Port 2:1 link active 100Mbs FULL duplex
<INFO:SYST> Port 2:1 link down
<INFO:SYST> User admin logged out from console
<INFO:SYST> Log cleared
<INFO:SYST> serial admin: clear log
```

History
This command was first available in ExtremeWare 6.1.
Platform Availability
This command is available on "i" platforms only.
configure debug-trace isis-cli

    configure debug-trace isis-cli <level>

Description
Controls logging of debug messages related to CLI actions.

**NOTE**
This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level. Following are the debug levels:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Critical/Error Messages</td>
</tr>
<tr>
<td>1 —</td>
<td>Warning Messages</td>
</tr>
<tr>
<td>2 —</td>
<td>Concise Messages</td>
</tr>
<tr>
<td>3 —</td>
<td>Verbose Messages</td>
</tr>
<tr>
<td>4 —</td>
<td>Packet Dumps</td>
</tr>
</tbody>
</table>

**Default**
The default is 0.

**Usage Guidelines**
The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

**History**
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available only on the “i” series platforms.
configure debug-trace isis-event

configure debug-trace isis-event <level>

Description
Controls logging of debug messages related to miscellaneous actions.

NOTE
This command is available only on the “i” series switches.

Syntax Description

debug level Specifies a debug level. Following are the debug levels:

<table>
<thead>
<tr>
<th>debug level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Critical/Error Messages</td>
</tr>
<tr>
<td>1</td>
<td>Warning Messages</td>
</tr>
<tr>
<td>2</td>
<td>Concise Messages</td>
</tr>
<tr>
<td>3</td>
<td>Verbose Messages</td>
</tr>
<tr>
<td>4</td>
<td>Packet Dumps</td>
</tr>
</tbody>
</table>

Default
The default is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace isis-hello

configure debug-trace isis-hello <level> vlan [<vlan name> | all]

Description
Controls logging of debug messages related to sending and receiving, and decoding and encoding of Hello messages.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level. Following are the debug levels:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Critical/Error Messages</td>
</tr>
<tr>
<td>1 —</td>
<td>Warning Messages</td>
</tr>
<tr>
<td>2 —</td>
<td>Concise Messages</td>
</tr>
<tr>
<td>3 —</td>
<td>Verbose Messages</td>
</tr>
<tr>
<td>4 —</td>
<td>Packet Dumps</td>
</tr>
</tbody>
</table>

| vlan name   | Specifies a VLAN name.                                  |

Default
The default is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on "i" platforms only.
configure debug-trace isis-lsp

configure debug-trace isis-lsp <level>

**Description**

Controls logging of debug messages related to sending and receiving and decoding and encoding of LSP Messages.

**NOTE**

This command is available only on the “i” series switches.

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>debug level</strong></th>
<th>Specifies a debug level. Following are the debug levels:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Critical/Error Messages</td>
</tr>
<tr>
<td>1 —</td>
<td>Warning Messages</td>
</tr>
<tr>
<td>2 —</td>
<td>Concise Messages</td>
</tr>
<tr>
<td>3 —</td>
<td>Verbose Messages</td>
</tr>
<tr>
<td>4 —</td>
<td>Packet Dumps</td>
</tr>
</tbody>
</table>

**Default**

The default is 0.

**Usage Guidelines**

The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on “i” platforms only.
configure debug-trace isis-snp

configure debug-trace isis-snp <level>

Description
Controls logging of debug messages related to sending and receiving, and decoding and encoding of PSNP and CSNP Messages.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level. Following are the debug levels:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Critical/Error Messages</td>
</tr>
<tr>
<td>1 —</td>
<td>Warning Messages</td>
</tr>
<tr>
<td>2 —</td>
<td>Concise Messages</td>
</tr>
<tr>
<td>3 —</td>
<td>Verbose Messages</td>
</tr>
<tr>
<td>4 —</td>
<td>Packet Dumps</td>
</tr>
</tbody>
</table>

Default
The default is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on”i” platforms only.
configure debug-trace isis-spf

configure debug-trace isis-spf <level>

Description
Controls logging of debug messages related to SPF Calculation.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug level</td>
<td>Specifies a debug level. Following are the debug levels:</td>
</tr>
<tr>
<td>0 —</td>
<td>Critical/Error Messages</td>
</tr>
<tr>
<td>1 —</td>
<td>Warning Messages</td>
</tr>
<tr>
<td>2 —</td>
<td>Concise Messages</td>
</tr>
<tr>
<td>3 —</td>
<td>Verbose Messages</td>
</tr>
<tr>
<td>4 —</td>
<td>Packet Dumps</td>
</tr>
</tbody>
</table>

Default
The default is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace mpls

configure debug-trace mpls <level>

**Description**

This command records debug information to the syslog.

**NOTE**

*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>None.</td>
</tr>
<tr>
<td>1</td>
<td>Records error and warning messages, such as session up, state machine errors, Initialization errors, label allocation errors, patricia tree failures, invalid message type or format, memory allocation errors, NVRAM parse errors, TLS tunnel creation errors, socket errors, label manager problems, and null pointer or handle.</td>
</tr>
<tr>
<td>2</td>
<td>Records informational messages, such as LDP entity up, LDP parameter setting, LSP bind event, NHLFE creation, and MPLS GPP and session down errors.</td>
</tr>
<tr>
<td>3</td>
<td>Records debug information, such as patricia Tree Adds/Deletes, Label Propagation and Release Msgs, Message encoding, Parameter setting, MPLS enable messages, Memory initialization, TLS setup messages, Invalid value messages, LSP Init/Tear down msgs, Event processing, RDB (route) callback information.</td>
</tr>
<tr>
<td>4</td>
<td>Records more detailed debug information.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

**Default**

The default level is 0.

**Usage Guidelines**

The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

**Example**

The following command sets the reporting level for MPLS errors to 3:

```
configure debug-trace mpls 3
```

Following is the log output at this level:

```
<DBG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBG:IPHS> last message repeated 3 times
<DBG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBG:IPHS> last message repeated 3 times
<DBG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBG:IPHS> last message repeated 3 times
<DBG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
```
<DBUG:IPHS> last message repeated 2 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:IPHS> last message repeated 2 times
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<INFO:SYST> smm-a-console admin: configure debug-trace mpls 0
<DBUG:MPLS> Slot6 MPLS: KRT CHG - Can't Add MpIdx 17 from Nh Entry 1324
<DBUG:MPLS> Slot6 MPLS: processNh1feTableAddMpIdx: Attempting to add Mp Entry 17 to 'unused' Nh1fe Idx 1324
<DBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DBUG:MPLS> ip_output.c 664: CONTINUING IP OUTPUT
<INFO:MPLS> mpls_lpe.c 3277: mpls_lpe_common_input() returned
MPLS_LPE_PACKET_UNLABELLED
<DBUG:MPLS> mpls_lsp_endpt.c 346: Attempt to delete endpt entry 10.3.1.1/32
:advertise=0
<DBUG:MPLS> mpls_gpp.c 1037: MPLS Del NHLFE
<INFO:MPLS> mpls_gpp.c 1617: Create ILM for FecIp=10.3.1.1, Nh1feIx=1324,
EndptIx=1332, InLabel=0x11, OutLabel=
<DBUG:MPLS> mpls_gpp.c 796: MPLS Del ILM
<DBUG:MPLS> mpls_lsp_bind.c 1434: Unbinding label 0x00000011 from outgoing Ifc 3 Label
0x00000003
<DBUG:MPLS> mpls_rdb.c 2689: RDB REQ not able to find 10.3.1.1/32 nhop 0.0.0.0
<DBUG:MPLS> mpls_rdb.c 2524: RDB REQ - Get Recompute Next Hop
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x00002356
<DBUG:MPLS> mpls_lsp_bind.c 1034: Ingress torn down for unknown LSP to endpt
10.3.1.1/32 LSP ID 0x00002356
<INFO:MPLS> mplsevnt.c 394: LMS Notify (0x8d3d1f2c): LSP TORN DOWN (5) FEC:10.3.1.1:32
nhop 0.0.0.0 LSPID:9046
<DBUG:MPLS> mpls_lsp_endpt.c 466: Unbinding LSP to 10.3.1.1/32 Label 0x00000003
<DBUG:MPLS> mpls_lsp_endpt.c 765: MPLS Initiating SPF caculation for unbinding LSP to
10.3.1.1
<DBUG:MPLS> mpls_lsp_endpt.c 759: Cannot unbind LSP to 10.3.1.1:32 Type 1 nhop
10.0.1.2 without route entry
<DBUG:MPLS> mpls_rdb.c 2689: RDB REQ not able to find 10.3.1.1/32 nhop 10.0.1.2
<DBUG:MPLS> mpls_lsp_endpt.c 735: unbind_from_ipv4_endpoint: 10.3.1.1/32 Type 1 nhop
10.0.1.2
<DBUG:MPLS> mpls_rdb.c 2689: RDB REQ not able to find 10.3.1.1/32 nhop 0.0.0.0
<DBUG:MPLS> mpls_rdb.c 2524: RDB REQ - Get Recompute Next Hop
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 17.17.17.1/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 956: Recompute Issued for 10.3.1.1/32 nhop 10.0.1.2
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 10.3.1.1/32 nhop
10.0.1.2 orig=33 watch 2
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 192.168.100.12/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 192.168.100.11/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 192.168.100.2/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 20.0.0.1/32 nhop
10.0.1.2 orig=33 watch 0
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x000002371
<DBUG:MPLS> mplsevnt.c 584: LDP DU LSP ID RELEASE: 0x000002362
<DBUG:MPLS> mpls_rdb.c 606: mpls_rdb_callback: delete route to 12.0.0.1/32 nhop
10.0.2.2 orig=33 watch 0
<DBUG:MPLS> mpls_rdb.c 1060: du_recognize_new_fec: ifIndex=3,
destIp=192.168.100.11/32, nHop=10.0.2.2
configure debug-trace mpls

History

This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability

This command is available on "i" platforms only.
configure debug-trace mpls-signalling

configure debug-trace mpls-signalling <level>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the MPLS module for the “i” series switches.

Syntax Description

default level | Specifies a debug level:
0 — None.
1 — Records peer interface state msgs.
2 — No additional information recorded.
3 — Records finite state machine events
4 — No additional information recorded.
5 — Records MPLS signalling packets, such as hello packets and label mappings.

Default
The default level is 1.

Usage Guidelines
The debug level range is 1 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for MPLS signalling subsystem errors to 1:

configure debug-trace mpls-signalling 1

Following is the log output at this level:

<DEBUG:IPHS> last message repeated 3 times
<DEBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DEBUG:IPHS> last message repeated 3 times
<DEBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DEBUG:IPHS> last message repeated 3 times
<DEBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<DEBUG:IPHS> last message repeated 3 times
<DEBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
<INFO:SYST> User admin logged out from telnet (100.100.105.1)
<INFO:USER> admin logged in through telnet (100.100.105.1)
<DEBUG:IPHS> Skipping FDB refresh for 10.3.1.1 due to LSP
configure debug-trace mpls-signalling

History
This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability
This command is available on the MPLS module.
configure debug-trace npcard

configure debug-trace npcard <debug level>

Description
This command enables system-level debug tracing for the MPLS, PoS, ARM, and ATM modules.

NOTE
This command is available only on the MPLS, PoS, ARM, and ATM modules for the “i” series switches.

Syntax Description

default level | Specifies a debug level:

<table>
<thead>
<tr>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Indicates that a severe event has occurred that most likely will result in the termination or improper operation of the ARM.</td>
</tr>
<tr>
<td>1</td>
<td>Indicates that a major event has occurred. It may represent a negative operation. It should be reviewed to ensure proper continuation of ARM operation.</td>
</tr>
<tr>
<td>2</td>
<td>Indicates a minor event has occurred.</td>
</tr>
<tr>
<td>3</td>
<td>Provides additional information to support engineers for the purpose of diagnosing network problems.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 1 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for module errors to 3:
configure debug-trace npcard 3

History
This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability
This command is available on the MPLS, PoS, ARM, and ATM modules.
configure debug-trace pim-cache

configure debug-trace pim-cache <debug level>

Description
This command records debug information to the syslog.

**NOTE**
*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

**Default**
The default level is 0.

**Usage Guidelines**
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the detailed process of adding, deleting, and modifying a multicast cache. The IP multicast cache is a hardware forwarding entry identified by a ptag index number. The following command displays the cache entries:

```shell
cmd show ipmc cache [detail] <IP multicast group>
```

The trace is based on the ingress VLAN of a cache. Use this tool if the egress list of a cache is incorrect, if there are missing cache entries, or if any multicast stream jitters.

**Example**
The following command sets the reporting level for PIM cache errors to 3:

```shell
cmd configure debug-trace pim-cache 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-cache 3
<DBG:PIM> PIM: 142.168.100.100/236.58.16.16: pimSendRegStop: dst 15.1.6.3
<DBG:PIM> PIM: ProcRegister: sptree flow exists
<DBG:PIM> PIM: 142.168.100.100/236.58.16.16: entry timer starting for 210
```
Troubleshooting Commands

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available only on the “i” series platforms.
configure debug-trace pim-hello

configure debug-trace pim-hello <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

| vlan name   | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all PIM hello messages coming into a VLAN. Use this command if switches connected to a common network have problems establishing or maintaining normal neighbor relationships.

Example
The following command sets the reporting level for PIM hello errors to 3:

configure debug-trace pim-hello 3

Following is the log output at this level:

<INFO:SYST> msm-a-console admin: configure debug-trace pim-hello 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.2.1.2 thro 15.2.1.1
<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.4.2 thro 15.1.4.1
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.2.1.1 to 224.0.0.13
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.4.1 to 224.0.0.13
Troubleshooting Commands

<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.6.3 thro 15.1.6.1
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.6.1 to 224.0.0.13
<INFO:SYST> msm-a-console admin: configure debug-trace pim-hello 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.4.1 to 224.0.0.13
<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.6.3 thro 15.1.6.1
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.6.1 to 224.0.0.13
<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.2.1.2 thro 15.2.1.1
<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.2.1.2 thro 15.1.4.1
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.2.1.1 to 224.0.0.13
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.4.1 to 224.0.0.13
<DBG:PIM> PIM: Receiving Hello pkt of len 18 from src 15.1.6.3 thro 15.1.6.1
<DBG:PIM> PIM: Xmitting Hello pkt of len 18 from src 15.1.6.1 to 224.0.0.13
<INFO:SYST> msm-a-console admin: configure debug-trace pim-hello 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<INFO:SYST> Log cleared

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on ”i” platforms only.
configure debug-trace pim-message

configure debug-trace pim-message <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

| vlan name   | Specifies a VLAN name.  |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all PIM system messages (join, prune, graft, graft acknowledgement, assert, and BSRM) coming into a VLAN. Use this command if a multicast stream cannot be stopped or does not come down to the receiver after the IGMP snooping entry is verified, or if the CPU load is unexpectedly high.

Example
The following command sets the reporting level for PIM message errors to 3:

configure debug-trace pim-message 3

Following is the log output at this level:

<INFO:SYST> msm-a-console admin: configure debug-trace pim-message 3 vlan all
<DBUG:PIM> PIM: Xmitting RP Adv(8) pkt of len 22 from src 15.2.1.1 to 15.1.6.3
<DBUG:PIM> PIM: Xmitting RP Adv(8) pkt of len 22 from src 15.1.6.1 to 15.1.6.3
<DBUG:PIM> PIM: Xmitting RP Adv(8) pkt of len 22 from src 15.1.4.1 to 15.1.6.3
<DBUG:PIM> PIM: ProcPrune: src 0.0.0.0 rp 15.1.4.1 type (*,g)
<DBUG:PIM> PIM: ProcJoinPrune: joins 0 prunes 1
Historical Notes

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on "i" platforms only.
configure debug-trace pim-neighbor

configure debug-trace pim-neighbor <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

| vlan name | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces the state of all PIM neighbors on a common VLAN to monitor if, when, or how frequently a neighbor is added or deleted.

Example
The following command sets the reporting level for PIM neighbor errors to 3:

```
configure debug-trace pim-neighbor 3
```

Following is the log output at this level:

```
<INFO:SYST> msm-a-console admin: configure debug-trace pim-neighbor 3 vlan all
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<INFO:SYST> Port 8:1 link down
<INFO:SYST> Port 8:2 link down
<INFO:SYST> Port 8:3 link down
<INFO:SYST> Port 8:4 link down
<DEBUG:PIM> PIM: pimDelNbr: nbr 15.1.4.2 thro iface 15.1.4.1
```
Troubleshooting Commands

<INFO:SYST> Port 8:4 link down
<INFO:SYST> Port 8:3 link down
<INFO:SYST> Port 8:2 link down
<INFO:SYST> Port 8:1 link down

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace pim-rp-mgmt

configure debug-trace pim-rp-mgmt <debug level>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records error messages.</td>
</tr>
<tr>
<td>1</td>
<td>Records warnings.</td>
</tr>
<tr>
<td>2</td>
<td>Records verbose warnings.</td>
</tr>
<tr>
<td>3</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

This command traces all RP advertisement and bootstrap messages carrying rp-set information coming into a VLAN. Use this command if RP or BSR is absent or unstable. This command is for sparse mode only.

Example
The following command sets the reporting level for PIM RP management errors to 3:

configure debug-trace pim-rp-mgmt 3

Following is the log output at this level:

<INFO:SYST> msm-a-console admin: configure debug-trace pim-rp-mgmt 3
<INFO:SYST> Log cleared
<INFO:SYST> msm-a-console admin: clear log static
<DBG:PIM> PIM: ProcBootstrap: Wrong iif for BSR 15.1.6.3
<DBG:PIM> PIM: ProcBootstrap: from 15.1.4.2 in 15.1.4.1 len 56
<DBG:PIM> PIM: rpDelEntry: 15.3.1.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.3.1.1 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.4.2 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.4.2 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.8.2 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.8.2 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.4.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.4.1 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.2.1.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.2.1.1 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.6.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.6.1 no longer listed
<DBG:PIM> PIM: rpGetEntry: 192.168.100.3
<DBG:PIM> PIM: ProcBootstrap: rp 192.168.100.3
<DBG:PIM> PIM: rpGetEntry: 15.1.6.3
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.6.3
<DBG:PIM> PIM: rpGetEntry: 15.1.8.3
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.8.3
<DBG:PIM> PIM: ProcBootstrap: grp 224.0.0.0
<DBG:PIM> PIM: ProcBootstrap: fragment Tag 40585
<DBG:PIM> PIM: ProcBootstrap: from 15.1.6.3 in 15.1.6.1 len 56
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.4.2 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.8.2 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.8.2 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.2.1.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.2.1.1 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.6.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.6.1 no longer listed
<DBG:PIM> PIM: rpDelEntry: 15.1.4.1 (Bootstrap)
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.4.1 no longer listed
<DBG:PIM> PIM: rpGetEntry: 192.168.100.3
<DBG:PIM> PIM: ProcBootstrap: rp 192.168.100.3
<DBG:PIM> PIM: rpGetEntry: 15.1.6.3
<DBG:PIM> PIM: ProcBootstrap: rp 15.1.6.3
<DBG:PIM> PIM: ProcBootstrap: grp 224.0.0.0
<DBG:PIM> PIM: ProcBootstrap: fragment Tag 41065
<DBG:PIM> PIM: ProcBootstrap: from 15.1.6.3 in 15.1.6.1 len 56

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on "i" platforms only.
configure debug-trace rip-message

configure debug-trace rip-message <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 — None.</td>
<td></td>
</tr>
<tr>
<td>1 — None.</td>
<td></td>
</tr>
<tr>
<td>2 — None.</td>
<td></td>
</tr>
<tr>
<td>3 — Records that the switch received a response from w.x.y.z (pier) len 24 at time.time. Records that the switch sent a response to 224.0.0.9 at time.time.</td>
<td></td>
</tr>
<tr>
<td>4 — Displays a dump of the RIP response. Displays a dump of the RIP response received.</td>
<td></td>
</tr>
<tr>
<td>5 — No additional information recorded.</td>
<td></td>
</tr>
</tbody>
</table>

| vlan name | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for RIP message errors to 3:

```
configure debug-trace rip-message 3
```

Following is the log output at this level:

```
<DBG:RIP> Sending Rsp to 224.0.0.9 at 1012569160.950000
<INFO:SYST> msm-a-console admin: configure debug-trace rip-message 3 vlan all
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace rip-route-change

configure debug-trace rip-route-change <debug level> vlan <vlan name | all>

Description
This command is not currently supported.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>1 —</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>2 —</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>3 —</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>4 —</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>5 —</td>
<td>Not currently supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>vlan name</th>
<th>Specifies a VLAN name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
This command is not currently supported.

Example
This command is not currently supported.

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace rip-triggered-update

    configure debug-trace rip-triggered-update <debug level> vlan <vlan name | all>

Description
This command records debug information to the syslog.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug level</td>
<td>Specifies a debug level:</td>
</tr>
<tr>
<td>0 —</td>
<td>None.</td>
</tr>
<tr>
<td>1 —</td>
<td>None.</td>
</tr>
<tr>
<td>2 —</td>
<td>None.</td>
</tr>
<tr>
<td>3 —</td>
<td>Records that the switch is suppressing triggered updates for x seconds.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for RIP triggered update errors to 3:

    configure debug-trace rip-triggered-update 3

Following is the log output at this level:

    <DBG:RIP > Suppressing triggered updates for 1 secs.
    <INFO:SYST> msm-a-console admin: enable rip
    <INFO:SYST> msm-a-console admin: disable rip

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace slb-3dns

configure debug-trace slb-3dns <debug level>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records serious errors that can cause 3DNS support to fail. This includes problems associated with system resources, invalid iQuery messages, and internal SLB and 3DNS table maintenance.</td>
</tr>
<tr>
<td>1</td>
<td>Records task and or socket layer errors. These errors might indicate other more serious problems.</td>
</tr>
<tr>
<td>2</td>
<td>Records informational 3DNS member change notifications, state changes, or age-outs.</td>
</tr>
<tr>
<td>3</td>
<td>Decodes and displays incoming and outgoing 3DNS iQuery messages. Also displays some internal table data when the 3DNS member entries are created or updated.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for SLB 3DNS errors to 3:
```bash
configure debug-trace slb-3dns 3
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace slb-connection

    configure debug-trace slb-connection <debug level>

**Description**
This command records debug information to the syslog.

**NOTE**
*This command is available only on the “i” series switches.*

**Syntax Description**

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records critical failures such as insufficient memory unexpected internal state.</td>
</tr>
<tr>
<td>1</td>
<td>Records unaccepted or dropped connections, as well as physical ports removed from a GoGo mode group since a failed health check and physical ports added to a GoGo mode group since a passed health check.</td>
</tr>
<tr>
<td>2</td>
<td>Records GoGo mode resources that fail health check, or that change health check status from fail to pass. An associated debug level 1 message will accompany this message only if this was either the first health-check to fail on a port, or the last remaining health-check to pass on a port.</td>
</tr>
<tr>
<td>3</td>
<td>Records all events associated with connecting and disconnecting resources, and some SLB configuration debugging information.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

**Default**
The default level is 0.

**Usage Guidelines**
The `debug level` range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

**Example**
The following command sets the reporting level for SLB connection errors to 3:

```
configure debug-trace slb-connection 3
```

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on "i" platforms only.
configure debug-trace slb-failover

configure debug-trace slb-failover <debug level>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 —</td>
<td>Records possible software errors such as unexpected function call failures and bad function arguments.</td>
</tr>
<tr>
<td>1 —</td>
<td>Records configuration errors, insufficient memory, and bad data from a peer SLB switch.</td>
</tr>
<tr>
<td>2 —</td>
<td>Records when a peer SLB switch has come up or gone down.</td>
</tr>
<tr>
<td>3 —</td>
<td>Displays debug messages.</td>
</tr>
<tr>
<td>4 —</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5 —</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for SLB failover errors to 3:
configure debug-trace slb-failover 3

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” platforms only.
configure debug-trace stacking

configure debug-trace stacking <debug level>

Description
This command provides system-level debug tracing for stacked switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0x01</td>
<td>Enables initialization logs.</td>
</tr>
<tr>
<td>0x02</td>
<td>Enables state event machine logs.</td>
</tr>
<tr>
<td>0x04</td>
<td>Enables ATP module logs.</td>
</tr>
<tr>
<td>0x08</td>
<td>Enables RPC module logs.</td>
</tr>
<tr>
<td>0x10</td>
<td>Enables event pre-processor module logs.</td>
</tr>
<tr>
<td>0x20</td>
<td>Enables timer module logs.</td>
</tr>
<tr>
<td>0x80</td>
<td>Enables layer 2 module logs.</td>
</tr>
<tr>
<td>0x100</td>
<td>Enables detailed logging including errors.</td>
</tr>
<tr>
<td>0x400</td>
<td>Enables topology module logs.</td>
</tr>
<tr>
<td>0x800</td>
<td>Enables logs related to processing packets from the background task.</td>
</tr>
<tr>
<td>0x2000</td>
<td>Enables state event transition logs.</td>
</tr>
<tr>
<td>0x8000</td>
<td>Enables logs related to failover processing.</td>
</tr>
<tr>
<td>0x10000</td>
<td>Enables the logs related to slot binding.</td>
</tr>
<tr>
<td>0x20000</td>
<td>Enables logs related to the background task, which is used for programming the hardware.</td>
</tr>
<tr>
<td>0x10000000</td>
<td>Enables minimal chipset level logs.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Do not configure this command for normal conditions.

Example
The following command enables debug-trace for stacking errors related to slot binding:
configure debug-trace stacking 0x100000

The following command disables debug-trace for stacking:
configure debug-trace stacking 0

History
This command was first available in ExtremeWare 7.4.
Platform Availability
This command is available on Summit 200, Summit 300-24, and Summit 400 switches.
configure debug-trace transceiver-test

configure debug-trace transceiver-test <debug level>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Disables debug tracing for the transceiver test and stops recording information to the syslog.</td>
</tr>
<tr>
<td>1</td>
<td>Enables debug tracing for the transceiver test and records information to the syslog.</td>
</tr>
<tr>
<td>2</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>3</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>4</td>
<td>No additional information recorded.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Level 0 disables the debug-trace for the transceiver testing, and level 1 enables debug-trace for the transceiver testing.

For levels 2 through 5, debug-trace for transceiver testing is enabled, but no additional information is recorded.

Example
The following command enables debug-trace for transceiver testing:
configure debug-trace transceiver-test 1

Following is sample log output at this level:

07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 2 returns pass
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 4 returns pass
07/09/2003 15:09:14.02 <Info:TRXDIAG> trxdiag: CPU NVRAM test on BPLNE returns pass
07/09/2003 15:09:14.03 <Info:TRXDIAG> trxdiag: TWISTER test on BPLNE returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 1 returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 2 returns pass
07/09/2003 15:09:15.00 <Info:TRXDIAG> trxdiag: EXT MAC test on slot 4 returns pass
The following command disables debug-trace for transceiver testing:

```
configure debug-trace transceiver-test 0
```

**History**

This command was first available in ExtremeWare 6.2.2b108.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

**Platform Availability**

This command is available on "i" platforms only.
configure debug-trace udp-forwarding

configure debug-trace udp-forwarding <debug level> vlan <vlan name>

Description
This command is not currently supported.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>1</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>2</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>3</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>4</td>
<td>Not currently supported.</td>
</tr>
<tr>
<td>5</td>
<td>Not currently supported.</td>
</tr>
</tbody>
</table>

| vlan name   | Specifies a VLAN name. |

Default
The default level is 0.

Usage Guidelines
This command is not currently supported.

Example
This command is not currently supported.

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure debug-trace vrrp

    configure debug-trace vrrp <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>debug level</th>
<th>Specifies a debug level:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Records critical errors, such as a task crash or an interface down.</td>
</tr>
<tr>
<td>1</td>
<td>Records warning messages.</td>
</tr>
<tr>
<td>2</td>
<td>Records concise packet information.</td>
</tr>
<tr>
<td>3</td>
<td>Records the same information recorded in level 2, with more detail.</td>
</tr>
<tr>
<td>4</td>
<td>Displays a dump of each packet.</td>
</tr>
<tr>
<td>5</td>
<td>No additional information recorded.</td>
</tr>
</tbody>
</table>

vlan name  Specifies a VLAN name.

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for VRRP to 5:

configure debug-trace vrrp 5

Following is the log output at this level:

<DBG:SYS > Vlan/Vrid=vlans/1 Putting virtualMac (00:00:5e:00:01:01) into arpcom
<DBG:SYS > Vlan/Vrid=vlans/1 Putting systemMac (00:01:30:04:c8:00) into arpcom

History
This command was first available in ExtremeWare 6.2.1.

Platform Availability
This command is available on “i” platforms.
configure debug-trace vrrp-hello

configure debug-trace vrrp-hello <debug level> vlan <vlan name>

Description
This command records debug information to the syslog.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>debug level</td>
<td>Specifies a debug level:</td>
</tr>
<tr>
<td></td>
<td>0 — Records critical errors, such as a task crash or an interface down.</td>
</tr>
<tr>
<td></td>
<td>1 — Records warning messages, such as incorrect address, incorrect protocol, and failed checksum.</td>
</tr>
<tr>
<td></td>
<td>2 — Records information such as VLAN, VRID, priority, auth-type, advert-interval, and IP address.</td>
</tr>
<tr>
<td></td>
<td>3 — Records the same information recorded in level 2, with more detail.</td>
</tr>
<tr>
<td></td>
<td>4 — Displays a dump of each packet.</td>
</tr>
<tr>
<td></td>
<td>5 — No additional information recorded.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
The default level is 0.

Usage Guidelines
The debug level range is 0 to 5. Higher levels record more verbose messages. Higher levels also record the messages recorded at lower levels.

Example
The following command sets the reporting level for VRRP hello messages to 4:

```
configure debug-trace vrrp-hello 4
```

Following is the log output at this level:

```
<DBG:SYS > Vlan=Default: vrrpTransmit: vrid=1,pri=255,cnt_ip_addr=1,auth_type=0 advert=1,ipaddr=10.45.208.10
<DBG:SYS > Vlan=Default: vrrpTransmit: vrid=1,pri=255,cnt_ip_addr=1,auth_type=0 advert=1,ipaddr=10.45.208.10
<DBG:SYS > Sending vrrp-pkt(0x8313d630) len 40 to 224.0.0.18 if rif0, mac=00:00:5e:00:01:01
<DBG:KERN> <--- Start of chain (84859200) --->
<DBG:KERN> m0 @ 0x84859200:  Length=40   m_off=20   m_data=0x84859214
<DBG:KERN> 0x0884859214: 00 00 00 28 00 00 00 00 ff 70 00 00 00 00 00 00
***(* *****p*****
```
**Troubleshooting Commands**

**History**
This command was first available in ExtremeWare 6.2.1.

**Platform Availability**
This command is available on "i" platforms.
configure debug-trace wireless

configure debug-trace wireless ports [<portlist> | all] [dot1x | radius | mac | snmp | wlan-driver | eth-driver | ap-scan | client-diag | mac-radius | wpa-wpa2 | iapp] <debug-level>

Description
Enables debug tracing for troubleshooting.

Syntax Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5, 2*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>dot1x</td>
<td>Configures debug tracing level for the 802.1x activity.</td>
</tr>
<tr>
<td>radius</td>
<td>Configures debug tracing level for the RADIUS activity.</td>
</tr>
<tr>
<td>mac</td>
<td>Configures debug tracing level for the MAC layer activity.</td>
</tr>
<tr>
<td>snmp</td>
<td>Configures debug tracing level for the SNMP activity.</td>
</tr>
<tr>
<td>wlan-driver</td>
<td>Configures debug tracing level for the WLAN driver activity.</td>
</tr>
<tr>
<td>eth-driver</td>
<td>Configures debug tracing level for the Ethernet driver activity.</td>
</tr>
<tr>
<td>ap-scan</td>
<td>Configures debug tracing level for the Access Point Scans.</td>
</tr>
<tr>
<td>client-diag</td>
<td>Configures debug tracing level for the Client Diagnostics.</td>
</tr>
<tr>
<td>mac-radius</td>
<td>Configures debug tracing level for the MAC-RADIUS activity.</td>
</tr>
<tr>
<td>wpa-wpa2</td>
<td>Configures debug tracing level for the WPA and WPA2 activities.</td>
</tr>
<tr>
<td>iapp</td>
<td>Configures debug tracing level for the IAPP activity.</td>
</tr>
<tr>
<td>debug-level</td>
<td>Specifies a debug level. The default is 0 (off).</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Use to trace messages for troubleshooting.

Example
The following example enables debug tracing for IAPP on port 1:15 with a debug level of 2:

configure debug-trace wireless ports 1:15 iapp 2

History
This command was first available in ExtremeWare 7.3e.
Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800 switches.
configure diagnostics

configure diagnostics [extended | fastpost | normal | off | verbose | quiet]

Description
Runs switch diagnostics at boot-up.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>extended</td>
<td>Selects an extended diagnostic routine to run at boot-up. Takes the switch fabric and ports offline, and performs extensive ASIC, ASIC-memory, packet switch, and packet loopback tests. This parameter is not supported in ExtremeWare 6.1.9 or 6.2.</td>
</tr>
<tr>
<td>fastpost</td>
<td>Selects fastpost diagnostic routine to run at boot-up. Takes the switch fabric offline and performs a simple ASIC test.</td>
</tr>
<tr>
<td>normal</td>
<td>Selects normal diagnostic routine to run at boot-up. Takes the switch fabric and ports offline, and performs a simple ASIC and packet loopback test on all the ports. This parameter is not supported in ExtremeWare 6.1.9 or 6.2.</td>
</tr>
<tr>
<td>off</td>
<td>Stops boot-up diagnostics.</td>
</tr>
<tr>
<td>verbose</td>
<td>Specifies that the results of every test are recorded in the log. The verbose option is not saved through a reboot, so you must reconfigure verbose mode after running diagnostics.</td>
</tr>
<tr>
<td>quiet</td>
<td>Specifies that only the pass or fail result is recorded in the log.</td>
</tr>
</tbody>
</table>

Default
Fastpost, quiet.

Usage Guidelines
To run diagnostics on an I/O module, use the following command:

run diagnostics [ cable | extended | normal packet-memory] slot [<slot> | msm-a | msm-b]

The cable, extended, and normal modes are not supported on bootup at this time.

To view results of the diagnostics test, use the following command:

show diagnostics

If the diagnostics fail, replace the module with another module of the same type.

Example
The following command configures the MSM to run the fastest diagnostics at boot-up:

configure diagnostics fastpost
History
This command was first available in ExtremeWare 6.1.9.

Platform Availability
This command is available on “i” series BlackDiamond switches.
configure reboot-loop-protection

configure reboot-loop-protection threshold <time-interval> <count>

Description
Configures reboot loop protection.

Syntax Description

<table>
<thead>
<tr>
<th>time-interval</th>
<th>The length of time during which the switch can reboot the specified count before entering minimal mode. The range is 0 - 255 minutes.</th>
</tr>
</thead>
<tbody>
<tr>
<td>count</td>
<td>The number of reboots within the specified time-interval. The range is 1 - 7.</td>
</tr>
</tbody>
</table>

Default
If you enter a time-interval but not a count, the default count is 3.

Usage Guidelines
Specifying a time interval of 0 disables reboot loop protection. Specifying any other value enables it. To view the current settings, use the show switch or show configuration commands.

If you reboot the switch manually or use the run msm-failover or run diagnostics commands, the time interval and count are both reset to 0.

Example
The following command configures the time interval to 5 minutes and the count to 4:
configure reboot-loop-protection threshold 5 4

History
This command was first available in ExtremeWare 6.2.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure system-dump server

    configure system-dump server <ip address>

Description
Configures the IP address to which to transfer a dump if the system-dump option is specified in the configuration.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address to which to transfer a system dump.</td>
</tr>
</tbody>
</table>

Default
The default is 0 or “no IP”.

Usage Guidelines
The IP address specified is also used if no address is provided in the upload system-dump command. The IP address must be reachable through the VLAN mgmt.

Example
The following command configures the IP address to transfer a system dump to 10.10.10.1:

    configure system-dump server 10.10.10.1 3

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is available only on platforms with an Ethernet management port.
configure system-dump timeout

    configure system-dump timeout <seconds>

Description
Configures an optional timeout for the dump transfer.

NOTE
This command is available only on the "i" series switches.

Syntax Description

| seconds | Specifies a time in seconds for the system dump timeout. |

Default
The default is 0.

Usage Guidelines
The minimum non-zero value is 120 seconds. The minimum recommended value is 480 seconds.

Example
The following command configures the system dump timeout to 600 seconds:

    configure system-dump timeout 600

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is available on platforms with an Ethernet management port.
disable log debug-mode


disable log debug-mode

Description
Disables debug mode. The switch stops generating debug events.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command disables debug mode. Debug mode must be enabled prior to configuring advanced debugging capabilities. These include allowing debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

The following configuration options require that debug mode be enabled:

- including a severity of debug-summary, debug-verbose, or debug-data when configuring filters
- target format options process-name, process-id, source-function, and source-line)

Example
The following command disables debug mode:
disable log debug-mode

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable log debug-mode

enable log debug-mode

Description
Enables debug mode. The switch generates debug events.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command enables debug mode. Debug mode must be enabled prior to configuring advanced debugging capabilities. These include allowing debug messages, which can severely degrade performance. For typical network device monitoring, debug mode should remain disabled, the default setting. Debug mode should only be enabled when advised by technical support, or when advanced diagnosis is required. The debug mode setting is saved to FLASH.

The following configuration options require that debug mode be enabled:

- including a severity of debug-summary, debug-verbose, or debug-data when configuring filters
- target format options process-name, process-id, source-function, and source-line.

Example
The following command enables debug mode:

enable log debug-mode

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
nslookup

        nslookup <hostname>

Description
Displays the IP address of the requested host.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Specifies a hostname.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command looks up the IP address of a computer with the name of bigserver.xyz_inc.com:
nslookup bigserver.xyz_inc.com

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
**ping**

For the “i” platforms:

```plaintext
ping [udp] {continuous} {size <start_size> {<-end_size}} [<ip_address> | <hostname>] {from <src_ipaddress> | with record-route | from <src_ipaddress> with record-route}
```

For the “e” platforms:

```plaintext
ping [udp] {continuous} {start-size <size number> {<-end_size}} [<ip_address> | <hostname>] {from <src_ipaddress> | with record-route | from <src_ipaddress> with record-route}
```

**Description**

Enables you to send User Datagram Protocol (UDP) or Internet Control Message Protocol (ICMP) echo messages or to a remote IP device.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>udp</td>
<td>Specifies that the ping request should use UDP instead of ICMP.</td>
</tr>
<tr>
<td>continuous</td>
<td>Specifies that UDP or ICMP echo messages to be sent continuously. This option can be interrupted by pressing any key.</td>
</tr>
<tr>
<td>start_size</td>
<td>Specifies the size, in bytes, of the packet to be sent, or the starting size if incremental packets are to be sent.</td>
</tr>
<tr>
<td>end_size</td>
<td>Specifies the maximum size, in bytes, of the packet to be sent in the UDP or ICMP request. When both the start_size and end_size are specified, ICMP requests are transmitted using 1 byte increments, per packet.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the host.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the name of the host.</td>
</tr>
<tr>
<td>src_ipaddress</td>
<td>Uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used.</td>
</tr>
<tr>
<td>record-route</td>
<td>Decodes the list of recorded routes and displays them when the ICMP echo reply is received.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

The `ping` command is used to test for connectivity to a specific host.

The `ping` command is available for both the user and administrator privilege level.

If a `ping` request fails, the switch continues to send `ping` messages until interrupted. Press any key to interrupt a `ping` request.

For ExtremeWare 6.1:

- You must configure DNS in order to use the `hostname` option.
For ExtremeWare 6.2:
- If you specify UDP as the protocol, the from <source> and with <record-route> options are not supported.

**Example**
The following command enables continuous ICMP echo messages to be sent to a remote host:

```
ping continuous 123.45.67.8
```

**History**
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.1 to support the hostname, from, and with record-route parameters, and incremental packets.

This command was modified in ExtremeWare 6.2 to support UDP.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
run diagnostics

For the “i” series switches:

```
run diagnostics [cable | extended | normal | packet memory] slot [<slot number> | msm-a | msm-b]
```

For the “e” series switches:

```
run diagnostics [extended | normal | stack-port]
```

**Description**

Runs normal or extended diagnostics on the switch, slot, stacking port, or the management module.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cable</td>
<td>Runs the cable diagnostic routine. Takes ports offline and checks the cable for faults.</td>
</tr>
<tr>
<td>extended</td>
<td>Runs an extended diagnostic routine. Takes the switch fabric and ports offline, and performs extensive ASIC, ASIC-memory, packet memory, and packet loopback tests.</td>
</tr>
<tr>
<td>normal</td>
<td>Runs a normal diagnostic routine. Takes the switch fabric and ports offline, and performs a simple ASIC and packet loopback test on all the ports.</td>
</tr>
<tr>
<td>packet memory</td>
<td>Runs packet memory diagnostics on an “i” series module or stackable. Note: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot number of an I/O module. Note: This option is available only on BlackDiamond switches.</td>
</tr>
<tr>
<td>msm-a</td>
<td>Specifies the slot letter of an MSM. Note: This option is available only on BlackDiamond switches.</td>
</tr>
<tr>
<td>stack-port</td>
<td>Specifies to run the diagnostic routine on the stacking port. Note: This option is available only on the Summit 400 switches.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

**NOTE**

_Run diagnostics when the switch can be brought off-line. The tests conducted are extensive and affect traffic that must be processed by the system CPU. The diagnostics are processed by the CPU whether you run them on an I/O or a management module._

The normal diagnostics are short series of tests that do not test all the internal ASIC functions. On a management module, the extended diagnostic routine tests all components including the internal ASIC functions. The management module is taken off-line while the diagnostic test is performed. It is reset and operational once the test is completed.
You can run up to two diagnostics tests at the same time.

To view results of normal or extended diagnostics tests, use the following commands:

- On an “i” series switch:
  `show diagnostics {slot [msm-a | msm-b | <slot number>]}`
- On an “e” series switch:
  `show diagnostics`

If the results for a module indicate that the diagnostic failed, replace the module with another module of the same type.

**For the “i” Series Switches.** If you run the diagnostic routine on an I/O module in an “i” series switch, that module is taken off-line while the diagnostic test is performed. The ports on the module do not forward traffic. When the diagnostic test is completed, the I/O module is automatically reset and becomes operational again.

On an I/O module, the extended diagnostic routine can require significantly more time to complete, depending on the number of ports on the module.

**For the BlackDiamond Switches.** To configure a BlackDiamond switch to run diagnostics on an MSM at boot-up, use the following command:

```
configure diagnostics [extended | fastpost | normal | off]
```

**Example**

The following command runs extended diagnostics on the module in slot 3 of a BlackDiamond chassis:

```
run diagnostics extended slot 3
```

A warning is displayed about the impact of this test, and you have the opportunity to continue or cancel the test.

```
Running extended diagnostics will disrupt network traffic on the system. Extended diagnostic will also execute Packet Memory Scan........
WARNING: Device may be taken offline. To prevent this first configure "sys-health-check auto-recovery online"
```

Are you sure you want to continue? yes/no

Y

Extended diagnostics can cause the following messages to appear in the log:

```
<CRIT:SYST> task tdiagTask cpu utilization is 98% PC: 806266e8
<INFO:SYST> task tdiagTask cpu utilization is 98% PC: 806266e8
```

You can ignore these messages; they indicate that the system is busy running the diagnostics.

**History**

This command was first available in ExtremeWare 6.1.5.

The command was modified to support the MPLS module in an ExtremeWare IP Technology Services Release based on ExtremeWare 6.1.8b12.
The command was modified to support MSM modules in ExtremeWare 6.1.9.

The command was modified to support Alpine and Summit switches in ExtremeWare 6.2.

The command was modified to support stacking on the Summit 400 switches in ExtremeWare 7.4.

**Platform Availability**

This command is available on all platforms. The `stack-port` option is only available on the Summit 400.
run diagnostics_noslot

   run diagnostics_noslot [normal | extended | packet-memory]

Description
Executes diagnostic tests on the switch.

NOTE
This command is available only on the Alpine and Summit series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Normal</td>
<td>Runs standard diagnostic tests.</td>
</tr>
<tr>
<td>Extended</td>
<td>Run full set of diagnostic tests, including packet-memory tests.</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot number of an I/O module.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The switch is taken off-line while the diagnostic test is performed.

NOTE
Run diagnostics when the switch can be brought off-line. The tests conducted are extensive and affect traffic that must be processed by the system CPU. The diagnostics are processed by the CPU whether you run them on an I/O or a management module.

Packet memory scanning scans to detect single bit-related memory defects and their associated buffer locations. If packet memory defects are detected, their locations are recorded in the module EEPROM. Up to eight occurrences can be recorded. If a defect was found during the scan process, the module is reset, the defective buffer is mapped out from further use, and the I/O module is returned to the operational state. If more than eight defects are detected, or if the defects cannot be mapped out, the module is treated as a failed module and left offline, unless sys-health-check is configured for online. The module should then be returned through the RMA process with Extreme Networks Technical Support.

When you enter the run diagnostic command, you are warned about any potential impacts on your switch and network (since the module will be taken offline during the diagnostic process) and you will have an opportunity to confirm or cancel the test.

NOTE
Run diagnostics when the switch can be brought off-line. The tests conducted are extensive and affect traffic that must be processed by the system CPU. The diagnostics are processed by the CPU whether you run them on an I/O or a management module.
Example

The following command runs the full diagnostics set on a Summit switch:
run diagnostics_noslot extended

The command initially generates the following messages:
Running Extended diagnostics will reset the switch and disrupt network traffic. 
Extended diagnostic will also execute Packet Memory Scan........
WARNING: Device may be taken offline. To prevent this 
first configure "sys-health-check alarm-level auto-recovery online"

Are you sure you want to continue? yes/no y

To display the diagnostics results, use the show diagnostics command.

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on Alpine and Summit series switches.
run diagnostics cable ports

run diagnostics cable ports <portlist>

Description
Runs diagnostics on Ethernet cables.

Syntax Description

| portlist | Runs cable diagnostics for one or more port numbers. |

Default
N/A

Usage Guidelines
This command tests each of the four unshielded twisted-pair (UTP) cables. When the test completes, the command prompts you to enter the show port portlist cable diagnostics command to see the results of the test.

By reviewing the output of the show command you can determine:

- The length of the cable
- Whether there is a successful termination, or whether there is an open or short

Examples
The following example tests the Ethernet cable inserted into port 1. The four copper pairs do not all have the same length, which might indicate a kink in the cable, or a open connection:

Summit400-48t:27 # run diagnostics cable ports 1
Cable Diagnostics has completed, to view results enter show port <port list> cable diagnostics

Summit400-48t:28 # show port 1 cable diagnostics

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pair A</td>
<td>3 meters</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td>Pair B</td>
<td>2 meters</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td>Pair C</td>
<td>1 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair D</td>
<td>1 meters</td>
<td>Open or Short</td>
</tr>
</tbody>
</table>

The following example shows none of the twisted pairs terminate successfully at port 1, which could indicate that the cable is not inserted into the port:

Summit400-48t:29 # run diagnostics cable ports 1
Cable Diagnostics has completed, to view results enter show port <port list> cable diagnostics
Summit400-48t:30 # show port 1 cable diagnostics

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pair A</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair B</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair C</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair D</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
</tbody>
</table>

**History**

This command was introduced in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
run diagnostics packet-memory slot

run diagnostics packet-memory slot [msm-a | msm-b | msm-c | msm-d | <slot number>]

Description
Executes packet memory scanning for all packet memory associated with the specified MSM or I/O slot.

NOTE
This command is available only on the BlackDiamond series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msm-a</td>
<td>msm-b</td>
</tr>
<tr>
<td>slot number</td>
<td>Specifies the slot number of an I/O module.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you run the diagnostic routine on a module, that module is taken off-line while the diagnostic test is performed. The ports on the module do not forward traffic. Once the diagnostic test is completed, the module is automatically reset and becomes operational again.

NOTE
Run diagnostics when the switch can be brought off-line. The tests conducted are extensive and affect traffic that must be processed by the system CPU. The diagnostics are processed by the CPU whether you run them on an I/O or a management module.

Packet memory scanning scans the specified module to detect single bit-related memory defects and their associated buffer locations. If packet memory defects are detected, their locations are recorded in the module EEPROM. Up to eight occurrences can be recorded. If a defect was found during the scan process, the module is reset, the defective buffer is mapped out from further use, and the module is returned to the operational state. If more than eight defects are detected, or if the defects cannot be mapped out, the module is treated as a failed module and left offline, unless sys-health-check is configured for online. The module should then be returned through the RMA process with Extreme Networks Technical Support.

When you enter the run diagnostic command, you are warned about any potential impacts on your switch and network (since the module will be taken offline during the diagnostic process) and you will have an opportunity to confirm or cancel the test.

To show the results of a packet-memory diagnostic, use the following command:

show diagnostics packet-memory slot <slot number>
Example

The following command runs a packet-memory scan on the board in slot 4 on a BlackDiamond:

```
run diagnostics packet-memory slot 4
```

The command initially generates the following messages:

```
Running packet memory diagnostics will disrupt network traffic on the system.
WARNING: Device may be taken offline. To prevent this
        first configure "sys-health-check auto-recovery online"
```

Are you sure you want to continue? yes/no

If you respond with “y” the scan proceeds.

If you run the packet-memory test on a slot that has no packet memory errors, the output from the command will be similar to the following:

```
* BD3>:17 # Starts scanning packet memory on card 4.
<diagPM-1> INFO: entering packet memory scanning for card 4
................|................|................
Finished scanning packet memory for card 4 --
>>> No new defect <<<
```

If packet memory errors are detected, output similar to the following is displayed:

```
* BD3>:23 # Starts scanning packet memory on card 2.
<diagPM-1> INFO: entering packet memory scanning for card 2
................|................|................
Checking Struct...has 0 entries
Received Packet
  00 | 34 26 49 80 64 50 14 1f 60 54 1d a3 27 ee 5c 44
  10 | 01 fd 1b 2a 15 0c 4e 79 71 c5 3c 19 1e 6b 36 83
  20 | 40 39 35 79 67 2e 25 6c 7e ae 01 06 49 10 61 0e
  30 | 3d da 55 9d 02 67 40 62 2a 2f 3a 64 47 dc 00 86
Transmit Packet
  00 | 34 26 49 80 64 50 14 1f 60 54 1d a3 27 ee 5c 44
  10 | 01 fd 1b 2a 15 0c 4e 79 71 c5 3c 19 1e 6b 36 83
  20 | 44 39 35 79 67 2e 25 6c 7e ae 01 06 49 10 61 0e
  30 | 3d da 55 9d 02 67 40 62 2a 2f 3a 64 47 dc 00 86
MEMID=9, recov=0, bit_position=0 , addr=101290, entry=0...
Finished scanning packet memory for card 2 --
>>> New defect(s) detected <<<
```

History

This command was first available in ExtremeWare 6.1.5.

The command was modified to support the MPLS module in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

The command was modified to support MSM modules in ExtremeWare 6.1.9.

The command was modified to support Alpine and Summit switches in ExtremeWare 6.2.

The command was modified to support Packet Memory scanning for Black Diamond I/O modules in ExtremeWare 6.2.1. See the Release Note for information on which modules are supported.
Platform Availability

This command is available on “i” series switches.
show debug-trace

On the “i” series switches:

```bash
cmd
```

On the “e” series switches:

```bash
cmd
```

**Description**
Displays the configured debug-trace levels.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting</td>
<td>Specifies accounting level.</td>
</tr>
<tr>
<td>bootprelay</td>
<td>Specifies BOOTP relay level.</td>
</tr>
<tr>
<td>card-state-change</td>
<td>Specifies card state change level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>debug-link</td>
<td>Specifies link detection level.</td>
</tr>
<tr>
<td>dvmrp-cache</td>
<td>Specifies DVMRP cache level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>dvmrp-hello</td>
<td>Specifies DVMRP hello level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>dvmrp-message</td>
<td>Specifies DVMRP message level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>dvmrp-neighbor</td>
<td>Specifies DVMRP neighbor level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>dvmrp-route</td>
<td>Specifies DVMRP route level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>dvmrp-timer</td>
<td>Specifies DVMRP timer level.</td>
</tr>
<tr>
<td>NOTE: This option is available only on the “i” series switches.</td>
<td></td>
</tr>
<tr>
<td>Command</td>
<td>Description</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>e1</td>
<td>Specifies E1 level.</td>
</tr>
<tr>
<td>eaps-system</td>
<td>Specifies EAPS system level.</td>
</tr>
<tr>
<td>eaps-slave-msm</td>
<td>Specifies EAPS slave MSM level.</td>
</tr>
<tr>
<td>flow-redirect</td>
<td>Specifies flow redirect level.</td>
</tr>
<tr>
<td>flowstats</td>
<td>Specifies flow statistics level.</td>
</tr>
<tr>
<td>health-check</td>
<td>Specifies health check level.</td>
</tr>
<tr>
<td>iparp</td>
<td>Specifies IP ARP level.</td>
</tr>
<tr>
<td>iproute</td>
<td>Specifies IP routing level.</td>
</tr>
<tr>
<td>ipxgns-messages</td>
<td>Specifies IPX GNS message level.</td>
</tr>
<tr>
<td>ipxrip-message</td>
<td>Specifies IPX RIP message level.</td>
</tr>
<tr>
<td>ipxrip-route</td>
<td>Specifies IPX RIP route level.</td>
</tr>
<tr>
<td>ipxsap-entry</td>
<td>Specifies IPX SAP entry level.</td>
</tr>
<tr>
<td>ipxsap-message</td>
<td>Specifies IPX SAP message level.</td>
</tr>
<tr>
<td>isis-cli</td>
<td>Specifies ISIS CLI level.</td>
</tr>
<tr>
<td>isis-event</td>
<td>Specifies ISIS event level.</td>
</tr>
<tr>
<td>isis-hello</td>
<td>Specifies ISIS hello level.</td>
</tr>
<tr>
<td>isis-lsp</td>
<td>Specifies ISIS LSP level.</td>
</tr>
<tr>
<td>isis-snp</td>
<td>Specifies ISIS SNP level.</td>
</tr>
<tr>
<td>isis-spf</td>
<td>Specifies ISIS SPF level.</td>
</tr>
<tr>
<td>lcp</td>
<td>Specifies LCP level.</td>
</tr>
<tr>
<td>mpls</td>
<td>Specifies MPLS level.</td>
</tr>
<tr>
<td>mpls-signaling</td>
<td>Specifies MPLS signaling level.</td>
</tr>
<tr>
<td>nat</td>
<td>Specifies NAT level.</td>
</tr>
<tr>
<td>Option</td>
<td>Description</td>
</tr>
<tr>
<td>------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>ncp</td>
<td>Specifies NCP level.</td>
</tr>
<tr>
<td>netlogin</td>
<td>Specifies Network Login level.</td>
</tr>
<tr>
<td>npcard</td>
<td>Specifies NP card level.</td>
</tr>
<tr>
<td>npdiag</td>
<td>Specifies NP diagnostic level.</td>
</tr>
<tr>
<td>pim-cache</td>
<td>Specifies PIM cache level.</td>
</tr>
<tr>
<td>pim-hello</td>
<td>Specifies PIM hello level.</td>
</tr>
<tr>
<td>pim-message</td>
<td>Specifies PIM message level.</td>
</tr>
<tr>
<td>pim-neighbor</td>
<td>Specifies PIM neighbor level.</td>
</tr>
<tr>
<td>pim-rp-mgmt</td>
<td>Specifies PIM RP level.</td>
</tr>
<tr>
<td>pppauth</td>
<td>Specifies PPP authorization level.</td>
</tr>
<tr>
<td>ppphexdump</td>
<td>Specifies the level of the PPP hex dump.</td>
</tr>
<tr>
<td>radius</td>
<td>Specifies RADIUS level.</td>
</tr>
<tr>
<td>rip-message</td>
<td>Specifies RIP message level.</td>
</tr>
<tr>
<td>rip-route-change</td>
<td>Specifies RIP route level.</td>
</tr>
<tr>
<td>rip-triggered-update</td>
<td>Specifies RIP triggered update level.</td>
</tr>
<tr>
<td>slave-msm</td>
<td>Specifies slave MSM level.</td>
</tr>
<tr>
<td>slb-3dns</td>
<td>Specifies SLB 3DNS level.</td>
</tr>
<tr>
<td>slb-connection</td>
<td>Specifies SLB connection level.</td>
</tr>
<tr>
<td>slb-failover</td>
<td>Specifies SLB failover level.</td>
</tr>
<tr>
<td>snmp-trace</td>
<td>Specifies SNMP trace level.</td>
</tr>
<tr>
<td>stp-in-pdu</td>
<td>Specifies incoming STP PDU level.</td>
</tr>
<tr>
<td>stp-out-pdu</td>
<td>Specifies outgoing STP PDU level.</td>
</tr>
<tr>
<td>stp-system</td>
<td>Specifies STP system level.</td>
</tr>
<tr>
<td>t1</td>
<td>Specifies T1 level.</td>
</tr>
<tr>
<td>t3</td>
<td>Specifies T3 level.</td>
</tr>
<tr>
<td>transceiver-test</td>
<td>Specifies transceiver-test level.</td>
</tr>
</tbody>
</table>
Usage Guidelines

Use this command to display the debug trace level configured for a particular system and VLAN. Some of the debug trace systems commands can be applied to a particular VLAN, and some apply to the switch as a whole. Therefore, the `vlan` option is not available with all systems.

Example

The following command displays the debug trace levels configured:

```
show debug-trace
```

Following is the output from this command:

```
OSPF SPF                  3
Flowstats                3

Vlan                  Debug    Level
---------------------------------------------
v49                    DVMRP route  3

Port Number Debug Level
-----------------------
No port-based debug-tracing configured
```

History

This command was first available in ExtremeWare 6.1.

Beginning in ExtremeWare 7.1.0, many debug trace facilities were moved to EMS.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
show diagnostics

For the “i” series switches:

    show diagnostics {slot [<slot number> | msm-a | msm-b]}

For the “e” series switches:

    show diagnostics {slot [<slot-id-list>]}

Description

Displays information from the most recent diagnostic test run on the switch, as well as the status of the system health checker on “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot number</td>
<td>Specifies the slot number of an I/O module.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>slot-id-list</td>
<td>Specifies that the command applies to one or more switches in a stack.</td>
</tr>
<tr>
<td></td>
<td>The slot ID is the number of the switch in the stack.</td>
</tr>
<tr>
<td>msm-a</td>
<td>msm-b</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

Use this command to display the status of the system health checker on “i” series switches, as well as information from the last diagnostic test run on any switch. The switch diagnostics are displayed in a tabular format with the day, month, date, year, and time of the diagnostic test at the top of the table. Table 19 describes the fields that may be included in the command output. Refer to the examples in this section to see how some of this information is presented.

Table 19: Show Diagnostics Command Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Platform</td>
<td>Specifies system type.</td>
</tr>
<tr>
<td>System Part No.</td>
<td>Specifies system part number, revision level, and serial number.</td>
</tr>
<tr>
<td>Main Board No.</td>
<td>Specifies main board part number, revision level, and serial number.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Specifies system MAC address.</td>
</tr>
<tr>
<td>Slot</td>
<td>Specifies the slot for which the results are displayed.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>CPU System</td>
<td>Indicates diagnostic results.</td>
</tr>
<tr>
<td>Registers Test</td>
<td>Indicates diagnostic results.</td>
</tr>
<tr>
<td>Memory Test</td>
<td>Indicates diagnostic results.</td>
</tr>
<tr>
<td>System Test</td>
<td>Indicates diagnostic results.</td>
</tr>
</tbody>
</table>
To run diagnostics, use the following command:

```
run diagnostics [extended | normal]
```

To run diagnostics on an I/O module or MSM, use the following command:

```
run diagnostics [extended | normal] slot [msm-a | msm-b | <slot number>]
```

Depending on the software version running on your switch or the model of your switch, additional or different diagnostics information might be displayed.

**Examples**

The following command displays the results of module diagnostics for the MSM in slot B:

```
show diagnostics slot msm-b
```

The results are similar to the following:

```
-----------------------------------------------
Diagnostic Test Result run on Mon Feb 14 03:24:22 2005

-----------------------------------------------
| Slot   | B | SN : | 0015P10930 |
-----------------------------------------------
| CPU System     |   Passed |
-----------------------------------------------
| Registers Test |   Passed |
-----------------------------------------------
| Memory Test    |   Passed |
-----------------------------------------------
| System Test    |   Passed |
-----------------------------------------------

-----------------------------------------------
| Packet memory defect info for card msm-a |
-----------------------------------------------
| Num of defects = 0, num of recoverable defects = 0 |
-----------------------------------------------

The following command shows the results of diagnostics run on a stand-alone switch:

```
show diagnostics
```

The results are similar to the following:

```
-----------------------------------------------
Diagnostic Test Result run on Thu Sep 14 16:01:15 2000

-----------------------------------------------
| CPU System     |   Passed |
-----------------------------------------------
| Registers Test |   Passed |
-----------------------------------------------
| Memory Test    |   Passed |
-----------------------------------------------
| System Test    |   Passed |
-----------------------------------------------
```
History
This command was available in ExtremeWare 4.1.19, and in ExtremeWare 6.1.5.
The command was modified to include MSM modules in ExtremeWare 6.1.9.
The command was modified to support Alpine and Summit switches in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show diagnostics backplane arm mapping

    show diagnostics backplane arm mapping {active}

**Description**
Displays diagnostic information related to the ARM module internal backplane switch ports. This command also displays the external I/O port to internal ARM module backplane switch port mappings.

**NOTE**
This command is available only on the BlackDiamond switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Specifies to limit the port mapping display to active external I/O ports only.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command is only supported when the backplane load-sharing policy mode is port-based. If the active parameter is specified, the port mapping display is limited to active external I/O ports only. Used in conjunction with the `show diagnostics backplane utilization` command, these commands are helpful for diagnosing over-subscription problems related to backplane I/O port switch mappings.

**Example**
The following command displays diagnostic information related to the ARM module internal backplane switch ports:

```
show diagnostics backplane arm mapping
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

**Platform Availability**
This command is available only on the ARM module in the BlackDiamond switch.
show diagnostics backplane mpls mapping

    show diagnostics backplane mpls mapping {active}

**Description**
Displays diagnostic information related to the MPLS module internal backplane switch ports. This command also displays the external I/O port to internal MPLS module backplane switch port mappings.

**NOTE**
This command is available only on the BlackDiamond switch.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>active</td>
<td>Specifies to limit the port mapping display to active external I/O ports only.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command is only supported when the backplane load-sharing policy mode is port-based. If the active parameter is specified, the port mapping display is limited to active external I/O ports only. Used in conjunction with the `show diagnostics backplane utilization` command, these commands are helpful for diagnosing over-subscription problems related to backplane I/O port switch mappings.

**Example**
The following command displays diagnostic information related to the MPLS module internal backplane switch ports:

```
show diagnostics backplane mpls mapping
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

**Platform Availability**
This command is available only on the MPLS module in the BlackDiamond switch.
show diagnostics backplane utilization

show diagnostics backplane utilization

Description
Displays backplane link utilization information.

NOTE
This command is available only on the BlackDiamond switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Displays information including:
- Real-time traffic utilization on configured backplane links between active modules and MSM modules.
- The number of packets transmitted and received.
- The percentage of bandwidth used on the link.

Backplane utilization statistics can be reset by pressing 0 while the information is being displayed.

Example
The following command displays backplane link utilization information:
show diagnostics backplane utilization

History
This command was first available in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12.

Platform Availability
This command is available only on the ARM and MPLS modules in the BlackDiamond switch.
show diagnostics cable

    show diagnostics cable {ports [all | <portlist>] mode [auto | both | manual] detail}

Description
Displays the results of the last run cable diagnostics ports command.

Default
N/A

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Runs cable diagnostics for one or more port numbers.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Runs cable diagnostics for all ports.</td>
</tr>
</tbody>
</table>

Usage Guidelines
The results of the command display in tabular format:

Port—The port number tested

Pair—Each Ethernet cable consists of four copper pairs of Unshielded Twisted-Pair (UTP). To have a successful link, two of the four cables must have a status of Terminated and even lengths. The pairs are labeled A through D. The output shows the test results of each pair.

Length—The length of the cable. All pairs should have the same length. An uneven length can indicate a kink in the cable, or a broken connection.

Status—The result of the test. The status of Terminated indicates a successful completion. The status of Open or Short indicates a failure in the cable.

Examples
The following example tests the Ethernet cable inserted into port 1:

# run diagnostics cable ports 1
Cable Diagnostics has completed, to view results enter
show port <port list> cable diagnostics
# show port 1 cable diagnostics

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pair A</td>
<td>3 meters</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td>Pair B</td>
<td>2 meters</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td>Pair C</td>
<td>1 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair D</td>
<td>1 meters</td>
<td>Open or Short</td>
</tr>
</tbody>
</table>

The following example shows none of the twisted pairs terminate successfully at port 1:
# run diagnostics cable ports 1

Cable Diagnostics has completed, to view results enter

show port <port list> cable diagnostics

# show port 1 cable diagnostics

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pair A</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair B</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair C</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair D</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
</tbody>
</table>

**History**

This command was introduced in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
show diagnostics packet-memory slot

show diagnostics packet-memory [msm-a | mem-b | mem-c | msm-d | <slot number>]

Description
Displays the results of the packet memory scan on BlackDiamond 6808 and BlackDiamond 6816 I/O modules or MSMs.

NOTE
This command is available only on the BlackDiamond switch.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>msm-a</td>
<td>msm-b</td>
</tr>
<tr>
<td></td>
<td>slot number</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to display the results of a packet memory scan. The command output displays the number of defects identified, and the number that were recoverable. If packet memory defects were found, it displays information about each defect.

In ExtremeWare 6.2.1, this applies only to the G8Xi, G8Ti, G12SXi, and F48Ti. MSMs are not supported in this release. In ExtremeWare 6.2.2, this applies to all “i” series modules and switches.

Example
The following command displays the results of a PM scan for slot 2, where a single defect was found:

show diagnostics packet-memory slot 2

If no defects are found, the output will look similar to the following:

Packet memory defect info for card 1

Num of defects = 0, num of recoverable defects = 0

If defects are found, the output displays the number of defects, and provides information about each identified defect.
Packet memory defect info for card 2

Num of defects = 1, num of recoverable defects = 1

Defect information:

Defect entry 1
    recoverable = 0
    mem ID = 9
    bit position = 0
    address = 0x18baa

History

This command was first available in ExtremeWare 6.2.1.

Platform Availability

This command is available on all “i” series switches.
show diagnostics slot fdb

show diagnostics slot <slot-number> fdb {<mac_address> | vlan <vlan name> |
tls-tunnel <tunnel_name>}

Description
Displays the MAC cache for a specific MPLS module.

NOTE
This command is available only on the BlackDiamond switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot number</td>
<td>Specifies a slot.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies the MAC cache entry.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a name of a VLAN.</td>
</tr>
<tr>
<td>tunnel_name</td>
<td>Specifies a tunnel name.</td>
</tr>
</tbody>
</table>

Default
By default, the entire MAC cache is displayed.

Usage Guidelines
This command displays the MAC cache for a specific MPLS module. By default, the entire MAC cache
is displayed. If you specify the <mac_address> parameter, only the matching MAC cache entry is
displayed. Specifying the VLAN displays all MAC cache entries learned on the VLAN. Specifying the
TLS tunnel displays all MAC cache entries learned on the TLS tunnel. The MAC address, VLAN name,
and TLS tunnel name are displayed for each MAC cache entry.

Example
The following command displays the MAC cache entries learned on the VLAN test_1 for the MPLS
module in slot 2:
show diagnostics slot 2 fdb vlan test_1

History
This command was first available in an ExtremeWare IP Technology Services Release based on
ExtremeWare 6.1.8b12.

This command was subsequently updated in ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show ports cable diagnostics

For BlackDiamond switches:
   show ports <portlist> stat cable diagnostics

For Summit switches:
   show ports stat cable diagnostics

Description
Displays the results of the last `run cable diagnostics ports` command.

NOTE
This command is available only on the “i” series switches.

Default
N/A

Syntax Description

| portlist  | Shows cable diagnostics for one or more port numbers. |

Usage Guidelines

The results of the command display in tabular format:

Port—The port number tested

Pair—Each Ethernet cable is comprised of four copper pairs of Unshielded Twisted-Pair (UTP). To have a successful link, two of the four cables must have a status of Terminated and even lengths. The pairs are labeled A through D. The output shows the test results of each pair.

Length—The length of the cable. All pairs should have the same length. An uneven length can indicate a kink in the cable, or a broken connection.

Status—The result of the test. The status of Terminated indicates a successful completion. The status of Open or Short indicates a failure in the cable.

Examples
The following example tests the Ethernet cable inserted into port 1:

```
Summit400-48t:27 # run diagnostics cable ports 1
Cable Diagnostics has completed, to view results enter
show port <port list> cable diagnostics
Summit400-48t:28 # show port 1 cable diagnostics
```

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
</table>

1232 ExtremeWare 7.5 Command Reference Guide
show ports cable diagnostics

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pair A</td>
<td>3 meters</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td>Pair B</td>
<td>2 meters</td>
<td>Terminated</td>
</tr>
<tr>
<td></td>
<td>Pair C</td>
<td>1 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair D</td>
<td>1 meters</td>
<td>Open or Short</td>
</tr>
</tbody>
</table>

The following example shows none of the twisted pairs terminate successfully at port 1:

Summit400-48t:29 # run diagnostics cable ports 1
Cable Diagnostics has completed, to view results enter
show port <port list> cable diagnostics

Summit400-48t:30 # show port 1 cable diagnostics

<table>
<thead>
<tr>
<th>Port</th>
<th>Pair</th>
<th>Length</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Pair A</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair B</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair C</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
<tr>
<td></td>
<td>Pair D</td>
<td>0 meters</td>
<td>Open or Short</td>
</tr>
</tbody>
</table>

**History**

This command was introduced in ExtremeWare 7.2e.

**Platform Availability**

This command is available only on “i” series platforms.
Troubleshooting Commands

show system-dump

Description
Displays the system-dump server IP and dump-timeout.

NOTE
This command is available only on switches with an Ethernet management port.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this command to display configured parameters for a system dump transfer. Dump transfers should not be initiated without the assistance of Technical Support.

Table 20 lists the fields displayed by this command.

Table 20: show system-dump command fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server ip</td>
<td>Displays the IP address to which a triggered system dump is sent. Indicates whether the server is reachable through the VLAN mgmt.</td>
</tr>
<tr>
<td>Dump timeout</td>
<td>Displays the time in seconds until a system dump transfer is halted.</td>
</tr>
</tbody>
</table>

To specify the IP address to which a system dump is sent, use the following command:

configure system-dump server

To specify the timeout, use the following command:

configure system-dump timeout

Example
The following command displays the system-dump server IP and dump-timeout:

show system-dump

Following is the output from this command with nothing configured:

Server ip : none
Dump timeout : none
Following is the output from this command with both an IP address and timeout configured:

Server ip : 10.5.2.82 (ok)
Dump timeout : 300 seconds

Following is the output from this command with an unreachable IP address:

Server ip : 1.2.3.4 - currently unreachable via "Mgmt" vlan
Dump timeout : 300 seconds

**History**

This command was first available in ExtremeWare 6.2.2.

**Platform Availability**

This command is available on platforms with an Ethernet management port.
show tech-support

    show tech-support [brief | all]

Description
Displays the output of various show commands to assist in monitoring and troubleshooting the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>brief</td>
<td>Specifies that all output will be displayed with the exception of FDB content (that is, L2FDB and IPFDB output).</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all output will be displayed, including FDB content (that is, L2FDB and IPFDB output).</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

Use this command to display detail information for a switch to assist in troubleshooting. In some environments, showing all the available information by using the all keyword can possibly lead to performance problems when used on switches with a large number of table entries. To control the output by limiting the output detail, use the brief keyword if your system supports it.

Use the show tech-support all form of the command to display all output for the following show commands:

- show version
- show switch
- show configuration
- show diag
- show slot (Supported only on “i” series switches)
- show fdb
- show iparp
- show ipfdb
- show ipstats
- show iproute
- show ipmc cache detail
- show ipmc fdb
- show igmp snooping detail
- show memory detail
- show log
- All show commands for wireless status

Use the show tech-support brief form of the command to display all the output shown above except for FDB output (that is, L2FDB and IPFDB output).
This command also displays the output from internal debug commands. This command disables the CLI paging feature.

This information can be useful for your technical support representative if you experience a problem. Depending on the software version running on your switch, additional or different show command output is displayed.

Use the `show tech-support wireless` form of the command to display output related to wireless only.

**Example**
The following command displays all the show command output on the switch:

```plaintext
show tech-support all
```

**History**
This command was first available in ExtremeWare 6.1.9.

This command was modified to capture the `show ipmc fdb` command output in ExtremeWare 6.22.

This command was modified to provide the `brief` and `all` keywords in ExtremeWare 7.3.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
top

top

Description
Displays real-time CPU utilization information by process.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this command to show the percentage of CPU processing devoted to each task, sampled every 30 seconds. In a healthy ExtremeWare system, only the BGTask uses significant CPU processing power. Investigate tasks showing consistent or periodic high CPU utilization.

You can change the display by typing a character while the display is active. These single character commands are as follows:

<table>
<thead>
<tr>
<th>u</th>
<th>Go up one screen</th>
</tr>
</thead>
<tbody>
<tr>
<td>d</td>
<td>Go down one screen</td>
</tr>
<tr>
<td>c</td>
<td>Clear max utilization</td>
</tr>
<tr>
<td>%</td>
<td>Sort tasks by CPU utilization</td>
</tr>
<tr>
<td>t</td>
<td>Sort tasks by task id</td>
</tr>
<tr>
<td>p</td>
<td>Sort tasks by program counter</td>
</tr>
<tr>
<td>n</td>
<td>Sort tasks by name</td>
</tr>
<tr>
<td>s</td>
<td>Sort tasks by task state</td>
</tr>
<tr>
<td>m</td>
<td>Sort tasks by max CPU utilization</td>
</tr>
<tr>
<td>h</td>
<td>Show the help screen</td>
</tr>
<tr>
<td>&lt;space&gt;</td>
<td>go to next sort type</td>
</tr>
<tr>
<td>q</td>
<td>Exit top</td>
</tr>
<tr>
<td>&lt;esc&gt;</td>
<td>Exit top</td>
</tr>
</tbody>
</table>

Table 21: TOP command display options

Table 22 defines the tasks. Depending on your switch model and the functions it is executing, you will see only a subset of these tasks.
### Table 22: ExtremeWare Task Descriptions

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>httpd</td>
<td>The HTTP daemon task manages the HTTP web management interface on the system.</td>
</tr>
<tr>
<td>Logpoll</td>
<td>In an active dual CPU system, the master CPU will initiate the log polling task (Logpoll) to periodically poll the secondary or slave CPU(s). This process clears the individual syslogs and consolidates them onto the master CPU switch log.</td>
</tr>
<tr>
<td>mportTask</td>
<td>The management port task.</td>
</tr>
<tr>
<td>pfifstate</td>
<td>The port interface state task (pfifstate) processes port link state changes. It is watchdog timer poll driven as opposed to interrupt driven by hardware events.</td>
</tr>
<tr>
<td>tAgentX</td>
<td>This task is used for Agent-X implementation on the switch.</td>
</tr>
<tr>
<td>tAgentXTrips</td>
<td>This task is used to process Agent-X related traps.</td>
</tr>
<tr>
<td>tAsyncSave</td>
<td>The tAsyncSave tasks the NVRAM asynchronous save/write processing task. This process manages the save or writes to the NVRAM.</td>
</tr>
<tr>
<td>tAXDn</td>
<td>The tAXDn task is used to download the configuration to the sub agent.</td>
</tr>
<tr>
<td>tAxSub</td>
<td>This task is used to register the Agent-X subagent (local subagent residing on the switch) with the Agent-X master.</td>
</tr>
<tr>
<td>tAXTimerTask</td>
<td>The tAXTimerTask task is used to process Agent-X related timers.</td>
</tr>
<tr>
<td>tbgpTask</td>
<td>The border gateway protocol task (tbgpTask) implements and processes BGP on the switch.</td>
</tr>
<tr>
<td>tbgpTimerTask</td>
<td>The BGP internal process timer task (tbgpTimerTask) manages the internal BGP timer delays for checking BGP networks and next hops.</td>
</tr>
<tr>
<td>tBgQosMon</td>
<td>The background Quality of Service monitor task (tBgQosMon) is a background version of the QoS monitoring task that monitors transmit count and kill count of ports and cycles as long as the monitor is enabled.</td>
</tr>
<tr>
<td>tBGTask</td>
<td>The background task (tBGTask) is the core task switching process. It receives packets from the hardware ASICs and switches them to the appropriate functional task to process that packet type or group. The tBGTask typically runs with a high CPU utilization (90% or greater). It is constantly checking for packets to be sent up by the hardware ASICs. It only releases control of the CPU if packets are sent to the switch or if timer functions signal another task to become active.</td>
</tr>
<tr>
<td>tCardTask</td>
<td>The I/O card event task (tCardTask) manages the event signaling hardware and state machine for the I/O modules in a chassis-based system.</td>
</tr>
<tr>
<td>tcdmTask</td>
<td>This cable diagnostic module takes care of cable diagnostic routines.</td>
</tr>
<tr>
<td>tChecksumPoll</td>
<td>The checksum polling task (tChecksumPoll) periodically polls the boards for fabric checksum errors.</td>
</tr>
<tr>
<td>tConsole</td>
<td>The console task.</td>
</tr>
<tr>
<td>tdiagTask</td>
<td>The diagnostic task (tdiagTask) executes the diagnostic routines for the particular hardware platform.</td>
</tr>
<tr>
<td>tDvmrpTask</td>
<td>The distance vector multicast routing protocol task (tDvmrpTask) implements and processes DVMRP on the switch.</td>
</tr>
<tr>
<td>tEapsTask</td>
<td>The Ethernet automatic protection switching task implements and processes EAPS on the switch.</td>
</tr>
<tr>
<td>tEdpTask</td>
<td>The Extreme Discovery Protocol task (tEdpTask) implements and processes the EDP neighbor discovery process.</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>The Extreme Standby Router Protocol (tEsrpTask) implements and processes ESRP on the switch.</td>
</tr>
</tbody>
</table>
Table 22: ExtremeWare Task Descriptions (Continued)

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tExcTask</td>
<td>If the operating system recognizes an exception condition, it will invoke the exception handling task (tExcTask).</td>
</tr>
<tr>
<td>tFastTimer</td>
<td>The fast timer task (tFastTimer) is used to maintain a queue of timer events triggering periodic or single event functions. These events have a small delay in time between re-occurrences. The tFastTimer has a higher priority than the slow timer task (tSlowTimer). Therefore, tFastTimer events are processed prior to tSlowTimer events occurring at the same time.</td>
</tr>
<tr>
<td>tfdbAgeTask</td>
<td>The forwarding database aging task (tfdbAgeTask) performs the aging of MAC FDB entries in the hardware and software tables.</td>
</tr>
<tr>
<td>tIpXTask</td>
<td>The IPX input task (tIpXTask) handles inbound IPX control packets such as RIP, SAP, and Xping.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>tIpXTx</td>
<td>The IPX transmit task (tIpXTx) handles the IPX transmission of control packets such as RIP and SAP.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>tIquery</td>
<td>The iQuery support task for 3DNS (tIquery) processes iQuery requests.</td>
</tr>
<tr>
<td>TIRDP</td>
<td>The ICMP router discovery protocol task (TIRDP) implements and processes IRDP on the switch.</td>
</tr>
<tr>
<td>tISRtask</td>
<td>The interrupt service routine task (tISRtask) manages the interrupt driven port link state changes.</td>
</tr>
<tr>
<td>tLinkEvent</td>
<td>The link event task (tLinkEvent) is the interrupt driven link event processing task. It handles hardware interrupts for link events.</td>
</tr>
<tr>
<td>tMACPoll</td>
<td>The media access controller poll task (tMACPoll) polls the various MAC PHY chips on the switch to pull up MAC Layer control messages for the CPU to process.</td>
</tr>
<tr>
<td>tmt32LinkPoll</td>
<td>F32F module link poll task.</td>
</tr>
<tr>
<td>tmuTelnetd</td>
<td>The telnet daemon task.</td>
</tr>
<tr>
<td>tNetTask</td>
<td>The network stack task (tNetTask) handles all the software-based processing of packets including:</td>
</tr>
<tr>
<td></td>
<td>• Packets that cannot be handled by the switch’s ASIC because the forwarding tables do not have entries built in.</td>
</tr>
<tr>
<td></td>
<td>• Packets destined to the CPU for one of the router interfaces.</td>
</tr>
<tr>
<td></td>
<td>• Packets that must be examined or snooped by the CPU.</td>
</tr>
<tr>
<td>tNMCEvent</td>
<td>The network management controller event task (tNMCEvent) manages event signaling hardware and state machine on a BlackDiamond switch’s redundant MSM CPU modules.</td>
</tr>
<tr>
<td>tOpenPort</td>
<td>A server load balancing (SLB) Layer 4/Layer 7 health check sub-task.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>tospfMsgTask</td>
<td>The OSPF message processing task (tospfMsgTask) implements and manages the processing of OSPF messages.</td>
</tr>
<tr>
<td>tospfSpfTask</td>
<td>The OSPF shortest path forward task (tospfSpfTask) executes the SPF algorithm run processing for OSPF.</td>
</tr>
<tr>
<td>tospfTimer</td>
<td>The OSPF timer task (tospfTimer) manages the internal timer trigger functions and delays for OSPF.</td>
</tr>
<tr>
<td>tPCSPoll</td>
<td>The tPCSPoll task services the Gigabit Ethernet PCS poll messages.</td>
</tr>
<tr>
<td>tPhyPoll</td>
<td>The PHY layer poll task (tPhyPoll) polls the Road Runner PHY layer every 2 seconds to verify the proper operation.</td>
</tr>
</tbody>
</table>
Investigate tasks that, for no apparent reason, show CPU utilization consistently above 25% (except for the BGTask). Configure the appropriate debug-trace command and look for messages indicating a problem. Common problems are source or destination addresses.

<table>
<thead>
<tr>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tPimTask</td>
<td>The protocol independent multicast task (tPimTask) implements and processes PIM on the switch.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “I” series switches.</td>
</tr>
<tr>
<td>tPingServer</td>
<td>The server load balancing (SLB) Layer 3 ping health check sub-task.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “I” series switches.</td>
</tr>
<tr>
<td>tPortProbe</td>
<td>A server load balancing (SLB) Layer 4/Layer 7 health check sub-task.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “I” series switches.</td>
</tr>
<tr>
<td>tPortUtilization</td>
<td>The port utilization data collection task (tPortUtilization) is a 30 second task that pulls physical port data statistics from the hardware and updates the software database tables.</td>
</tr>
<tr>
<td>tRip</td>
<td>The Routing Information Protocol task (tRip) implements and processes RIP on the switch.</td>
</tr>
<tr>
<td>tRipTimer</td>
<td>The RIP timer task (tRipTimer) manages the internal timer trigger functions and delays for RIP.</td>
</tr>
<tr>
<td>TRmonTask</td>
<td>The remote monitoring task</td>
</tr>
<tr>
<td>tRRPoll</td>
<td>The Road Runner poll task (tRRPoll) pulls the MAC and PHY layer statistics from the store in the software based tables.</td>
</tr>
<tr>
<td>tRxMsgTask</td>
<td>The receive message task (tRxMsgTask) is located on the secondary system. ExtremeWare 6.2 commences use of the secondary CPU in BlackDiamond switches. This is the secondary slave CPU inter-CPU receive task.</td>
</tr>
<tr>
<td>tServAlive</td>
<td>The server load balancing (SLB) health check server task.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “I” series switches.</td>
</tr>
<tr>
<td>tShell</td>
<td>The core operating system internal shell process (tShell) is spawned whenever the internal shell is accessed.</td>
</tr>
<tr>
<td>tSlbFailover</td>
<td>The server load balancing failover task.</td>
</tr>
<tr>
<td>tSlowTimer</td>
<td>The slow timer task (tSlowTimer) maintains a queue of timer events triggering periodic or single event functions. Typically these events have a large period gap in terms of time between recurrences.</td>
</tr>
<tr>
<td>tsmartTrap</td>
<td>Extreme smart trap task.</td>
</tr>
<tr>
<td>tSnmpd</td>
<td>The SNMP daemon task manages all SNMP processing on the system.</td>
</tr>
<tr>
<td>tSntpc</td>
<td>The simple network time protocol client task (tSntpc) implements the SNTP client function and processing.</td>
</tr>
<tr>
<td>tsshshell</td>
<td>The secure shell (SSH) task.</td>
</tr>
<tr>
<td>tStatsPoll</td>
<td>The port interface statistics poll task (tStatsPoll) polls the port interfaces for statistic counters.</td>
</tr>
<tr>
<td>tstpTask</td>
<td>The Spanning Tree protocol task (tstpTask) implements the STP algorithm and processing.</td>
</tr>
<tr>
<td>tSwFault</td>
<td>The software fault handler task (tSwFault) will perform a stack dump for any task that has crashed.</td>
</tr>
<tr>
<td>tsyslogTask</td>
<td>The system log task (tsyslogTask) receives messages/text from other tasks and asynchronously logs these to the switch NVRAM log area.</td>
</tr>
<tr>
<td>tTimeout</td>
<td>The Timeout task (tTimeout) is used to manage and execute various functions on timeouts.</td>
</tr>
<tr>
<td>tTRRecv</td>
<td>The trace route receiver task (tTRRecv) is spawned dynamically when the trace route utility is used.</td>
</tr>
<tr>
<td>tvrrpTask</td>
<td>The virtual router redundancy protocol task (tvrrpTask) implements and processes VRRP on the switch.</td>
</tr>
</tbody>
</table>
Example

The following command displays the show command output on the switch:

```
top
```

The output of this command looks similar to the following:

```
Total number of tasks: 46

<table>
<thead>
<tr>
<th>Task Name</th>
<th>Task Id</th>
<th>Task PC</th>
<th>Status</th>
<th>% CPU</th>
<th>Max % util</th>
</tr>
</thead>
<tbody>
<tr>
<td>tBGTask</td>
<td>8136f18e0</td>
<td>80748f98</td>
<td>READY</td>
<td>99</td>
<td>99</td>
</tr>
<tr>
<td>tExcTask</td>
<td>8137ce90</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tLogTask</td>
<td>8135e2a0</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tSlowTimer</td>
<td>813ccf50</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tFastTimer</td>
<td>813ff1f0</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tTimeout</td>
<td>81384f50</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tsyslogTas</td>
<td>81389660</td>
<td>8075ab2c</td>
<td>PEND+T</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tledPollTa</td>
<td>81390ef0</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tAsyncSave</td>
<td>814feb10</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tpifstate</td>
<td>81a85590</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbgpTask</td>
<td>81eaacc0</td>
<td>807169f4</td>
<td>PEND+T</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tbgpTimerT</td>
<td>81eaecd0</td>
<td>80749164</td>
<td>DELAY</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tBQosMon</td>
<td>81eb6be0</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tEapsTask</td>
<td>82bd2a00</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tSwFault</td>
<td>82c75530</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tFdbAgeTas</td>
<td>82c85530</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tFdbSyncTa</td>
<td>82c89530</td>
<td>807489a0</td>
<td>SUSPEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tdiagTask</td>
<td>82c8d620</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tIPxTask</td>
<td>82c91620</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>tIPxTx</td>
<td>836e97f0</td>
<td>8075ab2c</td>
<td>PEND</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
```

Press ‘h’ for help

History

This command was available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
unconfigure system-dump

unconfigure system-dump

Description
Unconfigures the system dump.

NOTE
This command is available only on the “i” series switches.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Returns the system-dump configuration to the defaults.

Example
The following command unconfigures the system dump:
unconfigure system-dump

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is available only on platforms with an Ethernet management port.
upload system-dump

    upload system-dump [<ip address>]

Description
This command transfers a system dump to an IP address.

NOTE
This command is available only on the “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies the IP address to which to transfer a system dump.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify an IP address, the configured system-dump server IP address is used.

Example
The following command transfers a system dump to 10.10.10.1:

upload system-dump 10.10.10.1 3

History
This command was first available in ExtremeWare 6.2.2.

Platform Availability
This command is available only on platforms with an Ethernet management port.
The Alpine switches, Summit 300 series switches and the Altitude 300 wireless port extend network service to wireless 802.11a/b/g clients within a fully integrated network infrastructure. Ports on the Summit 300 switch handle all of the management functions typically associated with an access point. The Altitude 300 wireless port serves as the radio transmitter and receiver, inheriting configuration information as soon as it is attached to the switch and as changes are made to the wireless profiles after the system is deployed.

**Summary of Wireless Features**

The Alpine and Summit 300 series switches support the following wireless features:

- Simultaneous support for 802.11a, 802.11b, and 802.11g
- EAP authentication for 802.1X devices—Protected Extensible Authentication Protocol (PEAP), EAP Tunneled TLS Authentication Protocol (EAP-TTLS), and Extensible Authentication Protocol Transport Layer Security (EAP-TLS)
- Wi-Fi Protected Access (WPA) using Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES)
- Per-user VLAN classification
- AccessAdapt™ management
- Remote troubleshooting
- Easy upgrading of wireless ports
- Detailed reports and logging

**Wireless Devices**

You configure ports on the Summit 300 or Alpine switch with the “personality” of the device to be connected. Each port contains separately configurable interfaces for each of its two radios (A and G).

Physical security for the wireless networks ceases to be a problem at the wireless access location because the Altitude 300 wireless port does not store any security settings. Information is not stored in the Altitude 300 wireless port, but loaded as needed from the switch. Even if the Altitude 300 wireless port is physically moved, it can only be reconnected to another Summit 300 model.

You can set network policies at layers 2 and 3 to cover both the wired and wireless networks. In this way you can block access to individuals suspected of intrusion across the entire network infrastructure.
In addition to traditional wired devices, the switch supports the Altitude 300 wireless port, third party access points, and devices that rely on Power over Ethernet (PoE).

**Command Support for Virtual Ports**

All ExtremeWare wireless commands support virtual ports, which are used with the Remote Connect feature (see Chapter 26). Virtual port numbers can range from 1 to 48; however, a maximum of 24 virtual ports can be configured at one time on a Summit 300-48 switch. Virtual ports are accommodated in the ExtremeWare CLI using the following convention for the <port> variable, where n is the port number:

<table>
<thead>
<tr>
<th>&lt;port&gt; value</th>
<th>Description</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:n</td>
<td>Physical port, Summit 300-48, Alpine 3800 series</td>
<td>configure wireless ports 1:2</td>
</tr>
<tr>
<td>n</td>
<td>Physical port, Summit 300-24</td>
<td>configure wireless port 2</td>
</tr>
<tr>
<td>virtual:n</td>
<td>Virtual port, Summit 300-48</td>
<td>configure wireless port virtual:2</td>
</tr>
</tbody>
</table>
clear APmgmt port history

clear APmgmt port <vport> history

**Description**
Deletes the information about the Altitude 300 wireless port currently running on the specified virtual port.

**Syntax Description**

| vport | Specifies a virtual port on the switch in the format virtual:n, where n is the virtual port number. |

**Default**
N/A.

**Usage Guidelines**
N/A.

**Example**
clear APmgmt port virtual:21 history

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on Summit 300-48, Summit 300-24, Summit 400-24p and Alpine 3800 switches.
clear wireless ports counters

    clear wireless ports [all | <portlist>] counters

Description
Clears the counters on one or more wireless ports.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to clear the counters for all wireless ports or for a port list.

Example
The following example clears all the counters for wireless ports:

clear wireless ports all counters

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
clear wireless ports interface ap-scan results

```
clear wireless ports [<portlist> | all] interface [1 | 2] ap-scan results
```

Description
This command clears the scan results table.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to clear the access point (AP) scan results on any interface: 1 or 2.

Examples
The following command clears the AP scan result table for port 1:18 on interface 1:
```
clear wireless port 1:18 interface 1 ap-scan results
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
clear wireless ports interface client-history

**Description**
Cleans the counters for a specific MAC address or for all clients.

**Syntax Description**

<table>
<thead>
<tr>
<th>Specification</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mac-address</td>
<td>Specifies the MAC address of the client network interface card.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Although this command clears the counters, client entries are not removed from the client information database.

**Example**
The following example clears the client-history counters on all ports and interface 1:

clear wireless ports all interface 1 client-history all

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
clear wireless ports interface client-scan counters

clear wireless ports [<portlist> | all] interface [1 | 2] client-scan counters [<hexoctet> | all]

Description
Clears the statistics associated with a particular client or with all clients.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>hexoctet</td>
<td>Specifies to use the hexadecimal value to identify a particular entry in the client scan information table.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all entries in the client scan information table.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to clear client scan counters on any interface: 1 or 2.

Examples
The following example clears ports 15 and interface 1 of all client-scan statistics:

clear wireless ports 15 interface 1 client-scan counters all

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
clear wireless ports interface client-scan results


**Description**
Cleans the contents of the client scan information table or for a specific client MAC address.

**Syntax Description**

| portlist | Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| all      | Specifies all ports. |
| interface| Specifies an interface: 1 or 2. |
| hexoctet | Specifies to use the hexadecimal value to identify a particular entry in the client scan information table. |
| all      | Specifies all entries in the client scan information table. |

**Default**
N/A

**Usage Guidelines**
Use this command to clear the client scan results on any interface: 1 or 2.

**Examples**
The following example clears ports 15 and interface 1 of all client-scan results:
clear wireless ports 15 interface 1 client-scan results all

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
clear wireless ports log

    clear wireless ports [all | <portlist>] log

Description
Clears the log on one or more wireless ports.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to clear the log for all wireless ports or for a port list.

Example
The following example clears the counters for wireless port 1:1:

clear wireless ports 1:1 counters

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure antenna-profile

configure antenna-profile <antenna_profile_name> 2.4ghz-gain <x> 5ghz-gain <y>

Description
Configure the antenna profile gain for the 2.4 GHz and 5 GHz bands.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>antenna_profile_name</td>
<td>Identifies the antenna profile.</td>
</tr>
<tr>
<td>x</td>
<td>Specifies the antenna gain for the 2.4 GHz band. (0-6dBi)</td>
</tr>
<tr>
<td>y</td>
<td>Specifies the antenna gain for the 5GHz band. (0-6dBi)</td>
</tr>
</tbody>
</table>

Default
4 dBi for the 2.4 GHz and 5 GHz bands

Usage Guidelines
N/A

Example
The following command configures the antenna profile antenna1 for antenna gain of 6 dBi in the 2.4 GHz band and 2 dBi in the 5 GHz band.

configure antenna-profile antenna1 2.4ghz-gain 6 5ghz-gain 2

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on Summit 300-48, Summit 300-24, Summit 400-24p and Alpine 3800 switches.
configure rf-profile beacon-interval

    configure rf-profile <name> beacon-interval <value>

**Description**
Specifies the frequency interval of the beacon in milliseconds.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the RF profile.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the interval of the beacon in milliseconds. Valid values are from 20 to 1000.</td>
</tr>
</tbody>
</table>

**Default**
40 ms

**Usage Guidelines**
A beacon is a packet broadcasted by the wireless port to synchronize the wireless network. The beacon-interval is the time in milliseconds between beacons.

**Examples**
The following command sets the beacon interval to 100 ms:

```
configure rf-profile rfprof1 beacon-interval 100
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure rf-profile dtim-interval

    configure rf-profile <name> dtim-interval <value>

**Description**
Specifies the interval of the delivery traffic indication message (DTIM) in number of beacons.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the RF profile.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the interval of the DTIM indicating the number of beacons. Valid values are integers from 1 to 100. The default value is 2.</td>
</tr>
</tbody>
</table>

**Default**
2

**Usage Guidelines**
A DTIM field is a countdown field informing clients of the next listening window to broadcast and multicast messages. When the wireless port has buffered broadcast or multicast messages, it sends the next DTIM with a DTIM interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.

Clients achieve greater power savings with larger DTIM intervals. However, a larger DTIM interval will increase the delay before multicast frames are delivered to all stations.

**Examples**
The following command sets the DTIM interval to every 5 beacons:

```
configure rf-profile rfprof1 dtim-interval 5
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure rf-profile frag-length

configure rf-profile <name> frag-length <value>

Description
Specifies the fragment size in bytes.

Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the RF profile.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the fragment size in bytes. Valid values are from 256 to 2345.</td>
</tr>
</tbody>
</table>

Default
2345 bytes

Usage Guidelines
This value should remain at its default setting of 2345. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.

Examples
The following command sets the fragment size to the default setting:

```
configure rf-profile rfprof1 frag-length 2345
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure rf-profile long-retry

    configure rf-profile <name> long-retry <value>

Description
Specifies the number of transmission attempts of a frame larger than the request-to-send (RTS) threshold.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the RF profile.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the number of transmission attempts of a frame. Valid values are from 1 to 255.</td>
</tr>
</tbody>
</table>

Default
7

Usage Guidelines
Use this command to set the number of transmission attempts for frames larger than the RTS threshold setting in the same RF profile. The long-retry value specifies the number of attempts before a frame will be discarded when a station attempts to retransmit a frame. Long retry applies to frames longer than the RTS threshold and it is set to 7 by default. A frame requiring RTS/CTS clearing is retransmitted seven times before being discarded.

To specify the number of transmission attempts of a frame smaller than the RTS threshold, use the following command:

    configure rf-profile <name> rts-threshold <value>.

Examples
The following command sets the transmission attempts to 10:

    configure rf-profile rfprof1 long-retry 10

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure rf-profile preamble

configure rf-profile <name> preamble [short | long]

Description
Specifies the size of the packet preamble.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>short</th>
<th>long</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the names of the RF profile.</td>
<td>Specifies 802.11a.</td>
<td>Specifies 802.11b and 802.11g.</td>
</tr>
</tbody>
</table>

Default
Short

Usage Guidelines
Use this command to configure the RF profile for 802.11b using the long packet preamble. Configure the RF profile for 802.11a and 802.11g using the short packet preamble.

Examples
The following command sets the preamble to long:

```
configure rf-profile rfprof1 preamble long
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure rf-profile rts-threshold

configure rf-profile <name> rts-threshold <value>

Description
Specifies the request to send (RTS) threshold in bytes.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the names of the RF profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Specifies the RTS threshold in bytes. Valid values are from 0 to 2347.</td>
</tr>
</tbody>
</table>

Default
2330 bytes

Usage Guidelines
Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS and clear-to-send (CTS) mechanism is not enabled. The wireless port sends RTS frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a CTS frame to acknowledge the right to begin transmission.

Examples
The following command sets the RTS threshold to the default setting:

configure rf-profile rfprof1 rts-threshold 2330

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure rf-profile short-retry

   configure rf-profile <name> short-retry <value>

Description
Specifies the number of transmission attempts of frames smaller than the request-to-send (RTS) threshold.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the names of the RF profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>Specifies the number of transmission attempts of a frame. Valid values are from 1 to 255.</td>
</tr>
</tbody>
</table>

Default
4

Usage Guidelines
Use this command to set the number of transmission attempts for frames smaller than the RTS threshold setting in the same RF profile. The short-retry value specifies the number of attempts before a frame will be discarded when a station attempts to retransmit a frame. Short retry applies to frames shorter than the RTS threshold and it is set to 4 by default. A frame requiring RTS/CTS clearing is retransmitted four times before being discarded.

To specify a the number of transmission attempts of a frame larger than the RTS threshold, use the following command:

   configure rf-profile <name> long-retry <value>.

Examples
The following command sets the transmission attempts to 3:

   configure rf-profile rfprof1 short-retry 3

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless country-code

configure wireless country-code <code>

Description
Configures the country identifier for the switch.

Syntax Description

| code | Sets the country identifier for the switch. |

Default
Extreme_default

Usage Guidelines
When the Summit 300 is set to factory defaults, you must configure the correct country code using the country code properties listed in the following table. The country code feature allows you to configure the approved 802.11a or 802.11b/g “channels” applicable to each of the supported countries.

<table>
<thead>
<tr>
<th>Australia</th>
<th>Austria</th>
<th>Belgium</th>
<th>Canada</th>
<th>China</th>
<th>Denmark</th>
</tr>
</thead>
<tbody>
<tr>
<td>extreme_default</td>
<td>Finland</td>
<td>France</td>
<td>Germany</td>
<td>Greece</td>
<td>Hong_Kong</td>
</tr>
<tr>
<td>Iceland</td>
<td>Ireland</td>
<td>Italy</td>
<td>Japan</td>
<td>Korea_Republic</td>
<td>Liechtenstein</td>
</tr>
<tr>
<td>Luxembourg</td>
<td>Mexico</td>
<td>Netherlands</td>
<td>Norway</td>
<td>Portugal</td>
<td>Spain</td>
</tr>
<tr>
<td>Sweden</td>
<td>Switzerland</td>
<td>Taiwan</td>
<td>Thailand</td>
<td>UK</td>
<td>USA</td>
</tr>
</tbody>
</table>

Extreme Networks ships the Summit 300 to be programmed with Extreme Network's special extreme_default country code, which brings up only the B/G radio in channel 6, and turns off the A radio. When an Altitude 300 wireless port is connected and the Summit 300 is unable to determine the country for which the Altitude is programmed, then the extreme_default country code is used. You must program the country code on the Summit 300 to enable the remaining channels for the desired country.

The Altitude 300 wireless port is shipped with a pre-programmed code for the following countries:

- North America (United States, Canada, Hong Kong)
- Japan
- Taiwan
- European Union and the Rest of the World.

If you do not program the country code in the Summit 300, then the switch inherits the country code of the first Altitude 300 wireless port that connects to it, if the Altitude is not programmed for the European Union and the Rest of World.

If there is a mismatch between the country codes between the Altitude 300 wireless port and the code programmed on the Summit 300, the Altitude 300 wireless port is not allowed to come up.
Example
The following example configures the switch level property for Spain:

```
configure wireless country-code Spain
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless default-gateway

configure wireless default-gateway <ip_address>

Description
Configures the default gateway IP address.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip_address</td>
<td>Indicates the IP address of the default gateway. By default, this is the same IP address as the management VLAN.</td>
</tr>
</tbody>
</table>

Default
0.0.0.0.

Usage Guidelines
The wireless default gateway IP address is usually set to the wireless management VLAN address. This address is used by all wireless client traffic whose destination is upstream switches.

Example
The following example configures the switch level property for the default gateway:

```
configure wireless default-gateway 192.168.1.1
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless management-vlan

configure wireless management-vlan <vlan name>

Description
Identifies the VLAN on which the Altitude 300 wireless port communicates with the Summit 300 switch.

Syntax Description

<table>
<thead>
<tr>
<th>vlan name</th>
<th>The name of the VLAN with which the Altitude 300 wireless port communicates with the Summit 300 switch.</th>
</tr>
</thead>
</table>

Default
Default VLAN

Usage Guidelines
Identifying the VLAN on which the Altitude 300 wireless port communicates with the switch is required before wireless features can work. This VLAN can be the default VLAN and it can either have a public or private IP address. This VLAN is an untagged VLAN on which all the Altitude 300 devices are connected.

Example
The following example configures the switch level property for the default gateway:

```
configure wireless management-vlan Default
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless port antenna-profile

configure wireless port <port> antenna-profile <antenna_profile_name>

Description
Bind a switch port to a specific antenna profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Identifies a port on the switch.</td>
</tr>
<tr>
<td>antenna_profile_name</td>
<td>Identifies the antenna profile.</td>
</tr>
</tbody>
</table>

Default
detachable_extr_15901

Usage Guidelines
N/A.

Example
The following command binds antenna profile antenna1 to port 1:2 on the switch.
configure wireless port 1:2 antenna-profile antenna1

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on Summit 300-48, Summit 300-24, Summit 400-24p and Alpine 3800 switches.
configure wireless ports antenna-location

configure wireless ports [<portlist> | all] antenna-location <indoor | outdoor>

Description
Sets the Altitude 300-2d detachable antenna for indoor or outdoor use.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>indoor</td>
<td>Specifies that the antenna is for indoor use.</td>
</tr>
<tr>
<td>outdoor</td>
<td>Specifies that the antenna is for outdoor use.</td>
</tr>
</tbody>
</table>

Default
Indoor

Usage Guidelines
The detachable Altitude 300-2d antenna is compatible with the Summit 300 switches. Use this command to configure the antenna type as indoor or outdoor and to comply with regulatory requirements.

Example
The following example configures all ports on the Altitude 300 for indoor use.

```
configure wireless ports all antenna-location indoor
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports detected-station-timeout

configure wireless ports [<portlist> | all] detected-station-timeout <seconds>

Description
Sets the client current state age time-out value.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the amount of time in seconds when the client current state table times out. Valid values are between 60 to 3600.</td>
</tr>
</tbody>
</table>

Default
600 seconds

Usage Guidelines
Client aging allows you to configure an aging timer for wireless stations. When a specified period of time elapses with no data traffic from the client to the Altitude 300, the client is de-authenticated and removed from all client station tables for that interface. After a client is aged out, it can reassociate and re-authenticate to the Altitude 300. Age-out information can be collected from such events as client station failures, station idle-timeouts, or a client abruptly leaving the wireless network without notifying the associated Altitude 300. The timeout value is configured for each port and affects both interfaces 1 and 2.

Example
The following command configures ports 13-24 to time-out the client current state table at 120 seconds.

```bash
configure wireless ports 13-24 detected-station-timeout 120
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports force-disassociation

configure wireless ports <portlist> force-disassociation [all-clients [every <hour <0-23>> <minute <0-59>> | time <month <1-12>> <day> <year <yyyy>> <hour <0-23>> <minute <0-59>>] | cancel-scheduler | <mac-address>]

Description
Configures the client force-disassociation capability.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all-clients</td>
<td>Specifies all clients associated with the port list.</td>
</tr>
<tr>
<td>every</td>
<td>Specifies a repeating disassociation.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies a single disassociation at a specific time and date. If you do not specify the every or time parameters, the user immediately disassociates.</td>
</tr>
<tr>
<td>cancel-scheduler</td>
<td>Specifies to disable forced disassociation.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies the MAC address of the client network interface card.</td>
</tr>
</tbody>
</table>

Default
No schedule.

Usage Guidelines
Force disassociation permits client user disassociation based on a recurring schedule, a date and time, or a particular MAC address. You can also disassociate a user immediately. You can specify access based on a preferred time periods, such as during off-hours, weekends, and holidays. You can also set up a user policy on a RADIUS server to allow user authentication based on time of day.

Example
The following command configures ports 1:18 to force disassociate all clients every day at noon:

```
configure wireless ports 1:18 force-disassociation all-clients every 12 0
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports health-check

configure wireless ports [<portlist> | all] health-check [on | off]

Description
Configures whether the health check reset function is on or off for the specified port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>on</td>
<td>Indicates that the health check reset function is on. The port should be reset if the health check timer expires.</td>
</tr>
<tr>
<td>off</td>
<td>Indicates that the health check reset function is off. The port is not reset if the health check timer expires.</td>
</tr>
</tbody>
</table>

Default
On

Usage Guidelines
This command determines whether the port is reset if the health check timer expires.

Example
The following command configures port 1:18 on the Summit 300-48 to use the health check facility:

configure wireless ports 1:18 health-check on

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan added-trap

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan added-trap [on | off]

Description
Use this command to have the access point (AP) scan to send an SNMP trap when new stations are added to the results table.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies that the AP scan should send an SNMP trap when new stations are added to the results table.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that the AP scan should not send an SNMP trap when new stations are added to the results table.</td>
</tr>
</tbody>
</table>

Default
Off.

Usage Guidelines
Use this command when an SNMP-based remote management application is used to monitor the network.

Example
The following command configures port 18 on the Summit 300-24 to have the AP scan to send an SNMP trap when new stations are added to the results table:

```
configure wireless ports 18 interface 2 ap-scan added-trap on
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan off-channel

configure wireless ports [portlist | all] interface [1 | 2] ap-scan off-channel <add | del> {current-channel | channel-number | all-channels | every-channel}

**Description**

Adds or removes specific channels for the off-channel access point (AP) scan.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>add</td>
<td>Specifies to add the specific channel.</td>
</tr>
<tr>
<td>del</td>
<td>Specifies to delete the specific channel.</td>
</tr>
<tr>
<td>current-channel</td>
<td>Specifies to perform the scan on the current channel only.</td>
</tr>
<tr>
<td>channel-number</td>
<td>Specifies to perform the scan on the channel indicated.</td>
</tr>
<tr>
<td>all-channels</td>
<td>Specifies to perform the scan on all channels in a given country code.</td>
</tr>
<tr>
<td>every-channel</td>
<td>Specifies to perform the scan on all channels regardless of the country code. No beacons are sent on out-of-country-code channels.</td>
</tr>
</tbody>
</table>

**Default**

All channels.

**Usage Guidelines**

Use this command when the AP scan must be started on a particular interface.

**Example**

The following command causes scans on the current channel for wireless port 1:5 using interface 2:

```
configure wireless ports 1:5 interface 2 add current channel
```

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan off-channel continuous

configure wireless ports [all | <portlist>] interface [1 | 2] ap-scan off-channel continuous [on | off]

Description
Turns continuous off-channel scan on or off.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies to turn the continuous off-channel scan on.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies to turn the continuous off-channel scan off.</td>
</tr>
</tbody>
</table>

Default
Scan on.

Usage Guidelines
Use this command to toggle continuous off-channel on a particular interface either on or off.

Example
The following command turns off the off-channel scan for wireless port 1:5 using interface 2:

```
configure wireless ports 1:5 interface 2 ap-scan off-channel continuous off
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan off-channel max-wait

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan off-channel max-wait <num>

Description
Use this command to set the maximum time an off-channel scan waits at a particular channel.

Syntax Description

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>num</td>
<td>Specifies the wait time in milliseconds. Valid entries are between 10 and 10000 milliseconds.</td>
</tr>
</tbody>
</table>

Default
600 ms.

Usage Guidelines
Use this command to specify the time that the access point (AP) should wait on a particular channel.

Example
The following command sets the wait time at 5 milliseconds:

configure wireless ports 1:5 interface 2 ap-scan off-channel max-wait 5

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan off-channel min-wait

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan off-channel min-wait <num>

Description
Use this command to set the minimum time an off-channel scan waits at a particular channel.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>num</td>
<td>Specifies the minimum wait time in milliseconds. Valid entries are between 10 and 10000 milliseconds.</td>
</tr>
</tbody>
</table>

Default
60 ms.

Usage Guidelines
Use this command to specify the minimum time that the access point (AP) should scan a particular channel.

Example
The following command sets the wait time at 5 milliseconds:

```
configure wireless ports 1:5 interface 2 ap-scan off-channel min-wait 5
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan probe-interval

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan probe-interval <msec>

Description
Use this command to configure the interval between probe request packets for active off-channel scanning.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>msec</td>
<td>Specifies the time between probe request packets in milliseconds. Valid entries are between 50 and 3600000 milliseconds.</td>
</tr>
</tbody>
</table>

Default
100 ms.

Usage Guidelines
Use this command to send probe requests at particular intervals on a selected channel during an access point (AP) scan.

Example
The following example configures the interval between probe request packets to be 10 ms for port 1:9 on interface 2:

configure wireless ports 1:9 interface 2 ap-scan probe-interval 10

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan removed-trap

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan removed-trap [on | off]

Description
Use this command to have the access point (AP) scan to send an SNMP trap when new stations are removed from the results table.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies that the AP scan should send an SNMP trap when new stations are removed from the results table.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that the AP scan should not send an SNMP trap when new stations are removed from the results table.</td>
</tr>
</tbody>
</table>

Default
Off.

Usage Guidelines
Use this command to see a trap when stations are removed from the results table.

Example
The following command configures port 18 on the Summit 300-24 to have the AP scan to send an SNMP trap when new stations are removed from the results table:

configure wireless ports 18 interface 2 ap-scan removed-trap on

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan results size

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan results size <num>

Description
Sets the number of elements that the wireless interface stores.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>num</td>
<td>Specifies the number of elements that the wireless interface stores. Valid numbers are between 1 and 128.</td>
</tr>
</tbody>
</table>

Default
128.

Usage Guidelines
Use this command to specify the size of the results table.

Example
The following command configures port 1:7 and interface 1 to store 100 elements:

configure wireless ports 1:7 interface 1 ap-scan results size 100

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan results timeout

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan results timeout <time>

Description
This command sets the timeout threshold that sets when entries are aged out from the table.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the time in seconds before an entry is aged out of the results table. Valid numbers are between 0 and n (any number).</td>
</tr>
</tbody>
</table>

Default
300 seconds.

Usage Guidelines
Use this command to specify the age-out time for the clients in the results table.

Example
The following command configures port 1:7 and interface 1 to have a timeout threshold of 5 seconds:

configure wireless ports 1:7 interface 1 ap-scan results timeout 5

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan send-probe

 configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan send-probe <on | off>

Description
Use this command to enable the sending of probes for active scanning.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies to send probes (active scanning).</td>
</tr>
<tr>
<td>off</td>
<td>Specifies not to send probes (passive scanning).</td>
</tr>
</tbody>
</table>

Default
Off.

Usage Guidelines
Use this command to enable the sending of probes. Setting send-probe to on specifies active scanning. Setting send-probe to off specifies passive scanning.

Example
The following example enables the port range 1:15-1:24 using interface 1 to enable probes.

```
configure wireless ports 1:15-1:24 interface 1 ap-scan send-probe on
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface ap-scan updated-trap

configure wireless ports [<portlist> | all] interface [1 | 2] ap-scan updated-trap <on | off>

Description
Use this command to configure the access point (AP) scan to send an SNMP trap when information about an AP has changed.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies to send an SNMP trap when an AP has changed.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies not to send an SNMP trap when an AP has changed.</td>
</tr>
</tbody>
</table>

Default
Off.

Usage Guidelines
None.

Example
The following example enables the port 20 on a Summit 300-24 using interface 1 to send an SNMP trap when an AP has changed.

configure wireless ports 20 interface 1 ap-scan updated-trap on

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface channel

configure wireless ports <portlist> interface [1 | 2] channel {0 | <channel>}

Description
Configures a channel for the specified interface. With Dynamic Frequency Selection (DFS), the command returns an error if RADAR interference is detected on the specified channel.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>0</td>
<td>Specifies that channels will be automatically selected. Enter '0' (zero) to specify auto selection.</td>
</tr>
<tr>
<td>channel</td>
<td>Specifies a particular channel. (See Table 23 for valid values.)</td>
</tr>
</tbody>
</table>

Default
Auto for both interfaces

Usage Guidelines
Each wireless port on the Summit 300 contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The configure wireless port interface channel command allows you to configure one of the two individual interfaces (1|2) on a port or ports. You can move an interface from one profile to another without having to shut it down.

Valid channel values are shown in Table 23.

Table 23: Valid wireless interface channel values

<table>
<thead>
<tr>
<th>WLAN Standard</th>
<th>Valid Channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.11a</td>
<td>0 (auto), 36, 40, 44, 48, 52, 56, 60, 64, 149, 153, 157, 161, 165, 169, (34, 38, 42, 46 for Japan)</td>
</tr>
<tr>
<td>802.11b and 802.11g</td>
<td>0 (auto), 1-14 (Must be valid entry for the country code range; e.g., valid range for USA is 1-11.)</td>
</tr>
</tbody>
</table>

Example
The following command configures a channel for interface 2 on port 5 on a Summit 300-24:

configure wireless port 5 interface 2 channel auto

The following example shows command output if RADAR interference is detected on the specified channel

# config wireless ports 15 interface 1 channel 44

Error: Interface 15:1 failed, please see log for details.
The system returns the following error message if you attempt to assign a RADAR channel on the interface.

Error: Channel belongs to DFS channel range in mode A. Valid values are 36, 40, 44, 48 for auto mode

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface client-history size

configure wireless ports [<portlist> | all] interface [1 | 2] client-history size <integer>

Description
Use this command to configure the client history size.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>integer</td>
<td>Specifies the size of the client-history table in terms of the number of entries. Valid values are between 1 and 128 entries.</td>
</tr>
</tbody>
</table>

Default
128.

Usage Guidelines
Use this command to specify the maximum number of entries that the client-history table can store.

Example
The following example sets the client-history table for ports 1:1-1:20 and interface 2 to 100 entries:

```
configure wireless ports 1:1-1:30 interface 2 client-history size 100
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface client-history timeout

configure wireless ports [<portlist> | all] interface [1 | 2] client-history timeout <number>

**Description**
Use this command to configure the client history timeout interval.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the timeout interval of the client-history table in seconds. Valid numbers are between 0 and n (any number).</td>
</tr>
</tbody>
</table>

**Default**
600 seconds.

**Usage Guidelines**
Use this command to specify the timeout interval for the clients in the client history table.

**Example**
The following example sets the timeout interval for the client-history table for ports 1:1-1:20 and interface 2 to 100 seconds.

```plaintext
configure wireless ports 1:1-1:20 interface 2 client-history timeout 100
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface client-scan added-trap

configure wireless ports [<portlist> | all] interface [1 | 2] client-scan added-trap [on | off]

Description
Enables or disables traps from the client-scan feature when a new client is detected.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Enables traps when a new client is detected.</td>
</tr>
<tr>
<td>off</td>
<td>Disables traps when a new client is detected.</td>
</tr>
</tbody>
</table>

Default
Off.

Usage Guidelines
Enabling traps can saturate management stations if an area is heavily populated.

Example
The following command enables traps for port 1:5 and interface 2:

```bash
configure wireless port 1:5 interface 2 client-scan added-trap on
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface client-scan removed-trap

configure wireless ports [<portlist> | all] interface [1 | 2] client-scan removed-trap [on |off]

Description
Enables or disables traps from the client-scan feature when a new client has aged-out of the table.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Enables traps when a client has aged out of the table.</td>
</tr>
<tr>
<td>off</td>
<td>Disables traps when a client has aged out of the table.</td>
</tr>
</tbody>
</table>

Default
Off.

Usage Guidelines
Enabling traps can saturate management stations if an area is heavily populated.

Example
The following command disables traps for port 1:9 and interface 1:

```
configure wireless port 1:9 interface 1 client-scan removed-trap off
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface client-scan results size

configure wireless ports [<portlist> | all] interface [1 | 2] client-scan
results size <value>

Description
Configures the maximum number of entries in the client scan information table.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. May be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the maximum number of entries in the client scan information table. The default value is 128. (Range is unlimited.)</td>
</tr>
</tbody>
</table>

Default
128.

Usage Guidelines
Use this command to specify the maximum number of entries that the client-history table can store.

Example
The following command configures the maximum number of entries in the client scan table as 1000 for port 1:5 and interface 2:

```
configure wireless port 1:5 interface 2 client-scan results size 1000
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface client-scan results timeout

configure wireless ports <portlist> interface [1 | 2] client-scan results timeout <number>

Description
Configures the timeout period for entries in the client scan information table.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| Interface | Specifies an interface: 1 or 2. |
| Number | Specifies the timeout in seconds for the client scan information table. Valid numbers are between 0 and n (any number). |

Default
600 seconds.

Usage Guidelines
Use this command to specify the age-out time for the clients in the client-scan results table.

Example
The following command sets the timeout period to 150 seconds for entries in the client scan information table:

configure wireless ports 1:5-1:20 interface 2 client-scan results timeout 150

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface max-clients

configure wireless ports [<portlist> | all] interface [1 | 2] max-clients <value>

Description
Sets the maximum number of clients that can connect simultaneously to a wireless interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. May be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies the maximum number of clients that are allowed to connect simultaneously. Valid values are from 0 to 128. The default value is 100.</td>
</tr>
</tbody>
</table>

Default
100.

Usage Guidelines
Use this command to limit the number of clients that can connect on any interface: 1 or 2.

Example
The following example sets the maximum client level to 72 for port 15 and interface 1:

```
configure wireless ports 15 interface 1 max-clients 72
```

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface rf-profile

configure wireless ports <portlist> interface [1 | 2] rf-profile <name>

Description
Attaches a port or ports and interface to an RF profile.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>name</td>
<td>Specifies the name of the profile.</td>
</tr>
</tbody>
</table>

Default
A for interface 1.
B_G for interface 2.

Usage Guidelines
Each wireless port on the Summit 300 contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The configure wireless port interface command allows you to configure one of the two individual interfaces (1|2) on a port or ports.

All ports in the port list must have the same wireless port version.

Example
The following command attaches the RF profile radio1 to interface 1 on port 1:7 on a Summit 300-48:

configure wireless port 1:7 interface 1 security-profile radio1

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface security-profile

configure wireless ports <portlist> interface [1 | 2] security-profile <name>

**Description**
Attaches a port or ports and interface to a security profile.

**Syntax Description**

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>name</td>
<td>Specifies the name of the profile.</td>
</tr>
</tbody>
</table>

**Default**
Unsecure.

**Usage Guidelines**
Each wireless port on the Summit 300 contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The configure wireless port interface command allows you to configure one of the two individual interfaces (1|2) on a port or ports.

All ports in the port list must have the same wireless port version.

**Example**
The following command attaches the security profile secure-wep to interface 1 on port 1:7 on a Summit 300-48:

```
configure wireless port 1:7 interface 1 security-profile secure-wep
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface transmit-power

configure wireless ports <portlist> interface [1 | 2] transmit-power <level>

Description
Configures the power-level for the specified interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>
| level     | Specifies the power level for the interface. Valid values are:  
- Full  
- Half  
- Quarter  
- One-eighth  
- Min (minimum) |

Default
Full

Usage Guidelines
Each wireless port on the Summit 300 contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The `configure wireless port interface transmit-power` command allows you to configure one of the two individual interfaces (1 | 2) on a port or ports. If there is radio interference from other devices, then you can adjust the power level to an appropriate level below full power.

Example
The following command configures the power level to half-power for interface 1 on ports 5 to 16 on a Summit 300-24:

configure wireless port 5-16 interface 1 transmit-power half

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e. In 7.4, the command syntax was changed from `configure wireless ports interface power-level` to `configure wireless ports interface transmit-power`.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine switches.
configure wireless ports interface transmit-rate

configure wireless ports <portlist> interface [1 | 2] transmit-rate <rate>

Description
Configures a transmission rate for the specified port.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| interface | Specifies an interface: 1 or 2. |
| rate | Specifies the transmission rate for the port. Entering auto specifies automatic transmission rate selection. Valid values are shown in Table 24. |

Default
54 Mbps

Usage Guidelines
Each wireless port on the Summit 300 contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The configure wireless port interface transmit-level command allows you to configure the transmission rate for one of the two individual interfaces (1|2) on a port or ports.

Valid transmission rate values are shown in Table 24.

Table 24: Valid transmission rate values

<table>
<thead>
<tr>
<th>Mode</th>
<th>Valid Transmission Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>6, 9, 12, 18, 24, 36, 48, 54, auto</td>
</tr>
<tr>
<td>B</td>
<td>1, 2, 5.5, 11, auto</td>
</tr>
<tr>
<td>G</td>
<td>1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54, auto</td>
</tr>
</tbody>
</table>

Example
The following command configures the port 14 on a Summit 300-24 to transmit at 54 Mbps for both interface 1 and 2 (A and G):

configure wireless port 14 interface 1 transmit-rate 54Mbps
configure wireless port 14 interface 2 transmit-rate 54Mbps

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports interface wireless-bridging

configure wireless ports <portlist> interface [1 | 2] wireless-bridging [on | off]

Description
Enables or disables the interface as a bridge for wireless clients.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports, an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies that the indicated interface is enabled. When enabled, wireless clients on the same interface are able to communicate.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that the indicated interface is disabled. When disabled, wireless clients on the same interface cannot communicate.</td>
</tr>
</tbody>
</table>

Default
On (enabled)

Usage Guidelines
Wireless bridging on an Summit 300 switches allow wireless users within the same VLAN to communicate with other wireless users on the same switch using layer 2 bridging. Wireless bridging can be enabled or disabled for each interface of the wireless port, and the setting is locally significant on each Altitude 300 wireless port. This setting does not prevent bridging between wired and wireless MAC addresses in the same VLAN or between remote wireless stations associated with a remote Altitude 300 wireless port.

Example
The following command disables bridging interface 2 on port 1:15 on a Summit 300-48:

```
configure wireless port 1:15 interface 2 wireless-bridging off
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports ipaddress

configure wireless ports <portlist> ipaddress <address>

Description
Configures the source IP address for the specified port or ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| address  | Indicates the source IP address. The IP address must be an IP address on the management VLAN. |

Default
The default address is 0.0.0.0.

Usage Guidelines
The source IP address can be public or private IP addresses in class A through class C.

Example
The following command configures the default IP address for port 1:18 on the Summit 300-48:

configure wireless ports 1:18 192.168.0.100.18

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
configure wireless ports location

configure wireless ports <portlist> location <location name>

Description
Configures the physical location of the access point (AP) for the specified port or ports.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| location name | Identifies the location to be configured. |

Default
Unknown Location

Usage Guidelines
Use this command to indicate the physical location of the access point (AP) for the specified port or ports. For example, you could designate a physical location as follows: bldg 1, pole 14, cube 7. Funk Radius can use this attribute for authentication.

Example
The following command configures the location, cube_a7, on port 18:

configure wireless ports 18 location cube_a7

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
create antenna-profile

create antenna-profile <antenna_profile_name>

Description
Creates a new antenna profile with the given name.

Syntax Description

| antenna_profile_name | Identifies the antenna profile. |

Default
N/A.

Usage Guidelines
Antenna profiles can be assigned any name except the default <antenna-profile-name>, detachable_extr_15901.

Example
The following command creates an antenna profile with the name antennal:
create antenna-profile antennal

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
create rf-profile copy

create rf-profile <profile_name> copy <name>

Description
Creates a new RF profile by copying an existing RF profile and assigning a new name.

Syntax Description

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Specifies the name of the new RF profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the names of the RF profile to be copied.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to create a new profile identified by the string name. The copy argument specifies the name of an existing profile from which to obtain the initial values.

Example
The following command creates a new RF profile called rfprof_alpha from an existing profile called wireless_prof:

create rf-profile rfprof_alpha copy wireless_prof

The following command can be used to validate that you created the new RF profile as entered:

show rf-profile rfprof_alpha

or

show rf-profile

The latter command shows all RF profiles.

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
create rf-profile mode

    create rf-profile <profile_name> mode [ A | B | B_G | G ]

**Description**

Creates a new RF profile by defining the interface mode.

**Syntax Description**

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Specifies the name of the new RF profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>Specifies the 802.11a interface mode.</td>
</tr>
<tr>
<td>B</td>
<td>Specifies the 802.11b interface mode.</td>
</tr>
<tr>
<td>B_G</td>
<td>Specifies the 802.11b or 802.11g interface modes.</td>
</tr>
<tr>
<td>G</td>
<td>Specifies the 802.11g interface mode.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

Use this command to create a new profile without copying from an existing profile.

**Example**

The following command creates a new RF profile called *rfprof_alpha* using interface mode G:

```
create rf-profile rfprof_alpha mode g
```

The following command can be used to validate that you created the new RF profile as entered:

```
show rf-profile rfprof_alpha
```

or

```
show rf-profile
```

The latter command shows all RF profiles.

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
delete antenna-profile

delete antenna-profile [<antenna profile name> | detachable_ext_15901]

Description
Deletes the new antenna profile with the given name or the dutiful profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>antenna_profile_name</td>
<td>Identifies the antenna profile.</td>
</tr>
<tr>
<td>detachable_ext_15901</td>
<td>Identifies the default antenna profile.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Antenna profiles can be assigned any name except the default name, detachable_ext_15901.

Example
The following command deletes the antenna profile with the name antenna1:

delete antenna-profile antenna1

History
This command is introduced in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
**delete rf-profile**

    delete rf-profile <name>

**Description**
Deletes the named RF profile.

**Syntax Description**

| name | Specifies the name of an existing RF profile to be deleted. |

**Default**
N/A

**Usage Guidelines**
Use this command to delete the named RF profile. The named profile cannot be attached to any active ports before deletion.

**Example**
The following example deletes the RF profile named *rfprof_alpha*:

`delete rf-profile rfprof_alpha`

The following command can be used to validate that you deleted the RF profile as entered:

`show rf-profile rfprof_alpha`

or

`show rf-profile`

The latter command shows all RF profiles.

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports

disable wireless ports <portlist>

Description
Administratively disables a wireless port for use.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |

Default
N/A

Usage Guidelines
Use this command to disable one or more wireless ports.

Example
The following command disables port 1:17:

disable wireless ports 1:17

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports cancel-scheduler

disable wireless ports <portlist> cancel-scheduler

**Description**

Cancels previously scheduled enable or disable scheduling commands for the port.

**Syntax Description**

| portlist | Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |

**Default**

N/A

**Usage Guidelines**

Use this command with the force disassociation scheduler to cancel a force disassociation schedule.

**Example**

The following command cancels all scheduled enable or disable commands:

disable wireless ports all cancel-scheduler

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports every

disable wireless ports <portlist> every <hour>

Description
Disables the specified port or ports every day at the specified hour.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>hour</td>
<td>Specifies the hour in military format (0-23).</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to configure the disabling of wireless ports according to a daily schedule. The selected port or ports will be disabled each day on the specified hour.

Example
The following command disables port 1:17 every day at 7 a.m.:

disable wireless ports every 1:17 7

History
a. It was added to the “i” series in 7.3.0 and to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interface

disable wireless ports <portlist> interface [1 | 2]

Description
Disables the specified port interface.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |

Default
N/A

Usage Guidelines
Use this command to disable one of the interfaces. If both interfaces are disabled, it’s the same as using the command: disable wireless ports x:x.

Example
The following command disables port 1:35 and interface 1:

disable wireless ports 1:35 interface 1

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interface ap-scan

   disable wireless ports <portlist> interface [1 | 2] ap-scan

Description
Stops an on-channel wireless port scan for the indicated port or ports and interface for the Altitude 300.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
When the scan feature is disabled, entries slowly age out of the scan results table until it is empty. If the scan is restarted, the table values from the previous scan will be kept.

Example
The following command disables interface 2 on ports 1:18 to 1:28 on a Summit 300-48:

disable wireless ports 1:18-1:28 interface 2 ap-scan

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interface ap-scan off-channel

disable wireless ports <portlist> interface [1 | 2] ap-scan off-channel [at | every] <time>

Description
Stops the access point (AP) scan on the indicated interface at the specified time.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>at</td>
<td>Specifies a once-only start time for a scan.</td>
</tr>
<tr>
<td>every</td>
<td>Specifies to start the scan every day at the specified time.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the hour in the format (0-23)</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to stop the off-channel AP scan.

Example
The following command disables port 23 using interface 1 on the Summit 300-24:

disable wireless ports 23 interface 1 ap-scan off-channel at 18

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interface client-history

disable wireless ports [portlist | all] interface [1 | 2] client-history

Description
Disables logging of client historical information.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. May be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
Disable.

Usage Guidelines
Use this command to disable logging of client-history information on the specified wireless interface.

Example
The following example sets port 1:23 and interface 1 to disable logging of historical information:

disable wireless ports 1:23 interface 1 client-history

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interface client-scan

    disable wireless ports <portlist> interface [1 | 2] client-scan

Description
Disables the client scan feature on the specified wireless interface.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to disable the client scan feature on the specified wireless interface. Disabling the feature can improve performance if the network is heavily populated and beginning to show degradation.

Example
The following command disables port 1:31 and interface 2:

disable wireless ports 1:31 interface 2 client-scan

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interface iapp

disable wireless ports [<portlist> | all] interface [1 | 2] iapp

Description
Disables Inter-Access Point Protocol (IAPP) on a per interface basis.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
Enabled.

Usage Guidelines
Use this command to disable IAPP for the selected ports and interface.

Example
The following example disables port 1:15 and interface 1 for IAPP:

disable wireless ports 1:15 interface 1 iapp

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports interfacesvp

disable wireless ports [<portlist> | all] interface [1 | 2] svp

Description
Disables the QoS protocol, SpectraLink Voice Protocol (SVP), for VoIP on the specified port and interface.

Syntax Description

| portlist     | Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| all          | Specifies all ports.                                      |
| interface    | Specifies an interface: 1 or 2.                           |

Default
Disabled

Usage Guidelines
Use this command to disable the QoS protocol for VoIP. By enabling QoS for VoIP, you give voice traffic a higher priority than data traffic. VoIP traffic has less tolerance for error recovery than data. Although voice traffic can tolerate some degree of error recovery, it can be noticeable to users. This command allows you to enable QoS for VoIP on the port and interface level.

Example
The following example, disables SVP on port 17 and interface 1:

disable wireless ports 17 interface 1 svp

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
disable wireless ports time

disable wireless ports <portlist> time <date> <hour>

Description
Disables the specified ports at the given date and hour.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Specifies one or more ports or slots and ports. can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Specifies the date in the format (m/d/yyyy).</td>
</tr>
<tr>
<td>Hour</td>
<td>Specifies the hour in the format (0-23)</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to disable one or more wireless ports at a specified time.

Example
The following command disables port 1:18 on June 29, 2005 at 3 p.m.:

disable wireless ports 1:18 time 6/29/2005 15

History
This command was first available in ExtremeWare 6.2a and added to the "e" series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports

    enable wireless ports <portlist>

Description
Administratively enables a wireless port for use.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |

Default
N/A

Usage Guidelines
Use this command to enable wireless ports.

Example
The following command enables port 1:17:

    enable wireless ports 1:17

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports cancel-scheduler

enable wireless ports <portlist> cancel-scheduler

**Description**
This command cancels the scheduler on all ports or on a particular port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to cancel the scheduler.

**Example**
The following command cancels all scheduled enable or disable commands:

```
enable wireless ports all cancel-scheduler
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports every

    enable wireless ports <portlist> every <hour>

Description
Enables the specified port or ports every day at the specified hour.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| hour    | Specifies the hour in military format (0-23). |

Default
N/A

Usage Guidelines
Use this command to automatically enable wireless ports according to a daily schedule. The selected port or ports will be enabled each day on the specified hour.

Example
The following command enables port 1:17 every day at 7 a.m.:

```
enable wireless ports every 1:17 7
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports interface

enable wireless ports <portlist> interface [1 | 2]

Description
Enables the specified port interface.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command for per interface enabling.

Example
The following command enables port 1:35 and interface 1:

```
enable wireless ports 1:35 interface 1
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports interface ap-scan

   enable wireless ports <portlist> interface [1 |2] ap-scan

**Description**
Starts a wireless port on-channel scan for the indicated port or ports and interface for the Altitude 300.

**Syntax Description**

| portlist | Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5. |
| interface | Specifies an interface: 1 or 2. |

**Default**
N/A.

**Usage Guidelines**
Use this command to start the wireless port on-channel scan on the indicated port and interface for the Altitude 300. The Altitude 300 continues to carry user traffic during scans operating on the current channel (“on-channel” scans).

**Example**
The following command enables interface 2 on ports 1:18 to 1:28:

```
enable wireless ports 1:18-1:28 interface 2 ap-scan
```

**History**

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports interface ap-scan off-channel

enable wireless ports <portlist> interface [1 | 2] ap-scan off-channel [at | every] <time>

**Description**
Starts the access point (AP) scan on the indicated interface at the specified time.

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>at</td>
<td>Specifies a once-only start time for a scan.</td>
</tr>
<tr>
<td>every</td>
<td>Specifies to start the scan every day at the specified time.</td>
</tr>
<tr>
<td>time</td>
<td>Specifies the hour in the format (0-23)</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to schedule the off-channel AP scan. During an “off-channel” scan, the Altitude 300 is not available for user traffic.

**Example**
The following command enables port 23 using interface 1:

```
enable wireless ports 23 interface 1 ap-scan off-channel at 18
```

**History**

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports interface client-history

```
  enable wireless ports [<portlist> | all] interface [1 | 2] client-history
```

**Description**
Sets the Altitude 300 to log client historical information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. May be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**
Disable

**Usage Guidelines**
Use this command to get the detail status about each associated client.

**Example**
The following example sets port 1:23 and interface 1 to keep historical information:
```
enable wireless ports 1:23 interface 1 client-history
```

**History**
This command was first available in ExtremeWare 6.2a and added to the "e" series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports interface client-scan

    enable wireless ports [<portlist> | all] interface [1 | 2] client-scan

**Description**

Enables the client scan feature on the specified wireless interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Use this command to enable the client scan feature on the specified wireless interface.

**Example**

The following command enables port 1:31 and interface 2:

```bash
enable wireless ports 1:31 interface 2 client-scan
```

**History**

This command was first available in ExtremeWare 6.2a and added to the "e" series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports interface iapp

   enable wireless ports [<portlist> | all] interface [1 | 2] iapp

**Description**
Enables Inter-Access Point Protocol (IAPP) on a per interface basis.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**
Enabled.

**Usage Guidelines**
Use this command to enable IAPP for the selected ports and interface.

**Example**
The following example enables port 1:15 and interface 1 for IAPP:

```plaintext
enable wireless ports 1:15 interface 1 iapp
```

**History**

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.

**enable wireless ports interface svp**

```
enable wireless ports [<portlist> | all] interface [1 | 2] svp
```

**Description**

Enables the QoS protocol, SpectraLink Voice Protocol (SVP), for VoIP on the specified port and interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**

Disabled

**Usage Guidelines**

Use this command to implement the QoS protocol for VoIP. By enabling QoS for VoIP, you give voice traffic a higher priority than data traffic. VoIP traffic has less tolerance for error recovery than data. Although voice traffic can tolerate some degree of error recovery, it can be noticeable to users. This command allows you to enable QoS for VoIP on the port and interface level.

**Example**

The following example, turns on SVP on port 17 and interface 1:

```
enable wireless ports 17 interface 1 svp
```

**History**

This command was first available in ExtremeWare 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
enable wireless ports time

    enable wireless ports <portlist> time <date> <hour>

Description
Enables the specified ports at the given date and hour.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Specifies the date in the format (m/d/yyyy).</td>
</tr>
<tr>
<td>Hour</td>
<td>Specifies the hour in the format (0-23)</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to enable selected wireless ports at a particular time.

Example
The following command enables port 1:18 on June 29, 2005 at 3 p.m.:

    enable wireless ports 1:18 time 6/29/2005 15

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
reset wireless ports

reset wireless ports <portlist>

Description
Resets the access point connected to the wireless ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports.</td>
</tr>
<tr>
<td></td>
<td>an be one or more port numbers. May be in the</td>
</tr>
<tr>
<td></td>
<td>form 1, 2, 1:2, 3-5.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to reboot the access point connected to the wireless port.

Example
The following example resets all the wireless ports to the default values:

```bash
reset wireless ports
```

The following example resets all the Remote Connect wireless ports on a Summit 300-48t switch to the default values:

```bash
reset wireless ports v:*
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
reset wireless ports interface

    reset wireless ports <portlist> interface [1 | 2]

Description
Forces the wireless port interface to reset.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to reset the wireless interface of given ports.

Example
The following example resets all of interface 1 ports to the default values:

    reset wireless ports interface 1

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show antenna-profile

    show antenna-profile [<antenna profile name> | detachable_extr_15901]

Description
Displays information about the antenna profile with the given name or the dutiful profile.

Syntax Description

<table>
<thead>
<tr>
<th>antenna_profile_name</th>
<th>Identifies the antenna profile.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detachable_extr_15901</td>
<td>Identifies the default antenna profile.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Antenna profiles can be assigned any name except the default name, detachable_extr_15901.

Example
The following command displays information regarding the antenna profile with the name antenna1:
show antenna-profile antenna1

History
This command is introduced in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
Wireless Commands

show APmgmt port

show APmgmt port <port> [detail | history]

Description
Displays information about the A300 currently running on the specified virtual port.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Identifies the wireless port on the switch.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays details about the A300 running on the wireless port.</td>
</tr>
<tr>
<td>history</td>
<td>Displays the port state machine log for the wireless port.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
N/A

Example
The following examples show output for the command with the detail and history parameters.

```plaintext
show APmgmt port virtual : 2 detail
ap management parameters:       keep alive period=1
    available bootrom:    AB-1_7.BIN      AB-2_4.BIN
    runtime:    AR-7_3.Z

--------------------------------------------------------------------------------
port state           timeout  enable mac                #ann  #tftp xmt  rcv
--------------------------------------------------------------------------------
v:2 RUNNING         20       1      00:04:96:0d:9e:f0  1     1     48   468
--------------------------------------------------------------------------------
 hardware ID      : Altitude 300-2i
 hardware Version : 1.1.1
 hardware serial  : 04078-00211
 hardware status  : 0x00f363e7 (OK=0x00f363e7)
 bootrom version  : 2.4 build 0
 filename sent     : AR-7_3.Z
--- Virtual Port v:2 info------
 Current BINDING  : AP MAC (2)
 Cached MAC       : 00:04:96:0d:9e:f0

--------------------------------------------------------------------------------
show APmgmt port virtual : 2 history
================================================================================
port state machine log for v:2
================================================================================
16/11/2004 15:29:27 hello: ip=10.211.37.88: 1026 mac=00:04:96:0d:9e:f0 hw id=Altitude 300-2i hw\ver=1.1.1 seria
```
show APmgmt port

1=04078-00211 status=0xf363e7(OK=0xf363e7)) bootrom ver=2.4.0
    id=Altitude 300-2i hw (ver=1.1.1 s
serial=04078-00211 status=0xf363e7(OK=0xf363e7)) bootrom ver=2.4.0
16/11/2004 15:29:29 STATE_ANNOUNCE_REPLY_SENT: TFTP Req received from 10.211.37.88 for
    file name. TFTP Reg Count 0 (limit 30)
16/11/2004 15:29:29 ANNOUNCE_REPLY_SENT: received TFTP_REQ
16/11/2004 15:29:29 TFTP_REQ_RCVD: nTFTPReq=1(limit=30)
16/11/2004 15:29:33 SERVICING_TFTP: received TFTPD_EXIT_OK
16/11/2004 15:29:48 AGENTX_OPENED:
16/11/2004 15:29:57 AGENTX_OPENED: received AGENTX_CONFIG_OK
16/11/2004 15:29:58 RUNNING:

Show APmgmt port 1:6 history
================================
port state machine log for 1:6
================================
    id=Altitude 300-2i hw (ver=1.1.1 s
serial=04078-00211 status=0xf363e7(OK=0xf363e7)) bootrom ver=2.4.0
16/11/2004 13:57:11 ANNOUNCE_REPLY_SENT: received EDP_ANNOUNCE
    id=Altitude 300-2i hw (ver=1.1.1 s
serial=04078-00211 status=0xf363e7(OK=0xf363e7)) bootrom ver=2.4.0
16/11/2004 13:57:12 STATE_ANNOUNCE_REPLY_SENT: TFTP Req received from 10.211.37.83 for
    file name. TFTP Reg Count 0 (limit 30)

**History**

This command was first available in an ExtremeWare 7.4.

**Platform Availability**

This command is available on Summit 300-48, Summit 300-24, Summit 400-24p, and Alpine 3800
switches.
show rf-profile

    show rf-profile (<profile_name>)

Description
Displays configuration attributes for a particular RF profile or all RF profiles.

Syntax Description

| profile_name | Specifies the name of the RF profile whose configuration is to be displayed. If you do not enter an RF profile name, configuration attributes will be displayed for all RF profiles. |

Default
All

Usage Guidelines
Use this command to display configuration attributes for a particular RF profile or all RF profiles. If you do not enter an RF profile name, configuration attributes are displayed for all RF profiles.

Example
The following command displays configuration information about the RF profile named rfprof_alpha:
show rf-profile rfprof_alpha

The output from this command is similar to:

    Profile Name: rfprof_alpha
    Mode: G
    Beacon Interval: 1000
    DTIM: 100
    Fragmentation Length: 2345
    RTS Threshold: 2330
    Preamble: Long
    Short Retry: 4
    Long Retry: 7
    No interfaces bound to this RF profile

The following command displays configuration information about all RF profiles:
show rf-profile

The output from this command is similar to:

    Profile Name: DEFAULT_A
    Mode: A
    Beacon Interval: 40
    DTIM: 2
    Fragmentation Length: 2345
    RTS Threshold: 2330
    Preamble: Short
    Short Retry: 4
show rf-profile

Long Retry: 7
Interfaces: 64

Profile Name: DEFAULT_BG
Mode: B_G
Beacon Interval: 40
DTIM: 2
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 4
Long Retry: 7
Interfaces: 63

Profile Name: DEFAULT_B
Mode: B
Beacon Interval: 100
DTIM: 2
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 4
Long Retry: 7
Interfaces: 1
2:1:2

Profile Name: DEFAULT_G
Wireless Commands

Mode: G
Beacon Interval: 40
DTIM: 2
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Short
Short Retry: 4
Long Retry: 7

No interfaces bound to this RF profile

Profile Name: MinSetting_A
Mode: A
Beacon Interval: 20
DTIM: 1
Fragmentation Length: 1020
RTS Threshold: 1024
Preamble: Short
Short Retry: 1
Long Retry: 1

No interfaces bound to this RF profile

Profile Name: MinSetting_B
Mode: B
Beacon Interval: 20
DTIM: 1
Fragmentation Length: 256
RTS Threshold: 0
Preamble: Long
Short Retry: 1
Long Retry: 1

No interfaces bound to this RF profile

Profile Name: MinSetting_G
Mode: G
Beacon Interval: 20
DTIM: 1
Fragmentation Length: 256
RTS Threshold: 0
Preamble: Long
Short Retry: 1
Long Retry: 1

No interfaces bound to this RF profile

Profile Name: MaxSetting_A
Mode: A
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Short
Short Retry: 255
Long Retry: 255
show rf-profile

No interfaces bound to this RF profile

Profile Name: MaxSetting_B
Mode: B
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 255
Long Retry: 255
No interfaces bound to this RF profile

Profile Name: MaxSetting_G
Mode: G
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 255
Long Retry: 255
No interfaces bound to this RF profile

Profile Name: MaxSetting_BG
Mode: B_G
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 255
Long Retry: 255
No interfaces bound to this RF profile

Profile Name: MaxBeacon_BG
Mode: B_G
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 4
Long Retry: 7
No interfaces bound to this RF profile

Profile Name: MaxBeacon_B
Mode: B
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
Wireless Commands

RTS Threshold: 2330
Preamble: Long
Short Retry: 4
Long Retry: 7
No interfaces bound to this RF profile

Profile Name: MaxBeacon_G
Mode: G
Beacon Interval: 1000
DTIM: 100
Fragmentation Length: 2345
RTS Threshold: 2330
Preamble: Long
Short Retry: 4
Long Retry: 7
No interfaces bound to this RF profile

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ap-scan results

show wireless ap-scan results (detail)

Description
Displays a switch-wide, correlated view of the results of the access point (AP) scan.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>This optional keyword, provides more in-depth information.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to see the results of an AP scan. Use the optional keyword, detail, to see all of the fields in Table 25.

Table 25: AP Scan Results (Alphabetized)

<table>
<thead>
<tr>
<th>Data Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APMAC</td>
<td>MAC address of the discovered AP</td>
</tr>
<tr>
<td>Capability</td>
<td>Capability field from a received information packet (in detail output only)</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel on which this AP was discovered</td>
</tr>
<tr>
<td>ESS Name</td>
<td>String ESS ID I.E.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Time value at which this entry was updated</td>
</tr>
<tr>
<td>Min/Max/Avg RSS</td>
<td>Received Signal Strength statistics</td>
</tr>
<tr>
<td>Network Type</td>
<td>Ad-hoc or BSSID network (in detail output only)</td>
</tr>
<tr>
<td>Number of beacons</td>
<td>Count of beacon packets seen from this AP (in detail output only)</td>
</tr>
<tr>
<td>Number of probe resp</td>
<td>Count of PROBE RESP packets sent from the AP (in detail output only)</td>
</tr>
<tr>
<td>Supported Rate Set</td>
<td>List of supported rates</td>
</tr>
<tr>
<td>WEP required/WEP</td>
<td>WEP information from beacon and probe packets</td>
</tr>
<tr>
<td>authentication supported</td>
<td>WPA information, including authentication and supported encryption algorithms</td>
</tr>
</tbody>
</table>

Example
The following command displays information about the AP scan.

show wireless ap-scan results

The output from the command is similar to:

```
AP Mac Address   Intf   ESS Name   AvgRSS Type Chan WEP WPA Last
```
The output from the command is similar to:

<table>
<thead>
<tr>
<th>AP Mac Address</th>
<th>Intf</th>
<th>ESS Name</th>
<th>AvgRSS</th>
<th>Type</th>
<th>Chan</th>
<th>WEP</th>
<th>WPA</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:96:05:80:00</td>
<td>5:2</td>
<td>Extreme_g</td>
<td>2</td>
<td>bss</td>
<td>12</td>
<td>Y</td>
<td>Y</td>
<td>01:36:17</td>
</tr>
<tr>
<td>00:04:96:05:80:08</td>
<td>5:2</td>
<td>fz-dot1x-128</td>
<td>0</td>
<td>bss</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>01:36:15</td>
</tr>
<tr>
<td>00:04:96:05:81:50</td>
<td>5:2</td>
<td>Extreme_g</td>
<td>8</td>
<td>bss</td>
<td>2</td>
<td>Y</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:05:82:00</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>0</td>
<td>bss</td>
<td>11</td>
<td>N</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:05:82:80</td>
<td>5:2</td>
<td>Extreme_g</td>
<td>0</td>
<td>bss</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>01:36:15</td>
</tr>
<tr>
<td>00:04:96:0C:00:05</td>
<td>5:2</td>
<td>wpadyn-g-tkip-ess</td>
<td>0</td>
<td>bss</td>
<td>11</td>
<td>Y</td>
<td>Y</td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:04:30</td>
<td>5:2</td>
<td>fz-shared-wep-64</td>
<td>0</td>
<td>bss</td>
<td>7</td>
<td>Y</td>
<td></td>
<td>01:36:11</td>
</tr>
<tr>
<td>00:04:96:0C:05:50</td>
<td>5:2</td>
<td>Extreme_gx</td>
<td>0</td>
<td>bss</td>
<td>1</td>
<td>Y</td>
<td>Y</td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:07:00</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>3</td>
<td>bss</td>
<td>3</td>
<td>N</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:07:60</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>3</td>
<td>bss</td>
<td>11</td>
<td>N</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:07:80</td>
<td>5:2</td>
<td>TFZ</td>
<td>0</td>
<td>bss</td>
<td>7</td>
<td>Y</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:07:80</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>0</td>
<td>bss</td>
<td>4</td>
<td>N</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:3C:30</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>0</td>
<td>bss</td>
<td>10</td>
<td>N</td>
<td></td>
<td>01:36:16</td>
</tr>
<tr>
<td>00:04:96:0C:3C:30</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>1</td>
<td>bss</td>
<td>10</td>
<td>N</td>
<td></td>
<td>01:35:58</td>
</tr>
<tr>
<td>00:04:96:0C:3C:70</td>
<td>5:2</td>
<td>fz-open-wep-64</td>
<td>4</td>
<td>bss</td>
<td>7</td>
<td>Y</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:5F:00</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>2</td>
<td>bss</td>
<td>11</td>
<td>N</td>
<td></td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:5F:00</td>
<td>5:2</td>
<td>Extreme_gx</td>
<td>5</td>
<td>bss</td>
<td>11</td>
<td>Y</td>
<td>Y</td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:DB:40</td>
<td>5:2</td>
<td>fz-wpa-dyn-aes</td>
<td>3</td>
<td>bss</td>
<td>11</td>
<td>Y</td>
<td>Y</td>
<td>01:36:18</td>
</tr>
<tr>
<td>00:04:96:0C:DB:40</td>
<td>5:2</td>
<td>Atheros</td>
<td>0</td>
<td>bss</td>
<td>12</td>
<td>Y</td>
<td>Y</td>
<td>01:36:17</td>
</tr>
<tr>
<td>00:04:96:0D:9C:70</td>
<td>5:2</td>
<td>DEFAULT_ESS</td>
<td>0</td>
<td>bss</td>
<td>14</td>
<td>N</td>
<td></td>
<td>01:35:50</td>
</tr>
</tbody>
</table>

History

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ap-scan results mac_address

    show wireless ap-scan results <mac_address>

Description
Displays information about the access point (AP) MAC-address that is entered.

Syntax Description

mac-address  Specifies the MAC address of the client network interface card.

Default
N/A

Usage Guidelines
Use this command to review details about the specified AP.

Example
The following command displays information about the AP 00:04:96:0C:23:70:

    show wireless ap-scan results 00:04:96:00:23:70

The results of the command are similar to:

<table>
<thead>
<tr>
<th>AP Mac Address</th>
<th>Intf</th>
<th>ESS Name</th>
<th>AvgRSS</th>
<th>Type</th>
<th>Chan</th>
<th>WEP</th>
<th>WPA</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:96:00:23:70</td>
<td>1:23:2</td>
<td>DEFAULT_ESS</td>
<td>27</td>
<td>bss 6</td>
<td>N02:18:51</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless client-scan results

    show wireless client-scan results {{detail }| {<mac-address} {detail}}

Description
Displays information about client scan results, optionally by MAC address from the client scan results table.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Provides more in-depth information.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies the MAC address of the client network interface card.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to get information about client scan results. Use the detail option to get further details of the client scan.

Examples
The following example displays information about the wireless configuration:

show wireless client-scan results

The output of the command is similar to:

```
Source :  00:04:23:90:03:91

<table>
<thead>
<tr>
<th>Intf</th>
<th>Probe</th>
<th>ProbeResp</th>
<th>FirstSeen</th>
<th>LastChange</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>LastRSS</th>
<th>LastRate</th>
<th>LastChan</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>

Source :  00:05:4E:48:45:F8

<table>
<thead>
<tr>
<th>Intf</th>
<th>Probe</th>
<th>ProbeResp</th>
<th>FirstSeen</th>
<th>LastChange</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:25:2</td>
<td>985</td>
<td>0</td>
<td>23:06:41</td>
<td>23:41:36</td>
</tr>
<tr>
<td>1:25:1</td>
<td>958</td>
<td>0</td>
<td>23:06:50</td>
<td>23:41:38</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LastRSS</th>
<th>LastRate</th>
<th>LastChan</th>
</tr>
</thead>
<tbody>
<tr>
<td>21</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>19</td>
<td>0</td>
<td>40</td>
</tr>
</tbody>
</table>
```
The following example shows the client scan results table:

<table>
<thead>
<tr>
<th>Source</th>
<th>Intf</th>
<th>Probes</th>
<th>ProbeResp</th>
<th>LastRSS</th>
<th>LastChan</th>
</tr>
</thead>
<tbody>
<tr>
<td>00:04:23:90:03:91</td>
<td>1:25:2</td>
<td>100445</td>
<td>0</td>
<td>15</td>
<td>6</td>
</tr>
</tbody>
</table>

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless configuration

show wireless configuration

Description
Displays the country, management VLAN, and gateway.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this command to check the basic wireless configuration on a switch.

Examples
The following example displays information about the wireless configuration:

show wireless configuration

The output of the command is similar to:

Summit300-48:4 # show wireless configuration
    Country Code: Extreme Default
  Management VLAN: Default
    Gateway:        192.168.0.1

Timed Command Information:
Summit300-48:5 #

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports

    show wireless ports [all | <portlist>]{detail}

Description
This command shows a summary or detailed report of all wireless ports.

Syntax Description

<table>
<thead>
<tr>
<th>all</th>
<th>Specifies all active ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>detail</td>
<td>This optional keyword, provides more in-depth information.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to show a summary of all ports or for a particular port.

Examples
The following example displays summary information about the wireless ports:

    show wireless ports all

The output is similar to:

<table>
<thead>
<tr>
<th>Port</th>
<th>HW Version</th>
<th>MAC Addr</th>
<th>Serial #</th>
<th>State</th>
<th>Last Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:8</td>
<td>01010001</td>
<td>00:04:96:0C:22:00</td>
<td>03418-00410</td>
<td>ON</td>
<td>Mon Sep 13 11:03:16 2004</td>
</tr>
<tr>
<td>1:9</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:10</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:11</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:12</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:13</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:14</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:15</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:16</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:17</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:18</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:19</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Press <SPACE> to continue or <Q> to quit:
History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports configuration

show wireless ports [all | <portlist>] configuration

Description
Displays a summary of the wireless configuration.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to review the configuration of one or more wireless ports.

Example
The following example displays a summary report of all the configured wireless ports:

show wireless ports all configuration

The output of the command is similar to:

<table>
<thead>
<tr>
<th>Port</th>
<th>IP Address</th>
<th>Location Descr</th>
<th>Ant-Loc</th>
<th>TOut</th>
<th>HealthChk</th>
<th>State</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>EN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:2</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:3</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:4</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:5</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:6</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:7</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:8</td>
<td>10.211.37.83</td>
<td>Unknown Location indoor 600 on</td>
<td>EN</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:9</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:10</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:11</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:12</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:13</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:14</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:15</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:16</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:17</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:18</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>1:19</td>
<td>0.0.0.0</td>
<td>Unknown Location indoor 600 on</td>
<td>DIS</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Press <SPACE> to continue or <Q> to quit:
History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports debug-trace

show wireless ports [all | <portlist>] debug-trace {detail}

Description
Displays whether debug-trace is enabled on one or more ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays all the available information.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to review the debug-trace status on a port.

Example
The following example displays a summary report of the status of debug-trace on all wireless ports:

```
show wireless ports all debug-trace
```

The output of the command is similar to:

```
Wireless Port         : 1:8
Messages Sent         : 0
Total Bytes Sent      : 0
Messages Suppressed   : 278409
Other Errors          : 0

Trace            Description                      CUR  MSGS  BYTES SUPP
-------------------------------------------------------------------------------
dot1x            802.1x Processing                0    0     0     69058
radius           Radius Backend                   0    0     0     0
mac              Wireless MAC                     0    0     0     34
snmp             SNMP Subagent                    0    0     0     1980
wlan-driver      WLAN Driver                      0    0     0     0
eth-driver       ETH Driver                       0    0     0     0
ap-scan          AP Scan                          0    0     0     46
client-diag      Client Diag                      0    0     0     6
mac-radius       MAC Radius                       0    0     0     0
wpa              WPA State Machine                0    0     0     207152
iapp             IAPP                             0    0     0     133
Wireless Port         : 1:25
Messages Sent         : 0
Total Bytes Sent      : 0
```
**Wireless Commands**

<table>
<thead>
<tr>
<th>Trace</th>
<th>Description</th>
<th>CUR</th>
<th>MSGS</th>
<th>BYTES</th>
<th>SUPP</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1x</td>
<td>802.1x Processing</td>
<td>0</td>
<td>0</td>
<td>69094</td>
<td></td>
</tr>
<tr>
<td>radius</td>
<td>Radius Backend</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>mac</td>
<td>Wireless MAC</td>
<td>0</td>
<td>0</td>
<td>334</td>
<td></td>
</tr>
<tr>
<td>snmp</td>
<td>SNMP Subagent</td>
<td>0</td>
<td>0</td>
<td>45947</td>
<td></td>
</tr>
<tr>
<td>wlan-driver</td>
<td>WLAN Driver</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>eth-driver</td>
<td>ETH Driver</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>ap-scan</td>
<td>AP Scan</td>
<td>0</td>
<td>0</td>
<td>35736423</td>
<td></td>
</tr>
<tr>
<td>client-diag</td>
<td>Client Diag</td>
<td>0</td>
<td>0</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>mac-radius</td>
<td>MAC Radius</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>wpa-wpa2</td>
<td>WPA or WPA2 State Machine</td>
<td>0</td>
<td>0</td>
<td>207188</td>
<td></td>
</tr>
<tr>
<td>iapp</td>
<td>IAPP</td>
<td>0</td>
<td>0</td>
<td>187</td>
<td></td>
</tr>
</tbody>
</table>

---

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface ap-scan configuration

show wireless ports [<portlist> | all] interface [1 |2] ap-scan configuration {detail}

Description
Displays the current configuration of the scan feature for the selected ports and interface.

Syntax Description

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to see the current configuration of the AP scan feature for the specified wireless port and interface. Use the optional keyword, detail, to see the detailed or expanded configuration.

Examples
The following example displays the configuration of port 1:5 and interface 1:

```
show wireless ports 1:5 interface 1 ap-scan configuration
```

The output of the command is similar to:

```
Intf   En  Add Rem Update Probe ProbeInt OCS Cont. Size Timeout Channels
-------------------------------------------------------------------------------
1:5:1  N   off off off    off   100      N   N     128  300
```

The following example shows the extra details shown when the keyword detail is added to the command:

```
show wireless ports 1:5 interface 1 ap-scan configuration detail
```

The output of the command is similar to:

```
Interface                : 1:5:1
Enabled                  : N
Send Added Trap          : off
Send Removed Trap        : off
Send Updated Trap        : off
Probe Interval           : 100 (msec)
Send Probe               : N
Result Table Size        : 128
```
Wireless Commands

Off Channel Scan (OCS) : N
  OCS Continuous Scan : N
  OCS Channels : 
  OCS Min-wait : 60 (msec)
  OCS Max-wait : 600 (msec)
  Scheduled OCS :
    Schedule#1 : Currently disabled
    Schedule#2 : Currently disabled
    Schedule#3 : Currently disabled
    Schedule#4 : Currently disabled
    Schedule#5 : Currently disabled
    Schedule#6 : Currently disabled
    Schedule#7 : Currently disabled
    Schedule#8 : Currently disabled

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches. **show wireless ports interface ap-scan results**

```plaintext
show wireless ports [<portlist> | all] interface [1 | 2] ap-scan results
{detail}
```

**Description**
Displays information about the results of an access point (AP) scan from the port perspective.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>Interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to see the results of an AP scan. Use the optional keyword, `detail`, to see all of the fields in Table 25.

**Table 26: AP Scan Results (Alphabetized)**

<table>
<thead>
<tr>
<th>Data Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APMAC</td>
<td>MAC address of the discovered AP</td>
</tr>
<tr>
<td>Capability</td>
<td>Capability field from a received information packet (in detail output only)</td>
</tr>
<tr>
<td>Channel</td>
<td>The channel on which this AP was discovered</td>
</tr>
<tr>
<td>ESSID Name</td>
<td>String ESS ID I.E.</td>
</tr>
<tr>
<td>Last Update</td>
<td>Time value at which this entry was updated</td>
</tr>
<tr>
<td>Min/Max/Avg RSS</td>
<td>Received Signal Strength statistics</td>
</tr>
<tr>
<td>Network Type</td>
<td>Ad-hoc or BSSID network (in detail output only)</td>
</tr>
<tr>
<td>Number of beacons</td>
<td>Count of beacon packets seen from this AP (in detail output only)</td>
</tr>
<tr>
<td>Number of probe resp</td>
<td>Count of PROBE RESP packets sent from the AP (in detail output only)</td>
</tr>
<tr>
<td>Supported Rate Set</td>
<td>List of supported rates</td>
</tr>
<tr>
<td>WEP required/WEP authentication supported</td>
<td>WEP information from beacon and probe packets</td>
</tr>
<tr>
<td>WPA</td>
<td>WPA information, including authentication and supported encryption algorithms</td>
</tr>
</tbody>
</table>
Example

The following example shows summary AP scan results for port 1:2 and interlace 1:

```
show wireless ports 1:2 interface 1 ap-scan results
```

The output of the command is similar to:

```
<table>
<thead>
<tr>
<th>Intf</th>
<th>AP Mac Address</th>
<th>ESS Name</th>
<th>AvgRSS</th>
<th>Type</th>
<th>Chan</th>
<th>WEP</th>
<th>WPA</th>
<th>Last</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:2:1</td>
<td>00:04:96:05:80:B0 Extreme_a</td>
<td>18</td>
<td>bss</td>
<td>36</td>
<td>Y</td>
<td>Y</td>
<td>19:05:33</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:CA:C0 Extreme_a</td>
<td>7</td>
<td>bss</td>
<td>40</td>
<td>Y</td>
<td>Y</td>
<td>19:05:33</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:05:82:80 Extreme_a</td>
<td>5</td>
<td>bss</td>
<td>40</td>
<td>Y</td>
<td>Y</td>
<td>19:05:33</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:05:80:F0 fz-dot1x-128</td>
<td>30</td>
<td>bss</td>
<td>56</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:05:81:50 Extreme_a</td>
<td>9</td>
<td>bss</td>
<td>64</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:00:00 wpadyn-a-aes-e</td>
<td>6</td>
<td>bss</td>
<td>48</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:23:60 DEFAULT_ESS</td>
<td>10</td>
<td>bss</td>
<td>52</td>
<td>N</td>
<td></td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:04:30 fz-open-wep-64</td>
<td>27</td>
<td>bss</td>
<td>64</td>
<td>Y</td>
<td></td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:02:40 fz-dot1x-128</td>
<td>25</td>
<td>bss</td>
<td>157</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:23:B0 fz-web-unsecure</td>
<td>24</td>
<td>bss</td>
<td>64</td>
<td>N</td>
<td></td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:3C:70 fz-web-unsecure</td>
<td>2</td>
<td>bss</td>
<td>64</td>
<td>N</td>
<td></td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0C:5F:F0 md-5</td>
<td>9</td>
<td>bss</td>
<td>161</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0D:9E:C0 wpapsk</td>
<td>13</td>
<td>bss</td>
<td>161</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0D:B4:20 QADS300-2410</td>
<td>149</td>
<td>bss</td>
<td>161</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0D:9E:C0 wpapsk</td>
<td>13</td>
<td>bss</td>
<td>161</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:04:96:0D:77:90 Extreme_a</td>
<td>3</td>
<td>bss</td>
<td>161</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
<tr>
<td>1:2:1</td>
<td>00:30:F1:92:44:39 fz-wpa-psk-tkip</td>
<td>39</td>
<td>bss</td>
<td>153</td>
<td>Y</td>
<td>Y</td>
<td>19:05:34</td>
<td></td>
</tr>
</tbody>
</table>
```

The following example shows detail AP scan results for port 2:2 and interlace 1:

```
show wireless ports 2:2 interface 1 ap-scan results detail
```

The output of the command is similar to:

```
Intf       :  2:2:1
AP Mac Address :  00:04:96:05:80:B0
ESS Name    :  Extreme_a
Network Type:  bss
Channel     :  36
First Seen  :  21:23:04
Last Change :  21:23:04
Rate Set    :  6,9*,12,18*,24,36*,48*,54*
Ext. Rate Set:
Number of Beacons   :  2
Number of Probes    :  0
RSS:  Min : 35
      Max : 37
      Avg : 23

WPA Information
Version     :  1
Unicast Ciphers : TKIP
Multicast Ciphers : WEP104
WPA Auth Suite :  DOT1X
```
Capability Information
N - G Short Slot
N - Channel Agility
N - PBCC
N - CF Poll REQ
N - CF Pollable
Y - WEP Required
bss - Network Type
L - Preamble

Intf : 2:2:1
AP Mac Address : 00:04:96:0C:CA:C0
ESS Name : Extreme_a
Network Type : bss
Channel : 40
First Seen : 21:23:04
Last Change : 21:23:04
Rate Set : 6,9*,12,18*,24,36*,48*,54*
Ext. Rate Set :
Number of Beacons : 1
Number of Probes : 0
RSS: Min : 14
Max : 14
Avg : 7

WPA Information
Version : 1
Unicast Ciphers : TKIP
Multicast Ciphers : WEP104
WPA Auth Suite : DOT1X

Capability Information
Y - G Short Slot
N - Channel Agility
N - PBCC
N - CF Poll REQ
N - CF Pollable
Y - WEP Required
bss - Network Type
L - Preamble

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface ap-scan results mac-address

show wireless ports [all | <portlist>] interface [1 | 2] ap-scan results <mac-address>

**Description**
Displays information about an access point (AP) whose MAC address is selected from the AP scan results table.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports, an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies the MAC address selected from the AP scan results table.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to get information about an AP using its MAC address.

**Example**
The following example display information about an AP by MAC address:

```
show wireless ports 1:8 interface 2 ap-scan results 00:04:96:5:80:B0:
```

The output of the command is similar to:

```
AP Mac Address    Intf   ESS Name       AvgRSS Type Chan WEP WPA Last
================================================================================
00:04:96:05:80:B0 1:8:2  Extreme_g      8      bss  11   Y       23:53:34
```

**History**

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches. `show wireless ports interface ap-scan status`

```
show wireless ports [<portlist> | all] interface [1|2] ap-scan status
```

**Description**
Displays the status of the AP scan for the port and interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;portlist&gt;</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to check the AP scan status on a particular port and interface.

**Examples**
The following command shows the status of the AP scan for the port and interface:
```
show wireless port 1:5 interface 1 ap-scan status
```
The output of the command is similar to the following:

```
Intf  Enabled  Num-Probes  Num-APs  WaterMark  TimeOuts  Overflows  OCS
--------------------------------------------------------------------------
1:1    N        0          0        0         0        0         N
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client mac-statistics

show wireless ports [all | <portlist>] interface [1 | 2] client <mac-address> mac-statistics

Description
Displays information about a client whose MAC address is selected from the client list.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies the MAC address of the client network interface card.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to review MAC statistic information for a client by MAC address.

Example
The following example displays MAC statistic information for port 1:8 on interface 1:

```
show wireless ports 1:8 interface 1 client 00:0D:54:98:AC:35 mac-statistics
```

The output of the command is similar to:

```
Intf            : 1:8:1
AP Mac Address  : 00:0D:54:98:AC:35
RSS:    Min        : 0
Max        : 0
Avg        : 0
Total PROBE REQ   : 0
Total AUTH REQ    : 1
Total ASSOC REQ   : 2
Total REASSOC REQ : 0
Total DEASSOC REQ : 0
Total DEAUTH REQ  : 0
Total PS POLL     : 0
Total Data Frames : 0
NAV Value        : 0
--------------------------------------------------------------------------------------
```

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-history configuration

show wireless ports [<portlist> | all] interface [1 | 2] client-history configuration

**Description**
Displays the current configuration of the client history and diagnostic features.

**Syntax Description**

```
portlist  Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.
all       Specifies all active ports.
interface Specifies an interface: 1 or 2.
```

**Default**
N/A

**Usage Guidelines**
Use this command to see the current configuration of the client-history feature for the specified wireless port and interface.

**Example**
The following example displays the client history and diagnostic features on port 1:25 and interface 1:

```
show wireless ports 1:25 interface 1 client-history configuration
```

The output of the command is similar to:

```
Intf   Enabled   TableSize  Timeout
----------------------------------------
1:25:1 Y           128        600
```

**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-history diagnostics

show wireless ports [<portlist> | all] interface [1 | 2] client-history diagnostics <mac_address>

Description
Displays counters and errors the information collected on a per-client basis.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies the MAC address of the wireless client.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to display diagnostic counters and error information contained in the extremeWirelessClientDiagTable.

Example
The following example displays client-history diagnostics information for port 1:25 and interface 1 based on the MAC address of the client:

```bash
show wireless ports 1:25 interface 1 client-history diagnostics 00:0D:54:98:AC:35
```

The output of the command is similar to:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>1:25:1</td>
</tr>
<tr>
<td>AP Mac Address</td>
<td>00:0D:54:98:AC:35</td>
</tr>
<tr>
<td>State Watermark</td>
<td>FORWARDING</td>
</tr>
<tr>
<td>Events In Detected</td>
<td></td>
</tr>
<tr>
<td>Enters</td>
<td>1</td>
</tr>
<tr>
<td>Errors</td>
<td>0</td>
</tr>
<tr>
<td>AUTH REQ</td>
<td>0</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
</tr>
<tr>
<td>MGMT Action</td>
<td>0</td>
</tr>
<tr>
<td>Time Outs</td>
<td>0</td>
</tr>
<tr>
<td>Events In Authenticated</td>
<td></td>
</tr>
<tr>
<td>Enters</td>
<td>1</td>
</tr>
<tr>
<td>Errors</td>
<td>0</td>
</tr>
<tr>
<td>ASSOC REQ</td>
<td>1</td>
</tr>
<tr>
<td>Other</td>
<td>1</td>
</tr>
<tr>
<td>MGMT Action</td>
<td>0</td>
</tr>
<tr>
<td>Time Outs</td>
<td>0</td>
</tr>
<tr>
<td>Events In Associated</td>
<td></td>
</tr>
</tbody>
</table>
Enters : 1
Errors : 0
MGMT Action : 0
Time Outs : 0

Events In Forwarding
Enters : 1
MGMT Action : 0
Time Outs : 1

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-history mac-layer

show wireless ports [<portlist> | all] interface [1 | 2] client-history mac-layer <mac_address>

**Description**
Displays 802.11 MAC layer information collected on a per-client basis.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies the MAC address of the wireless client.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to display information on the operation of the 802.11 MAC layer.

**Example**
The following example displays client-history information for port 1:25 and interface 1 based on the MAC address of the client:

```
show wireless ports 1:25 interface 1 client-history mac-layer 00:0D:54:98:AC:35
```

The output of the command is similar to:

```
Intf : 1:25:1
AP Mac address : 00:0D:54:98:AC:35

Authentication Information
Authenticated : Y
Total AUTH REQ : 1
Total AUTH RESP : 1
Total AUTH OK : 1
Total AUTH Failed : 0
Total AUTH (open) : 0
Total AUTH (shared) : 1
Last AUTH REQ : 19:40:06
Last Auth Type : OPEN

Authentication Error Information
Last Error Time : 00:00:00
Last Error Type : NONE
Errors by Type
  Sequence Number : 0
  Challenge Text (key) : 0
  Type Mismatch (open|shared) : 0
```
Key Index : 0
Other : 0

Association Information
Associated : Y
Total ASSOC REQ : 2
Total REASSOC REQ : 0
Total ASSOC RESP : 1
Total ASSOC OK : 1
Total ASSOC Fail : 0

Association Error Information
Last Error Time : 00:00:00
Last Error Type : NONE
Errors by Type
Rate Mismatch : 0
Capability : 0
Counter Measure : 0
Cipher Suite : 0
Max Associations : 0
RSN Required : 0
RSN Mismatch : 0
Other : 0
Rate Set : 6*,9*,12*,18*,24*,36*,48*,54*

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-history status

show wireless ports [<portlist> | all] interface [1 | 2] client-history status

Description
Displays the current status of the historical client information.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. May be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command displays information about the client diagnostic and history database. The output has the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>This value indicates if historical information is being collected on this interface or not.</td>
</tr>
<tr>
<td>TableSize</td>
<td>This is the number of entries allowed in each of the historical client tables.</td>
</tr>
<tr>
<td>Timeout</td>
<td>This is the time, in seconds, that entries will persist in the historical client tables after the referenced client is removed from the SIB.</td>
</tr>
<tr>
<td>CurrentSize</td>
<td>The current number of entries in the historical client database</td>
</tr>
<tr>
<td>Watermark</td>
<td>The maximum number of entries which have ever been in the historical client database.</td>
</tr>
<tr>
<td>Overflows</td>
<td>Number of entries which have been overwritten in order to make room for a new entry.</td>
</tr>
<tr>
<td>AgeOuts</td>
<td>Number of entries which have been aged out of the table</td>
</tr>
</tbody>
</table>

Example
The following example displays the client diagnostic information for port 1 and interface 1:

```
show wireless ports 1 interface 1 client-history status
```

The output of the command is similar to:

```
Intf   Enabled TableSize Timeout CurrSize Watermark Overflows Ageouts
-----------------------------------------------
 1:1   N       128       600     0        0         0         0
```
History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-scan configuration

`show wireless ports [<portlist> | all] interface [1 | 2] client-scan configuration`

**Description**
Displays the current configuration of the client scan feature.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Displays the current configuration of the client scan feature, including:

- **Port:** The port number used in the scan
- **Interface:** 1 or 2
- **Enabled:** Y (yes) N (no)
- **Send Added:** on | off
- **Send Removed:** on | off
- **Timeout:** Parameter specified for scan timeouts
- **Max Size:** Parameter specified for the number of entries for the table

**Examples**
The following example displays the current configuration of the client scan feature on port 1:5 and interface 1:

```
show wireless ports 1:5 interface 1 client-scan configuration
```

It produces output similar to the following:

```
Summit300-48:15 # show wireless ports all interface 1 client-scan configuration
Intf  Enabled  Send-Added  Send-Removed  Timeout  Max-Size
--------------------------------------------------------------
  1:5:1 N       off       off       600       128
```
**History**
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-scan results

    show wireless ports [<portlist> | all] interface [1 | 2] client-scan results {detail}

**Description**
Displays the current contents of the probe information table.

**Syntax Description**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The output of this command displays the probe information table, which has the following fields:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intf</td>
<td>Wireless port and interface on which this client is seen</td>
</tr>
<tr>
<td>MAC address of the source</td>
<td>MAC address of the source</td>
</tr>
<tr>
<td>Probe REQs</td>
<td>Number of PROBE REQ packets seen from this source</td>
</tr>
<tr>
<td>Last RSS</td>
<td>RSSI of last received PROBE REQ packet</td>
</tr>
<tr>
<td>Channel</td>
<td>Channel on which last PROBE REQ was received</td>
</tr>
<tr>
<td>Last Seen</td>
<td>Time last PROBE REQ was seen from this source</td>
</tr>
<tr>
<td>Client</td>
<td>Client is associated to the Altitude 300 (Y</td>
</tr>
</tbody>
</table>

**Example**
The following example displays the probe information table for port 1:25 and interface 2:

    show wireless port 1:25 interface 2 client-scan results

This command produces output similar to the following:

<table>
<thead>
<tr>
<th>Intf</th>
<th>Source</th>
<th>Probe REQs</th>
<th>Last RSS</th>
<th>Channel</th>
<th>Last Seen</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:25:2</td>
<td>00:20:A6:4C:40:69</td>
<td>8005</td>
<td>52</td>
<td>1</td>
<td>19:37:36</td>
<td>N</td>
</tr>
<tr>
<td>1:25:2</td>
<td>00:09:5B:92:43:63</td>
<td>262</td>
<td>34</td>
<td>1</td>
<td>19:37:37</td>
<td>N</td>
</tr>
<tr>
<td>1:25:2</td>
<td>00:09:5B:68:27:A6</td>
<td>482</td>
<td>43</td>
<td>1</td>
<td>19:37:37</td>
<td>N</td>
</tr>
<tr>
<td>1:25:2</td>
<td>00:09:5B:66:ED:F3</td>
<td>390</td>
<td>47</td>
<td>1</td>
<td>19:37:35</td>
<td>N</td>
</tr>
<tr>
<td>1:25:2</td>
<td>00:09:5B:66:E4:C9</td>
<td>314</td>
<td>12</td>
<td>1</td>
<td>19:37:30</td>
<td>N</td>
</tr>
</tbody>
</table>
History

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-scan results mac-address

    show wireless ports [<portlist> | all] interface [1 | 2] client-scan results <mac_address> {detail}

Description
Displays the details about the specified client MAC address.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to check details about the clients in the client scan table.

Example
The following example shows the details of client MAC address 00:03:7F:BE:FE:9D.

    show wireless port 5 interface 1 client-scan results 00:03:7F:BE:FE:9D

It produces output similar to the following:

<table>
<thead>
<tr>
<th>Intf</th>
<th>Source</th>
<th>Probe REQs</th>
<th>Last RSS</th>
<th>Channel</th>
<th>Last Seen</th>
<th>Client</th>
</tr>
</thead>
<tbody>
<tr>
<td>5:1</td>
<td>00:03:7F:BE:FE:9D</td>
<td>17</td>
<td>4</td>
<td>161</td>
<td>01:39:48</td>
<td>N</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface client-scan status

show wireless ports [<portlist> | all] interface [1 | 2] client-scan status

**Description**
Displays the overall operation of the client scan results.

**Syntax Description**

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The output of this command displays the performance results for the following variables on a per wireless interface basis:

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CurrentTableSize</td>
<td>The current size of the table (in entries)</td>
</tr>
<tr>
<td>TableWatermark</td>
<td>The maximum size the table has been since the last reset of the historical statistics</td>
</tr>
<tr>
<td>TotalOverflows</td>
<td>The number of times an entry has been overwritten because the table is full</td>
</tr>
<tr>
<td>TotalTimeouts</td>
<td>The number of times an entry has been aged out from the table</td>
</tr>
<tr>
<td>LastElement</td>
<td>The last time an element was added to the table</td>
</tr>
<tr>
<td>TotalProbes</td>
<td>The total number of probes received on this interface</td>
</tr>
</tbody>
</table>

**Examples**
The following example displays the performance results for port 5 on interface 1:

```bash
show wireless ports 5 interface 1 client-scan status
```

It produces output similar to the following:

```
S300-24-FZ:28 # show wireless ports 1 interface 1 client-scan status
    Intf   Table-Size WaterMark Overflows Timeouts LastElement Total-Probes
-----------------------------------------------
    1:1    0          0         0         0        0         0       0
S300-24-FZ:29 #
```
History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface clients

    show wireless ports [<portlist> | all] interface [1 | 2] clients [<mac-address> (detail) | {detail}]

Description
Displays the current wireless client state of a selected port or ports and interface.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. an be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies to use the MAC address to select the client from the client list.</td>
</tr>
<tr>
<td>detail</td>
<td>(Optional) Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Client current state information is available for all clients that have sent an authentication message to the Altitude 300. Information in this table is timed out if no packets are received from the client by the configurable period of time set by the administrator.

The following fields of the client state table are displayed with this command:

<table>
<thead>
<tr>
<th>Fields</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client MAC</td>
<td>MAC address of the client adapter</td>
</tr>
<tr>
<td>Current State</td>
<td>DETECTED, AUTHED, ASSOC, or FORWARD. Indicates which part of the state machine the client is currently in.</td>
</tr>
<tr>
<td>Last state change</td>
<td>The system time when the client last changed states</td>
</tr>
<tr>
<td>Encryption Type</td>
<td>Type of MAC-level encryption the client is using. This is negotiated during the association state machine, so is only valid if client state is FORWARDING.</td>
</tr>
<tr>
<td>Authentication Type</td>
<td>Last type of authentication the client tried. In the case of a client in FORWARDING, indicates the type of authentication that granted access to the network.</td>
</tr>
<tr>
<td>ESSID</td>
<td>Extended service set identifier of the network</td>
</tr>
<tr>
<td>Wireless Port</td>
<td>Wireless switch port serving the client</td>
</tr>
<tr>
<td>Client VLAN</td>
<td>VLAN assigned to this client by a radius VSA or other mechanism. This is only valid for clients in FORWARDING.</td>
</tr>
<tr>
<td>Client Priority</td>
<td>Quality of service (QoS) level for the client</td>
</tr>
<tr>
<td>Tx Frames</td>
<td>Number of frames transferred to the client</td>
</tr>
<tr>
<td>Rx Frames</td>
<td>Number of frames returned by the client</td>
</tr>
<tr>
<td>Tx Bytes</td>
<td>Number of bytes transferred to the client</td>
</tr>
<tr>
<td>Rx Bytes</td>
<td>Number of bytes returned by the client</td>
</tr>
</tbody>
</table>
Example

The following command displays information about client MAC address 00:09:5B:A1:1F:8F on port 1:

```bash
show wireless ports 1 interface 1 clients 00:09:5B:A1:1F:8F detail
```

The output of the command is similar to:

```plaintext
Client MAC : 00:09:5B:A1:1F:8F
Wireless Port : 1:1
Current State : FORWARD
Last State Change : 4:42:39
Authentication Type : PSK
Encryption Type : AES
ESS ID : fz-wpa-psk-aes
Client VLAN : SKSPVlan
Client Priority : 0
Received Signal Strength : 195
TX Frames : 17067
RX Frames : 34228
TX Bytes : 1712753
RX Bytes : 3857802
```

History

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface configuration

show wireless ports [<portlist> | all] interface [1 | 2] configuration (detail)

**Description**
Displays information about wireless configuration for the selected ports and interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3:5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Use this command to show in table or list format the configuration and state of the interface of the selected port or ports.

**Examples**
The following example displays information about the wireless port configuration for ports 1:26-1:30 and interface 1:

```plaintext
show wireless ports 1:26-1:30 interface 1 configuration
```

Output of the command is similar to:

<table>
<thead>
<tr>
<th>Port</th>
<th>Intf</th>
<th>State</th>
<th>RF Prof.</th>
<th>Sec. Prof.</th>
<th>TxRate</th>
<th>Power</th>
<th>Chan.</th>
<th>Max Cl.</th>
<th>Bridging</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:26</td>
<td>1 EN</td>
<td>rf_26</td>
<td>Unsecure</td>
<td>54</td>
<td>FULL</td>
<td>0</td>
<td>100</td>
<td>EN</td>
<td></td>
</tr>
<tr>
<td>1:27</td>
<td>1 EN</td>
<td>rf_27</td>
<td>Unsecure</td>
<td>54</td>
<td>FULL</td>
<td>0</td>
<td>100</td>
<td>EN</td>
<td></td>
</tr>
<tr>
<td>1:28</td>
<td>1 EN</td>
<td>rf_28</td>
<td>Unsecure</td>
<td>54</td>
<td>FULL</td>
<td>0</td>
<td>100</td>
<td>EN</td>
<td></td>
</tr>
<tr>
<td>1:29</td>
<td>1 EN</td>
<td>DEFAULT_A</td>
<td>Unsecure</td>
<td>54</td>
<td>FULL</td>
<td>0</td>
<td>100</td>
<td>EN</td>
<td></td>
</tr>
<tr>
<td>1:30</td>
<td>1 EN</td>
<td>DEFAULT_A</td>
<td>Unsecure</td>
<td>54</td>
<td>FULL</td>
<td>0</td>
<td>100</td>
<td>EN</td>
<td></td>
</tr>
</tbody>
</table>

EN = Enabled, DIS = Disabled

The following example shows the extra details shown when the keyword detail is added to the command:

```plaintext
show wireless ports 1:26-1:30 interface 1 configuration detail
```
The detailed output is similar to:

```
Summit300-48:20 # show wireless ports 1:26-1:30 interface 1 configuration detail

Wireless Interface: 1:26:1
  State: Enabled
  RF Profile: rf_26
  Security Profile: Unsecure
  Transmit Rate: 54
  Power: FULL
  Channel: 0
  Max Clients: 100
  Wireless Bridging: Enabled

Wireless Interface: 1:27:1
  State: Enabled
  RF Profile: rf_27
  Security Profile: Unsecure
  Transmit Rate: 54
  Power: FULL
  Channel: 0
  Max Clients: 100
  Wireless Bridging: Enabled

Wireless Interface: 1:28:1
  State: Enabled
  RF Profile: rf_28
  Security Profile: Unsecure
  Transmit Rate: 54
  Power: FULL
  Channel: 0
  Max Clients: 100
  Wireless Bridging: Enabled

Wireless Interface: 1:29:1
  State: Enabled
  RF Profile: DEFAULT_A
  Security Profile: Unsecure
  Transmit Rate: 54
  Power: FULL
  Channel: 0
  Max Clients: 100
  Wireless Bridging: Enabled

Wireless Interface: 1:30:1
  State: Enabled
  RF Profile: DEFAULT_A
  Security Profile: Unsecure
  Transmit Rate: 54
  Power: FULL
  Channel: 0
  Max Clients: 100
  Wireless Bridging: Enabled
```
History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface pae-diagnostics

show wireless ports [<portlist> | all] interface [1 | 2] pae-diagnostics {detail}

Description
Displays Port Authentication Entity (PAE) diagnostics for the selected port and interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. May be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to display the PAE diagnostics of the clients associated with the access point (AP).

Examples
The following example lists the output of the PAE diagnostics for ports 1:11 on interface 2:

```
show wireless ports 1:11 interface 2 pae-diagnostics
```

The output of the command is similar to:

```
PAE Diagnostic Statistics
CLIENT MAC Port Intf Failures Timeouts Success Logoffs ReAuth
================================================================================
00:0D:54:98:AC:35 1:11 2 0 0 2 0 0
```

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.

```
show wireless ports interface pae-statistics
```

```
show wireless ports [<portlist> | all] interface [1 | 2] pae-statistics
(detai
```

**Description**

Displays Port Authentication Entity (PAE) statistics for the selected port and interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Use this command to display the PAE statistics of the clients associated with the access point (AP).

**Examples**

The following example lists the output of the PAE statistics for ports 1:11 on interface 2:

```
show wireless ports 1:11 interface 2 pae-statistics
```

The output of the command is similar to:

```
PAE Statistics
CLIENT MAC Port Intf STATE TX RX ERRORS CLIENT ID
===================================================================
00:0D:54:98:AC:35 1:11 2 AUTHED 16 17 0 sqalab\labu
```

**History**

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches. 

```
show wireless ports interface rf-status
```

```
show wireless ports [<portlist> | all] interface [1 | 2] rf-status {detail}
```

**Description**

Displays data rates for the selected port and interface. If Dynamic Frequency Selection (DFS) is used, the detail command output includes a list of channels on which interference is detected.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Each wireless port on the Summit 300 contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The `show wireless port interface rf-status` command allows you to display information about one of the two individual interfaces (1|2) on a port or ports.

**Examples**

The following example displays RF status of all active ports of the switch:

```
show wireless ports all interface 1 rf-status
```

```
Port    Intf  Tx Rate  Channel  Noise Floor
-------- ------- -------- -------- ------------
1:37     1      54      64       85
1:38     1      54      64       84
```

The following command shows detailed RF status. The output includes a list of channels recorded in the no-occupancy list (NOL) due to RADAR interference for the DFS feature.

```
show wireless ports all interface 1 rf-status detail
```

```
Wireless Interface: 15:1
Transmit Rate: 54
Beacon Interval: 40
DTIM: 2
Preamble: Short
Long Retry: 7
Short Retry: 4
Fragmentation Length: 2345
RTS Threshold: 2330
```
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Power</td>
<td>FULL</td>
</tr>
<tr>
<td>RF Mode</td>
<td>A</td>
</tr>
<tr>
<td>Channel</td>
<td>48</td>
</tr>
<tr>
<td>Noise Floor (dBm)</td>
<td>82</td>
</tr>
<tr>
<td>Supported Rates</td>
<td>6, 9, 12, 18, 24, 36, 48, 54</td>
</tr>
<tr>
<td>Supported Modes</td>
<td>A</td>
</tr>
<tr>
<td>Channels with RADAR interface</td>
<td>52, 56</td>
</tr>
</tbody>
</table>

**History**

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

**Platform Availability**

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface security-status

show wireless ports [<portlist> | all] interface [1 | 2] security-status {detail}

**Description**
Displays Wired Equivalent Privacy (WEP) protocol, authentication, dot1x, and ESS name information for the selected port and interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Each wireless port on the switch contains two interfaces. Interface 1 supports 802.11a, and interface 2 supports 802.11b/g radio signals. The `show wireless port interface security-status` command allows you to display security status information about one of the two individual interfaces (1|2) on one or more ports.

**Examples**
The following example displays the security setting of all active wireless ports of the switch:

```
show wireless ports all interface 2 security-status
```

The output of the command is similar to:

<table>
<thead>
<tr>
<th>Port</th>
<th>Intf</th>
<th>Dot11 Auth</th>
<th>Network Auth</th>
<th>ESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:37</td>
<td>2</td>
<td>shared</td>
<td>none</td>
<td>TFZ</td>
</tr>
<tr>
<td>1:38</td>
<td>2</td>
<td>open</td>
<td>none</td>
<td>fz-open-wep-64</td>
</tr>
</tbody>
</table>

The following example shows the detailed security setting of all active wireless ports of the switch:

```
show wireless ports all interface 2 security-status detail
```

The output of the command is similar to:

<table>
<thead>
<tr>
<th>Wireless Interface:</th>
<th>1:37:2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dot11 Authentication:</td>
<td>shared</td>
</tr>
<tr>
<td>Network Authentication:</td>
<td>none</td>
</tr>
<tr>
<td>ESS Name:</td>
<td>TFZ</td>
</tr>
<tr>
<td>Encryption:</td>
<td>wep128</td>
</tr>
</tbody>
</table>
Specified WEP Keys: 0,1,2,3
Default WEP Key: 0
SSID in Beacon: on
User VLAN: ExtrAvaya
Use Dynamic Vlan: Yes

Wireless Interface: 1:38:2
Dot11 Authentication: open
Network Authentication: none
ESS Name: fz-open-wep-64
Encryption: wep64
Specified WEP Keys: 0
Default WEP Key: 0
SSID in Beacon: on
User VLAN: SKSPVlan
Use Dynamic Vlan: Yes
Noise Floor (dBm): 85
Supported Rates: 6,9,12,18,24,36,48,54
Supported Modes: A

History
This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
show wireless ports interface stats

show wireless ports [<portlist> | all] interface [1 | 2] stats

Description
Displays 802.11 interface statistics for the selected port and interface.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to search for errors on a per interface basis.

Examples
The following example displays 802.11 interface statistics for ports 1:5-1:34 and interface 1:

show wireless ports 1:5-1:34 interface 1 stats

The output of the command is similar to:

<table>
<thead>
<tr>
<th>802.11 Interface Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
</tr>
<tr>
<td>------</td>
</tr>
<tr>
<td>2</td>
</tr>
</tbody>
</table>

History

Platform Availability
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.

**show wireless ports interface status**

```
show wireless ports [<portlist> | all] interface [1 | 2] status
```

**Description**

Displays the current state of the selected port and interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. An be one or more port numbers. May be in the form 1, 2, 1-2, 3-5.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all active ports.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies an interface: 1 or 2.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

Use this command to examine RF profiles on a per wireless port basis. This command allows you to view the log of a specific port or ports, filtering out the switch log.

**Examples**

The following example displays the status for wireless ports 3 on interface 1:

```
show wireless ports 3 interface 1 status
```

The output of the command is similar to:

```
Intf    St. Tx Rate Power Ch ESS                Max Cl. Last State Change
-------------------------------------------------------------------------------
3:1     EN  54      FULL      52  fz-wpa-psk-aes     100     Mon Jul 26 17:15:11 2004
```

**History**

**Platform Availability**
This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches. **show wireless ports log**

```
show wireless ports [<portlist>| all] log {summary}
```

**Description**

Displays the event log of the selected port or ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Description</th>
<th>Syntax</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Can be one or more port numbers. May be in the form 1, 2, 1-2, 3-5.</td>
</tr>
<tr>
<td>summary</td>
<td>Specifies to display a summary of the log information.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Use this command to display the Altitude 300 local log for debugging errors.

**Examples**

The following command displays log information for all ports on the device:

```
show wireless ports all log
```

The output of the command is similar to:

```
S300-24-P2:36 # show wireless ports 3 log
Log Servers for port 3:
    Server 192.168.1.244:514, Facility local0, Severity info
[3] Jul 26 17:51:06 :2 Client 00:0C:41:2B:E4:27 aged out (name "OPEN:labupda@labuwifi.com")
[3] Jul 26 17:40:00 :2 DOT1X 00:0C:41:2B:E4:27 Exhausted retries on RADIUS servers.
[3] Jul 26 17:17:36 :2 Client 00:0D:88:C2:4D:AC Auth Failed (name "802.1x:unknown")
[3] Jul 26 17:15:10 :1 Radio channel updated to 52
```
Wireless Commands

This command was first available in ExtremeWare 6.2a and added to the “e” series in 7.3e.

Platform Availability

This command is available on the Summit 300-48, Summit 300-24, Summit 400-24p and Alpine switches.
unconfigure wireless ports ipaddress

unconfigure wireless ports <portlist> ipaddress

Description
Unconfigures the source IP address for the specified port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. Must be one or more port numbers. May be in the form 1, 2, 1:2, 3-5.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to delete the ipaddress for a wireless port.

Examples
The following command deletes the IP address for port 1:18 on the Summit 300-48:

unconfigure wireless ports 1:18 ipaddress

History

Platform Availability
This chapter describes commands for managing switch stacking. The commands include:

- Enabling or disabling stacking.
- Configuring stacking priority.
- Saving stacking configurations.
- Determining if stacking is enabled or disabled.
- Configuring or unconfiguring stacking for fall back IP addresses.
- Configuring a request for a slot number.
- Binding a slot to a MAC address.
- Showing stack and slot configurations

The following command are also related to stacking, but are located in other chapters in this manual:

- `configure debug-trace stacking`
- `download image hostname filename`
- `run diagnostics`
- `save configuration`
- `show slot`

**NOTE**

When stacking is enabled, the above commands support the stacking slot number. Otherwise, the slot number is not recognized in the commands.

## Introducing Stacking

*Stacking* allows users to physically connect up to eight individual Summit switches together as a single logical unit. This logical unit behaves as a single switch with a single IP address and a single point of authentication.

In ExtremeWare, a stack is controlled by a master switch, called the *stack manager*. The stack manager runs full ExtremeWare and is responsible for maintaining all of the software tables for all the switches in the stack. There can only be one stack manager in a stack of switches. The remaining switches in the
Stacking Commands

stack are considered to be stack members. Because the stack manager maintains all of the software tables, stack members need only run a sub-set of ExtremeWare.

An easy way to understand a stack is to think of a stack being a virtual chassis. Each stack member acts as if it were a slot in a chassis and waits for configuration information from the stack manager. The high-speed stacking links are like the backplane of the stack and are called stacking ports.

The stack manager stores any configuration information for the stack in its primary or secondary flash memory. Because the stack manager has the knowledge of the state and the configuration of all the other switches in the stack, it can respond to all external requests for those switches. For example, the stack manager can respond to a request for SNMP information from all ports within the stack.

**Stack Discovery and Manager Election**

The order in which ExtremeWare assigns the stack manager and the stack members is called stack discovery. The process of determining the stack manager for the stack is referred to as the election of the manager. If stacking is enabled at switch startup, the switch comes up running the sub-set of ExtremeWare. Stack discovery starts by sending and receiving probe packets among the members of the stack until all the members are known. The priority of each switch is evaluated and if one switch alone has the highest priority, that switch is elected as the manager. If two or more switches have the same priority, the switch with the lowest MAC address is elected the stack manager. The remaining switches are assigned a stacking ID based upon the same evaluation of their priority and MAC address. The stack manager runs from this point with the full version of ExtremeWare.
**configure stacking fallback-ip-address**

```
configure stacking fallback-ip-address <address> {</mask-length>|<mask>}
[slot <slotnumber> vlan <vlan-id]}
```

**Description**

Configures a backup IP address to protect against duplicate IP addresses.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>address</td>
<td>Specifies the IP address of the VLAN ID or default VLAN.</td>
</tr>
<tr>
<td>mask-length</td>
<td>Specifies a subnet mask as the number of bits (e.g. /24).</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a mask in dotted-quad notation (e.g. 255.255.255.0).</td>
</tr>
<tr>
<td>slotnumber</td>
<td>Specifies the ID of a switch in a stack.</td>
</tr>
<tr>
<td>vlan-id</td>
<td>Specifies the VLAN ID of the management VLAN.</td>
</tr>
</tbody>
</table>

**Default**

None

**Usage Guidelines**

If the stack master should lose connectivity with the stack members, the stack would separate into two segments. Each of the segments would become independent stacks and inherits the same configuration from the previous single stack. When a stack splits into two segments, a duplicate management IP address can result causing the switch not to be manageable or accessible through telnet.

To prevent a duplicate IP address, assign a fall back IP address for each slot. The fall back IP address configuration is stored in the NVRAM and is not part of the system configuration. Because the fall back IP address is stored in non-volatile storage, users can individually specify the fall back IP address for each slot.

For Summit 200 and Summit 300-24 systems, the fall back IP is configured on the given VLAN ID. If the VLAN ID is not configured, then the IP Address is configured for the default VLAN. For Summit 400 systems operating as a slot, the VLAN option is not applicable. In Summit 400 systems, the fall back IP address protects the IP address of the VLAN to which the management port is assigned.

If the slot number is not given, the configuration is applied for the local switch.

**NOTE**

The same duplicate IP address scenario can occur with other VLANs. Take appropriate care to prevent any operational issues that can arise due to duplicate IP addresses being used in a non-management VLAN.

**Example**

The following example sets a fall back IP address for slot 5:

```
configure stacking fallback-ip-address ipaddress 10.12.123.1 255.255.255.0 slot 5
```
History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
configure stacking priority

configure stacking priority <number>[<slot <slot-number> | all ]

Description
Configures a stacking priority on specified switch, or on all switches in the stack.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Assigns a numeric value as the priority. Valid ranges are 0 to 15 with 15 being the highest priority and 0 being the lowest priority.</td>
</tr>
<tr>
<td>slot-number</td>
<td>Configures stacking priority on one or more switches using the slot number of the switch in the stack.</td>
</tr>
<tr>
<td>all</td>
<td>Configures stacking priority on all ports and switches in the stack.</td>
</tr>
</tbody>
</table>

Default
The current slot (switch).

Usage Guidelines
Use this command to configure the priority of switches in the stack. The stack manager should have the highest priority in the stack. If you configure all of the switches to have the same priority using the all parameter, the stack manager will raise its priority internally to remain the stack manager.

Example
In the following examples, slot 2 is the stack manager of a stack containing four switches. This example assigns the stack manager the highest priority in the stack:

```
configure stacking priority slot 2 15
```
In this example, stacking priority is also given to slot 1:

```
configure stacking priority slot 1 14
```
The result is that slot 1 has priority over slots 3 and 4, but not over slot 2.

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
configure stacking requested-slot

configure stacking requested-slot <slot number> [current-slot <slot number>]

Description
Configures a request to the stack manager for a specific slot number in the stack.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>requested-slot &lt;slot number&gt;</td>
<td>Specifies the desired slot ID the next time this member joins the stack.</td>
</tr>
<tr>
<td>current-slot &lt;slot number&gt;</td>
<td>Specifies the member's slot ID that is applicable for this request. If this option is not given, the command applies to the member on which it is run.</td>
</tr>
</tbody>
</table>

Default
The current slot (switch).

Usage Guidelines
Use this command to request a particular slot number for a member the next time the member joins the stack. If the slot number is unavailable, the stack manager can assign any available slot number.

Example
The following command requests a slot ID of 2 for the switch currently with the slot ID of 5:

```
configure stacking requested-slot 2 current-slot 5
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
configure stacking slot-binding

configure stacking slot-binding <slot number> <mac addr> module <switch model> [priority <number>]

Description
Configures the current slot number to MAC address binding of the switches in the stack.

Syntax Description

| slot number | Specifies to bind the switch with this slot ID to the MAC address. |
| mac addr    | Specifies the member's MAC address being bound to the slot.         |
| switch model| Specifies the Summit model number for the member. Valid entries are: |
|             | S200-24, S200-48, S300-24, S400-24t, S400-24p, S400-48t.            |
| priority <number> | (Optional) Specifies the current priority of the slot. |

Default
NA

Usage Guidelines
Use this command to ensure proper binding of the MAC address to a slot ID when the configuration is being uploaded to a TFTP server for reuse. When the configuration is downloaded from the TFTP server, the stack manager can update the MAC address binding for the members and properly assign the slot numbers and restore the stack.

This command can also be helpful for pre-staging, where multiple stacks exist that have identical configurations. In this case, the uploaded configuration can be modified with the proper MAC-address for the specific stack and downloaded.

Example
The following example binds MAC address 00:04:96:1F:88:21 to slot 3, a Summit 300-24:

```
configure stacking slot-binding 3 00:04:96:1F:88:21 module s300-24
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
disable stacking

disable stacking [port<port_list> | slot <slot-number> | all]

Description

This command disables stacking on the specified slot and port combination.

Syntax Description

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port_list</td>
<td>Specifies to disable stacking on one or more ports.</td>
</tr>
<tr>
<td>slot-number</td>
<td>Configures stacking priority on one or more switches using the slot number of the switch in the stack.</td>
</tr>
<tr>
<td>all</td>
<td>Disables all ports and switches in the stack.</td>
</tr>
</tbody>
</table>

Default

Disabled.

Usage Guidelines

Use this command to specify port and slot (switch) combinations, or use the all option to disable stacking on all elements.

By default, the disable stacking command disables stacking on all the previously stacking enabled ports on the current switch. When stacking is disabled, the switch acts as an independent single switch.

NOTE

In Summit 400-48 systems, the two stacking ports on the rear-side of the switch are represented by port numbers 52,53 respectively.

Example

The following command disables all stacking:

disable stacking all

The following command disables the third switch in the stack:

disable stacking slot 3

The following command disables ports 52 and 53 on a Summit 400-48:

disable stacking port 1:52,1:53

History

This command was first available in ExtremeWare 7.4.
Platform Availability

This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
enable stacking

   enable stacking [port <port_list>]

Description

This command enables stacking on the specified port.

Syntax Description

| port_list | Specifies to enable stacking on one or more ports. |

Default

The enable stacking command defaults to the following on the listed platforms:

Table 27: Stacking Default Ports

<table>
<thead>
<tr>
<th>Platform</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Summit 200-24</td>
<td>enable stacking port 25,26</td>
</tr>
<tr>
<td>Summit 200-48</td>
<td>enable stacking port 49,50</td>
</tr>
<tr>
<td>Summit 300-24</td>
<td>enable stacking port 25,26</td>
</tr>
<tr>
<td>Summit 400-24</td>
<td>enable stacking port 25,26</td>
</tr>
<tr>
<td>Summit 400-48</td>
<td>enable stacking port 52,53</td>
</tr>
</tbody>
</table>

Usage Guidelines

Use this command to enable stacking on the port list. After stacking is enabled, the port number appears as a slot and port combination, such as 1:49,1:50. If the slot and port format is not present, the command applies to the current switch.

Example

The following command enables stacking using the default ports:

   enable stacking

The following command enable stacking using unique ports:

   enable stacking ports 5,6

History

This command was first available in ExtremeWare 7.4.

Platform Availability

This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
show stacking

Description
This command displays information from the stacking database.

Syntax Description
This command has no options or parameters.

Default
Summary information.

Usage Guidelines
Use this command to display the stacking configuration. The detail option displays all information in the stacking database, including the platform type, MAC address, the enabled stacking ports, stack manager status, stack priority, and the fallback IP address (if configured).

The output of the command is in two parts. The first part is common information; the second is switch-specific information. The fields in the output represent:

- **Common Information**
  - Mode: Indicates whether the stack is connected in a ring or a non-ring (daisy-chain) mode.
  - State: The state of the slot:
    - Init: Applies to member slots only. It indicates that the stack manager has learned of the slot in a previous run, but has not been able to detect the slot in the current run.
    - Master-RPC: Occurs when the stack manager has not completed initialization for the member. The manager is attempting to obtain information from the member.
    - Up-Master: The switch elected as stack manager is fully operational.
    - Up-Slave: Member switches are operational and can be verified with the `show slot` command.
  - Stacking: Indicates whether stacking is enabled or disabled.
  - Master slot: Indicates the stack number of the stack manager.
  - Switches: Indicates the total number of switches in the stack.
  - Local slot: Indicates the local slot number.
  - Configured slot: Indicates that a user-configured request for a specific slot number exists.

- **Slot-Specific Information**
  - Status: Indicates whether the switch is active in the stack. If the switch is not yet part of the stack and the manager has learned of the switch during a previous run, then the state of Disabled displays until it is replaced by another switch.
  - Master: Indicates whether the switch is the stack manager.
  - MAC: Indicates the MAC address of the switch.
  - Binding: Indicates the slot binding and whether it is active or inactive. Slot binding is inactive until the switch joins the stack.
  - CPU Pri: Indicates the configured priority of the switch. The higher the number, the higher the priority.
Stacking Commands

Example

The following command displays all the information in the stacking database:

```
show stacking
```

Output from the command is similar to:

```
Stacking Data Base
==================
Common Info
Mode : Dup-No-Ring State : Up-Master Stacking : Enabled
Master Slot: 3 Switches: 8 Local Slot: 3
Config Slot: 3

Slot 1: State SLAVE
Status : Enabled Master : No MAC : 00:04:96:1F:88:21
Binding : Active Cpu Pri : 0 Platform : Summit300-24
Stacking Ports: 2
  Port-1 *1:25
  Port-2 *1:26

Slot 2: State SLAVE
Status : Enabled Master : No MAC : 00:04:96:1F:88:29
Binding : Active Cpu Pri : 0 Platform : Summit300-24
Stacking Ports: 2
  Port-1 *2:25
  Port-2 *2:26

Slot 3: State MASTER
Status : Enabled Master : Yes MAC : 00:04:96:18:41:2D
Binding : Active Cpu Pri : 0 Platform : Summit300-24
Stacking Ports: 1
  Port-1 *3:25

Slot 4: State SLAVE
Status : Enabled Master : No MAC : 00:04:96:1F:88:B0
Binding : Active Cpu Pri : 0 Platform : Summit300-24
Stacking Ports: 2
  Port-1 *4:25
  Port-2 *4:26

Slot 5: State SLAVE
Status : Enabled Master : No MAC : 00:04:96:1F:89:D9
Binding : Active Cpu Pri : 0 Platform : Summit300-24
Stacking Ports: 2
  Port-1 *5:25
  Port-2 *5:26

Slot 6: State SLAVE
Status : Enabled Master : No MAC : 00:04:96:1F:89:E8
Binding : Active Cpu Pri : 0 Platform : Summit300-24
Stacking Ports: 2
  Port-1 *6:25
  Port-2 *6:26
```

Platform
Indicates the platform type.

Stacking Ports
Indicates the stacking ports configured for the switch. An asterisk "*" indicates that the port is enabled (not link status) and an exclamation point "!" indicates that the port is disabled for stacking.
Slot 7: State SLAVE
  Status : Enabled  Master : No  MAC : 00:04:96:1F:89:E3
  Binding : Active  Cpu Pri : 0  Platform : Summit300-24
  Stacking Ports: 2
    Port-1   *7:25
    Port-2   *7:26

Slot 8: State SLAVE
  Status : Enabled  Master : No  MAC : 00:04:96:1F:88:05
  Binding : Active  Cpu Pri : 0  Platform : Summit300-24
  Stacking Ports: 1
    Port-1   *8:25

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
show stacking port

    show stacking port <stacking-port-no> [stats | rxerror | txerror | utilization | packets]

Description
Displays statistics about the stacking port on the current switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>stacking-port-no</td>
<td>Specifies the stacking port number of the current switch. For a list of stacking port numbers by switch model, see Table 27 on page 1396.</td>
</tr>
<tr>
<td>stats</td>
<td>Specifies to display port statistics for the stacking port.</td>
</tr>
<tr>
<td>rxerror</td>
<td>Specifies to display real-time receive error statistics.</td>
</tr>
<tr>
<td>txerrors</td>
<td>Specifies to display real-time transmission error statistics.</td>
</tr>
<tr>
<td>utilization</td>
<td>Specifies to display port utilization.</td>
</tr>
<tr>
<td>packets</td>
<td>Specifies to display a histogram of packet statistics.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If only a stacking port is specified, the switch displays all the information available for the port.

Example
The following example displays port utilization statistics for a Summit 400-48t:

```
show stacking port 53 utilization
```

The output of the command is similar to:

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
unconfigure stacking fallback-ip-address

unconfigure stacking fallback-ip-address  [slot <slotnumber>]

Description
Removes the fall-back IP address that was configured for the switch in the given slot or for the local switch.

Syntax Description

| slotnumber   | The number of the switch to unconfigure. |

Default
NA

Usage Guidelines
Use this command to remove the fall-back IP address configured for the given slot. If the slot number is not given, the fall-back IP address is un-configured for the local switch.

Example
unconfigure stacking fallback-ip-address ipaddress 10.12.123.1 255.255.255.0 slot 5

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
unconfigure stacking requested-slot

unconfigure stacking requested-slot [current-slot <slot number>]

Description
Removes previous configurations for a specific slot number in the stack.

Syntax Description

| current-slot <slot number> | Specifies the member’s slot ID that is applicable for this request. If this option is not given, the command applies to the member on which it is run. |

Default
The current slot (switch).

Usage Guidelines
Use this command to remove a particular slot number assignment for a stack member. The configuration marks the slot ID as invalid. The next time the member joins the stack the stack manager assigns a new slot number.

Example
The following command removes previous requests for a specific slot ID:

unconfigure stacking requested-slot current-slot 5

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is only available on the Summit 200, Summit 300-24, and Summit 400 switches.
This chapter describes commands for configuring and monitoring Ethernet Automatic Protection Switching (EAPS).

To use EAPS, you must enable EDP on the switch and the EAPS ring ports.

The EAPS protocol provides fast protection switching to layer 2 switches interconnected in an Ethernet ring topology, such as a metropolitan area network (MAN) or large campuses. EAPS protection switching is similar to what can be achieved with the Spanning Tree Protocol (STP), but offers the advantage of converging in less than a second when a link in the ring breaks.

To take advantage of the Spatial Reuse technology and broaden the use of the ring’s bandwidth, EAPS supports multiple EAPS domains running on the ring at the same time.

EAPS operates by declaring an EAPS domain on a single ring. Any VLAN that warrants fault protection is configured on all ring ports in the ring, and is then assigned to an EAPS domain. On that ring domain, one switch, or node, is designated the master node, while all other nodes are designated as transit nodes.

One port of the master node is designated the master node’s primary port (P) to the ring; another port is designated as the master node’s secondary port (S) to the ring. In normal operation, the master node blocks the secondary port for all non-control traffic belonging to this EAPS domain. If the master node detects a break in the ring, it unblocks its secondary port and allows data traffic to be transmitted and received through it.

EAPS fault detection on a ring is based on a single control VLAN per EAPS domain. This EAPS domain provides protection to one or more data-carrying VLANs called protected VLANs. The control VLAN is used only to send and receive EAPS messages; the protected VLANs carry the actual data traffic. As long as the ring is complete, the EAPS master node blocks the protected VLANs from accessing its secondary port.

A master node detects a ring fault in any of three ways:

- “Link down” message sent by a transit node on the control VLAN
- Ring port down event from lower hardware layers
- Failed response to a periodic health-check packet on the control VLAN

When the master node detects a failure, it declares a “failed” state and opens its logically blocked secondary port on all the protected VLANs. The master node also flushes its forwarding database (FDB) and sends a message on the control VLAN to all of its associated transit nodes to flush their forwarding databases.
configure eaps add control vlan

configure eaps <name> add control vlan <vlan_name>

Description
Adds the specified control VLAN to the specified EAPS domain.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_name</td>
<td>Specifies the name of the control VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
You must configure one control VLAN for each EAPS domain. The control VLAN is used only to send and receive EAPS messages.

The VLAN that will act as the control VLAN must be configured as follows:

- The VLAN must NOT be assigned an IP address, to avoid loops in the network.
- Only ring ports may be added as members of the control VLAN.
- The ring ports of the control VLAN must be tagged. This ensures that EAPS control VLAN traffic is serviced before any other traffic and that control VLAN messages reach their intended destinations.
- The control VLAN must be assigned a QoS profile of QP8 with the QoS profile priority setting HighHi.

A control VLAN cannot belong to more than one EAPS domain.

Example
The following command adds the control VLAN “keys” to the EAPS domain “eaps_1.”

configure eaps eaps_1 add control vlan keys

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure eaps add protect vlan

configure eaps <name> add protect vlan <vlan_name>

Description
Adds the specified protected VLAN to the specified EAPS domain.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_name</td>
<td>Specifies the name of the protected VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
You must configure one or more protected VLANs for each EAPS domain. The protected VLANs are the data-carrying VLANs.

When you configure the VLAN that will act as a protected VLAN, the ring ports of the protected VLAN must be tagged (except in the case of the default VLAN). As long as the ring is complete, the master node blocks the protected VLANs on its secondary port.

Example
The following command adds the protected VLAN “orchid” to the EAPS domain “eaps_1”:
configure eaps eaps_1 add protect vlan orchid

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure eaps delete control vlan

configure eaps <name> delete control vlan <vlan_name>

Description
Deletes the specified control VLAN from the specified EAPS domain.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan_name</td>
<td>Specifies the name of the control VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command deletes the control VLAN “keys” from the EAPS domain “eaps_1”:

configure eaps eaps_1 delete control vlan keys

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure eaps delete protect vlan

    configure eaps <name> delete protect vlan <vlan_name>

**Description**
Deletes the specified protected VLAN from the specified EAPS domain.

**Syntax Description**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of an EAPS domain.</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Specifies the name of the protected VLAN.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command deletes the protected VLAN “orchid” from the EAPS domain “eaps_1”:
configure eaps eaps_1 delete protect vlan orchid

**History**
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure eaps failtime

configure eaps <name> failtime [<seconds>]

Description
Configures the value of the failtimer the master node uses for EAPS health-check packets.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds the master node waits to receive a health-check packet before the failtimer expires. Default is 3 seconds.</td>
</tr>
</tbody>
</table>

Default
The default is three seconds.

Usage Guidelines
Use the failtime keyword and its associated seconds parameter to specify the amount of time the master node waits before the failtimer expires. The seconds parameter must be set greater than the configured value for hellotime. The default value is three seconds.

Increasing the failtime value provides more protection by waiting longer to receive a health-check packet when the network is congested.

NOTE
In previous versions of ExtremeWare, the secondary port on the Master node would open when the failtimer expired. In ExtremeWare 7.1 the default behavior has been modified to not open the secondary port. You can configure the action taken when the failtimer expires by using the configure eaps failtime expiry-action command.

Example
The following command configures the failtimer value for the EAPS domain “eaps_1” to 15 seconds:

configure eaps eaps_1 failtime 15

History
This command was first available in ExtremeWare 6.2.

The behavior for this command was modified in ExtremeWare 7.1 to follow the parameters configured in configure eaps failtime expiry-action.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure eaps failtime expiry-action

configure eaps <name> failtime expiry-action [ open-secondary-port | send-alert]

Description
Configures the action taken when the failtimer expires.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of an EAPS domain.</td>
</tr>
<tr>
<td>open-secondary-port</td>
<td>Specifies to open the secondary port when the failtimer expires.</td>
</tr>
<tr>
<td>send-alert</td>
<td>Specifies that a critical message is sent to the syslog when the failtimer expires.</td>
</tr>
</tbody>
</table>

Default
Default is send-alert.

Usage Guidelines
In earlier releases of ExtremeWare, when the failtimer of a master node expired, the default action was to open the secondary port. If the master node loses three Hello-PDUs in a row, the failtimer will expire, but there might not necessarily be a break in the ring. Opening the secondary port in this situation would create a loop.

The configure eaps failtime expiry-action command allows you to configure the action taken when the failtimer expires.

By default the action is to send an alert if the failtimer expires. Instead of going into a “Failed” state, the master node remains in a “Complete” or “Init” state, maintains the secondary port blocking, and writes a critical error message to syslog warning the user that there is a fault in the ring. An SNMP trap is also sent.

To use the failtimer expiry action of earlier releases, use the open-secondary-port parameter.

**NOTE**
You must explicitly configure the failtimer expiry action to open-secondary-port if the EAPS ring includes a section composed of non-EAPS devices.

**NOTE**
If you have a previous release of ExtremeWare and are upgrading to ExtremeWare 7.1, or later, the failtimer expiry action will default to send-alert.
**Example**
The following command configures the failtimer expiry-action for EAPS domain “eaps_1”:
```
configure eaps eaps_1 failtime expiry-action open-secondary-port
```

**History**
This command was first available in ExtremeWare 7.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure eaps fast-convergence

configure eaps fast-convergence [on | off]

Description
Enables EAPS to converge more quickly.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Turns fast-convergence on.</td>
</tr>
<tr>
<td>off</td>
<td>Turns fast-convergence off.  Default is off.</td>
</tr>
</tbody>
</table>

Default
Default is off.

Usage Guidelines
In certain environments to keep packet loss to a minimum, configure EAPS with fast-convergence turned on. If fast convergence is turned on, it will be displayed under the show eaps command. For example:

```
ALP_2_22:2 # show eaps
EAPS Enabled: Yes
EAPS Fast-Convergence: On
Number of EAPS instances: 2
EAPSD-Bridge links: 4
```

NOTE
If fast-convergence is turned on, the link-filters on all EAPS ring-ports are turned off. This could result in a problem if the port's hardware had a problem and started “flapping” between link-up/link-down states.

Example
The following command configures fast convergence for EAPS domain “eaps_1”:

```
configure eaps eaps_1 fast-convergence on
```

History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is only available on the “i” series platforms. This command is not supported on mini-GBICs on the Summit 48si.
configure eaps hellotime

configure eaps <name> hellotime <seconds>

Description
Configures the value of the hello timer the master node used for the EAPS health-check packet.

Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of an EAPS domain.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the number of seconds to wait between transmission of the health-check packets on the control VLAN. Must be greater than 0.</td>
</tr>
</tbody>
</table>

Default
Default is 1 second.

Usage Guidelines

Use the hellotime keyword and its associated seconds parameter to specify the amount of time the master node waits between transmissions of health-check packets on the control VLAN. Increasing the hellotime value keeps the processor from sending and processing too many health-check packets. Increasing the hellotime value should not affect the network convergence time, because transit nodes are already sending “link down” notifications.

This command applies only to the master node. If you configure the polling timers for a transit node, they will be ignored. If you later reconfigure that transit node as the master node, the polling timer values will be used as the current values.

Example

The following command configures the hellotime value for the EAPS domain “eaps_1” to 2 seconds:

configure eaps eaps_1 hellotime 2

History

This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
configure eaps mode

configure eaps <name> mode [master | transit]

Description
Configures the switch as either the EAPS master node or as an EAPS transit node for the specified domain.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>Specifies that this switch should be the master node for the named EAPS domain.</td>
</tr>
<tr>
<td>transit</td>
<td>Specifies that this switch should be the transit node for the named EAPS domain.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command identifies this switch as the master node for the domain named eaps_1:
configure eaps eaps_1 mode master

The following command identifies this switch as a transit node for the domain named eaps_1:
configure eaps eaps_1 mode transit

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure eaps name

    configure eaps <old_name> name <new_name>

Description
Renames an existing EAPS domain.

Syntax Description

<table>
<thead>
<tr>
<th>old_name</th>
<th>Specifies the current name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>new_name</td>
<td>Specifies a new name for the EAPS domain.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command renames EAPS domain “eaps-1” to “eaps-5”:

    configure eaps eaps-1 name eaps-5

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure eaps port

configure eaps <name> [primary | secondary] port <port number>

Description
Configures a node port as the primary or secondary port for the specified EAPS domain.

Syntax Description

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of an EAPS domain.</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies that the port is to be configured as the primary port.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies that the port is to be configured as the secondary port.</td>
</tr>
<tr>
<td>port number</td>
<td>Specifies the port number.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Each node on the ring connects through two ring ports. One port must be configured as the primary port; the other must be configured as the secondary port.

Example
The following command adds port 1 of the module installed in slot 8 of a BlackDiamond switch to the EAPS domain “eaps_1” as the primary port:

```
configure eaps eaps_1 primary port 8:1
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure eaps shared-port link-id

configure eaps shared-port <port> link-id <id>

Description
Configures the link ID of the shared port.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Specifies the port number of the common link port.</td>
</tr>
<tr>
<td>id</td>
<td>Specifies the link ID of the port.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Each common link in the EAPS network must have a unique link ID. The controller and partner shared ports belonging to the same common link must have matching link IDs. No other instance in the network should have that link ID.

Example
The following command configures the EAPS shared port 1:1 to have a link ID of 1.

```
configure eaps shared-port 1:1 link-id 1
```

History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is available on the “i” series of switches.
configure eaps shared-port mode

    configure eaps shared-port <port> mode <controller | partner>

Description
Configures the mode of the shared port.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>port</td>
<td>Specifies the port number of the shared port.</td>
</tr>
<tr>
<td>controller</td>
<td>Specifies the controller mode. The controller is the end of the common link</td>
</tr>
<tr>
<td></td>
<td>responsible for blocking ports when the common link fails thereby preventing</td>
</tr>
<tr>
<td></td>
<td>the superloop.</td>
</tr>
<tr>
<td>partner</td>
<td>Specifies partner mode.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The shared port on one end of the common link must be configured to be the controller. This is the end responsible for blocking ports when the common link fails thereby preventing the superloop.

The shared port on the other end of the common link must be configured to be the partner. This end does not participate in any form of blocking. It is responsible for only sending and receiving health-check messages.

Example
The following command configures the shared port 1:1 to be the controller.

```shell
configure eaps shared-port 1:1 mode controller
```

History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is available on the “i” series of switches.
create eaps

    create eaps <name>

Description
Creates an EAPS domain with the specified name.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain to be created. May be up to 32 characters in length.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
The name parameter is a character string of up to 32 characters that identifies the EAPS domain to be created. EAPS domain names and VLAN names must be unique: Do not use the same name string to identify both an EAPS domain and a VLAN.

On “e” Series of Switches. Only four EAPS domains per switch are supported and these domains must share a common ring port.

Example
The following command creates EAPS domain eaps_1:
create eaps eaps_1

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
create eaps shared-port

    create eaps shared-port <port>

**Description**

Creates an EAPS shared port on the switch.

**Syntax Description**

| port | Specifies the port number of the common link port. |

**Default**

N/A.

**Usage Guidelines**

To configure a common link, you must create a shared port on each switch of the common link.

**Example**

The following command creates a shared port on the EAPS domain.

```bash
create eaps shared-port 1:2
```

**History**

This command was first available in ExtremeWare 7.1.

**Platform Availability**

This command is available on the “i” series of switches.
delete eaps

    delete eaps <name>

Description
Deletes the EAPS domain with the specified name.

Syntax Description

| name | Specifies the name of an EAPS domain to be deleted. |

Default
N/A.

Usage Guidelines
An EAPS domain must be disabled first before it can be deleted. (See the `disable eaps {<name>}` command.)

Example
The following command deletes EAPS domain eaps_1:

```
delete eaps eaps-1
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
delete eaps shared-port

dele eaps shared-port <port>

**Description**
Deletes an EAPS shared port on a switch.

**Syntax Description**

| port | Specifies the port number of the Common Link port. |

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command deletes shared port 1:1.
```
delete eaps shared-port 1:1
```

**History**
This command was first available in ExtremeWare 7.1.

**Platform Availability**
This command is available on the “i” series of switches.
disable eaps

disable eaps {<name>}

Description
Disables the EAPS function for a named domain or for an entire switch.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
</table>

Default
Disabled for the entire switch.

Usage Guidelines
If you disable EAPS for the switch it automatically disables all EAPS domains.

Example
The following command disables the EAPS function for entire switch:

disable eaps

The following command disables the EAPS function for the domain “eaps-1”:

disable eaps eaps-1

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable eaps

    enable eaps {<name>}

Description
Enables the EAPS function for a named domain or for an entire switch.

Syntax Description

| name                | Specifies the name of an EAPS domain. |

Default
Disabled.
Default command enables for the entire switch.

Usage Guidelines
EDP must be enabled on the switch and EAPS ring ports.

EAPS must be enabled on the switch before you can enable it for a domain. If you enable EAPS on the switch after you’ve created and configured domains, you must still enable the domains individually.

Example
The following command enables the EAPS function for entire switch:

    enable eaps

The following command disables the EAPS function for the domain “eaps-1”:

    enable eaps eaps-1

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show eaps

    show eaps {<name>} {detail}

Description
Displays EAPS status information.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the name of an EAPS domain.</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies all available detail for each domain.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If you enter the `show eaps` command without a keyword, the command displays less than with the `detail` keyword.

Use the optional domain name parameter to display status information for a specific EAPS domain.

The output displayed by this command depends on whether the node is a transit node or a master node. The display for a transit node contains information fields that are not shown for a master node. Also, some state values are different on a transit node than on a master node.

The fields displayed are as follows:

- **EAPS Enabled:** Current state of EAPS on this switch:
  - Yes—EAPS is enabled on the switch.
  - No—EAPS is not enabled.
- **EAPS Fast Convergence:** Displays only when Fast Convergence is on.
- **Number of EAPS instances:** Number of EAPS domains created. The maximum number of EAPS domains per switch is 64.
- **EAPSD-Bridge links:** The total number of EAPS bridge links in the system. The maximum count is 8192 on "i" series switches and 4096 on "e" series switches. Each time a VLAN is added to EAPS, this count increments by 1.
- **Name:** The configured name for this EAPS domain.
- **(instance= )** The instance number is created internally by the system.
## State:

On a transit node, the command displays one of the following states:

- **Idle**—The EAPS domain has been enabled, but the configuration is not complete.
- **Links-Up**—This EAPS domain is running, and both its ports are up and in the FORWARDING state.
- **Links-Down**—This EAPS domain is running, but one or both of its ports are down.
- **Preforwarding**—This EAPS domain is running, and both of its ports are up, but one of them is in a temporary BLOCKED state.

On a master node, the command displays one of the following states:

- **Idle**—The EAPS domain has been enabled, but the configuration is not complete.
- **Init**—The EAPS domain has started but has not yet determined the status of the ring. The secondary port is in a BLOCKED state.
- **Complete**—The ring is in the COMPLETE state for this EAPS domain.
- **Failed**—There is a break in the ring for this EAPS domain.
- **[Failtimer Expired]**—When the failtimer expires and it's action is set to send-alert, this flag is set. This flag indicates there is a misconfiguration or hardware problem in the EAPS ring. The EAPS master node will continue to remain in COMPLETE or INIT state with it's secondary port blocking.

### [Running: …]

- **Yes**—This EAPS domain is running.
- **No**—This EAPS domain is not running.

### Enabled:

Indicates whether EAPS is enabled on this domain.

- **Y**—EAPS is enabled on this domain.
- **N**—EAPS is not enabled.

### Mode:

The configured EAPS mode for this switch: transit (T) or master (M).

### Primary/Secondary port:

The port numbers assigned as the EAPS primary and secondary ports. On the master node, the port distinction indicates which port is blocked to avoid a loop.

### Port status:

- **Unknown**—This EAPS domain is not running, so the port status has not yet been determined.
- **Up**—The port is up and is forwarding data.
- **Down**—The port is down.
- **Blocked**—The port is up, but data is blocked from being forwarded.

### Tag status:

Tagged status of the control VLAN:

- **Tagged**—The control VLAN has this port assigned to it, and the port is tagged in the VLAN.
- **Untagged**—The control VLAN has this port assigned to it, but the port is untagged in the control VLAN.
- **Undetermined**—Either a VLAN has not been added as the control VLAN to this EAPS domain or this port has not been added to the control VLAN.

### Hello Timer interval:

The configured value of the timer in seconds, specifying the time that the master node waits between transmissions of health check packets.

### Fail Timer interval:

The configured value of the timer in seconds, specifying the time that the master node waits before the failtimer expires.
The following command displays detailed EAPS information for domain “eaps1”:

```
show eaps eaps1 detail
```

The results for domain “eaps1” on a master node are shown as follows:

```
Name: "eaps1" (instance=0)
State: Complete        [Running: Yes]
Enabled: Yes    Mode: Master
Primary port: 10          Port status: Up        Tag status: Tagged
Secondary port: 20            Port status: Blocked   Tag status: Tagged
Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
Fail timer expiry action: Send alert
EAPS Domain has ... Controller Vlans:
Vlan Name            VID             QosProfile
"cvlan"              0100            QP8
EAPS Domain has ... Protected Vlans:
Vlan Name            VID             QosProfile
"pvlan"              0200            QP1
Number of Protected Vlans: 1
```

The following command displays detailed EAPS information:

```
show eaps detail
```

The results for a transit node are shown as follows:

```
EAPS Enabled: Yes
Number of EAPS instances: 1
EAPSD-Bridge links: 2
Name: "eaps1" (instance=0)
State: Links-Up          [Running: Yes]
Enabled: Yes    Mode: Transit
Primary port: 13          Port status: Up        Tag status: Tagged
```
show eaps

Secondary port: 14        Port status: Up        Tag status: Tagged
Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
Preforwarding Timer interval: 3 sec
Last update: From Master Id 00:01:30:B9:4B:E0, at Tue May 6 12:49:25 2003
Eaps Domain has following Controller Vlan:
  Vlan Name       VID     QosProfile
    "rhsc"       0020     QP8
EAPS Domain has following Protected Vlan(s):
  Vlan Name       VID
    "traffic"     1001
Number of Protected Vlans: 1

The following command displays EAPS information:
show eaps eaps2

The results for a transit node are shown as follows:

  Name: "eaps2" (instance=1)
  State: Link-Down       [Running: Yes]
  Enabled: Yes    Mode: Transit
  Primary port: 3           Port status: Down      Tag status: Tagged
  Secondary port: 2         Port status: Up        Tag status: Tagged
Hello Timer interval: 1 sec     Fail Timer interval: 3 sec
Preforwarding Timer interval: 6 sec
Last update: From Master Id 00:01:30:B9:4B:E0, at Tue May 6 12:49:25 2003
EAPS Domain has following Controller Vlan:
  Vlan Name       VID     QosProfile
    "cv2"       4002     QP8
Number of Protected Vlans: 2

The following command displays summary EAPS information:
show eaps summary

The results for this command are as follows:

EAPS Enabled: Yes
Number of EAPS instances: 1
EAPSD-Bridge links: 2

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Pri Mo</th>
<th>Pri En</th>
<th>Sec Port</th>
<th>Sec Port</th>
<th>Control-Vlan (VID)</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>eaps1</td>
<td>Complete</td>
<td>M</td>
<td>Y</td>
<td>1</td>
<td>2</td>
<td>cv1</td>
<td>1</td>
</tr>
</tbody>
</table>

History

This command was first available in ExtremeWare 6.2.

The summary option was added in ExtremeWare 6.2.2.

This command was modified in ExtremeWare 7.1 to display primary and secondary ring-ports and show the status of the failtimer.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
show eaps shared-port

    show eaps shared-port [detail]

Description
Displays shared-port information for one or more EAPS domains.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the status of all segments and VLANs.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If you enter the `show eaps shared-port` command without an argument or keyword, the command displays a summary of status information for all configured EAPS shared ports. You can use the `detail` keyword to display more detailed status information about the segments and VLANs associated with each shared port.

The fields displayed are as follows:

Example
The following command displays shared-port statistics on “eaps2”, “eaps3”, and “eaps4”: The EAPS domain is in a “ready” state in this example:

```
show eaps shared-port
```

The results for this command are as follows:

```
BD_3_42:7 # show eaps shared-port
EAPS shared-port count: 1

Shared-port Mode Link Domain Vlan RB RB
---------- ---------- ---- ------ ---- ----
1:1 Controller 2 Y Ready 3 1 Yes None None

EAPS Domain list: "eaps2" "eaps3" "eaps4"
```

History
This command was first available in ExtremeWare 7.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
EAPS Commands

Platform Availability
This command is available on all platforms.
show eaps summary

Description
Displays summary information on one or more EAPS domains.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Displays EAPS domains and associated info such as Domain Name, Domain State, EAPS Mode, Enabled State, Control VLAN and VLAN ID and the Number of Protect VLANs in the domain. This is helpful when viewing the status info for large numbers of EAPS domains quickly.

Example
The following command displays summary EAPS information on a transit node:

show eaps summary

The results for this command are as follows:
EAPS Enabled: Yes
Number of EAPS instances: 3
EAPSD-Bridge links: 6

<table>
<thead>
<tr>
<th>Domain</th>
<th>State</th>
<th>Pri</th>
<th>Sec</th>
<th>Port</th>
<th>Port</th>
<th>Control-Vlan (VID)</th>
<th>count</th>
</tr>
</thead>
<tbody>
<tr>
<td>eaps4</td>
<td>Links-Up</td>
<td>T</td>
<td>Y</td>
<td>1:1</td>
<td>1:4</td>
<td>cv4</td>
<td>(1004)</td>
</tr>
<tr>
<td>eaps3</td>
<td>Links-Up</td>
<td>T</td>
<td>Y</td>
<td>1:1</td>
<td>1:3</td>
<td>cv3</td>
<td>(1003)</td>
</tr>
<tr>
<td>eaps2</td>
<td>Links-Up</td>
<td>T</td>
<td>Y</td>
<td>1:1</td>
<td>1:2</td>
<td>cv2</td>
<td>(1002)</td>
</tr>
</tbody>
</table>

EAPS shared-port count: 1

<table>
<thead>
<tr>
<th>Shared-port</th>
<th>Mode</th>
<th>Link</th>
<th>Domain Vlan</th>
<th>RB</th>
<th>RB</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>Controller</td>
<td>2</td>
<td>Y</td>
<td>Ready</td>
<td>3</td>
</tr>
</tbody>
</table>

EAPS Domain list: "eaps2" "eaps3" "eaps4"
History
This command was first available in ExtremeWare 6.2.
The summary option was added in ExtremeWare 6.2.2.
This command was modified in ExtremeWare 7.1 to show shared-port statistics.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
unconfigure eaps port

unconfigure eaps <name> [primary | secondary] port

**Description**
Sets the specified port’s internal configuration state to INVALID.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies the name of an EAPS domain.</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies that the primary port should be unconfigured.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies that the secondary port should be unconfigured.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Unconfiguring an EAPS port sets its internal configuration state to INVALID, which causes the port to appear in the Idle state with a port status of Unknown when you use the `show eaps detail` command to display the status information about the port.

**Example**
The following command unconfigures this node’s EAPS primary ring port on the domain eaps_1:
```
unconfig eaps eaps_1 primary port
```

**History**
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
unconfigure eaps shared-port link-id

unconfigure eaps shared-port <port> link-id

**Description**
Unconfigures an EAPS link ID on a shared port on the switch.

**Syntax Description**

| port | Specifies the port number of the Common Link port. |

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command unconfigures the link ID on shared port 1:1.

unconfigure eaps shared-port 1:1 link-id

**History**
This command was first available in ExtremeWare 7.1.

**Platform Availability**
This command is available on the “i” series of switches.
unconfigure eaps shared-port mode

unconfigure eaps shared-port <port> mode

Description
Unconfigures the EAPS shared port mode.

Syntax Description

| Port | Specifies the port number of the Common Link port. |

Default
N/A.

Usage Guidelines
None.

Example
The following command unconfigures the shared port mode on port 1:1.
unconfigure eaps shared-port 1:1 mode

History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is available on the “i” series of switches.
This chapter describes commands related to:

- Creating, configuring, enabling, and disabling Spanning Tree Protocol (STP) on the switch
- Enabling and disabling Rapid Spanning Tree Protocol (RSTP) on the switch
- Displaying and resetting STP settings on the switch

The Spanning Tree Protocol (STP) is a bridge-based mechanism for providing fault tolerance on networks. STP is a part of the 802.1d bridge specification defined by the IEEE Computer Society. To explain STP in terms used by the 802.1d specification, the switch will be referred to as a bridge.

STP allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational.
- A redundant path is enabled if the main path fails.

The Rapid Spanning Tree Protocol (RSTP; 802.1w) provides an enhanced spanning tree algorithm that improves the convergence speed of bridged networks. RSTP takes advantage of point-to-point links in the network and actively confirms that a port can safely transition to the forwarding state without relying on any timer configurations. If a network topology change or failure occurs, RSTP rapidly recovers network connectivity by confirming the change locally before propagating that change to other devices across the network. For broadcast links, there is no difference in convergence time between STP and RSTP.

RSTP supersedes legacy STP protocols, supports the existing STP parameters and configurations, and allows for seamless interoperability with legacy STP.

**Spanning Tree Domains**

The switch can be partitioned into multiple virtual bridges. Each virtual bridge can run an independent Spanning Tree instance. Each Spanning Tree instance is called a *Spanning Tree Domain* (STPD). Each STPD has its own root bridge and active path. After an STPD is created, one or more VLANs can be assigned to it.

A port can belong to multiple STPDs. In addition, a VLAN can span multiple STPDs.

The key points to remember when configuring VLANs and STP are:

- Each VLAN forms an independent broadcast domain.
- STP blocks paths to create a loop-free environment.
When STP blocks a path, no data can be transmitted or received on the blocked port.

Within any given STPD, all VLANs belonging to it use the same spanning tree.

If you delete a STPD, the VLANs that were members of that STPD are also deleted. You must remove all VLANs associated with the STP before deleting the STPD.

**STPD Modes**

An STPD has two modes of operation:

- **802.1d mode**
  
  Use this mode for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1d. When configured in this mode, all rapid configuration mechanisms are disabled.

- **802.1w mode**
  
  Use this mode for compatibility with Rapid Spanning Tree (RSTP). When configured in this mode, all rapid configuration mechanisms are enabled. This mode is available for point-to-point links only. RSTP is enabled or disabled on a per STPD basis only. You do not enable RSTP on a per port basis.

By default, the following conditions exist:

- STPD operates in 802.1d mode.
- The default device configuration contains a single STPD called s0.
- The default VLAN is a member of STPD s0.

All STP parameters default to the IEEE 802.1d values, as appropriate.

**Port Modes**

An STP port has three modes of operation:

- **802.1d mode**
  
  This mode is used for backward compatibility with previous STP versions and for compatibility with third-party switches using IEEE standard 802.1d. BPDUs are sent untagged in 802.1d mode. Because of this, on any given physical interface there can be only one STPD running in 802.1d mode.

- **Extreme Multiple Instance Spanning Tree Protocol (EMISTP) mode**
  
  EMISTP mode is an extension of STP that allows a physical port to belong to multiple STPDs by assigning the port to multiple VLANs. EMISTP adds significant flexibility to STP network design. BPDUs are sent with an 802.1Q tag having an STPD instance Identifier (StpdID) in the VLANid field.

- **PVST+ mode**
  
  This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.

These port modes are for STP ports, not for physical ports. When a physical port belongs to multiple STPDs, it is associated with multiple STP ports. It is possible for the physical port to run in different modes for different domains to which it belongs.
configure stpd add vlan

configure stpd <spanning tree name> add vlan <vlan name> (ports <portlist> [dot1d | emistp | pvst-plus])

Description
Adds one or more VLANs, or a list of ports within a VLAN, to a specified STPD.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>ports</td>
<td>Specifies the port or ports to be included in the STPD. (6.2)</td>
</tr>
<tr>
<td>dot1d</td>
<td>Specifies the STP port mode of operation to be 802.1d. (6.2)</td>
</tr>
<tr>
<td>emistp</td>
<td>Specifies the STP port mode of operation to be EMISTP. (6.2)</td>
</tr>
<tr>
<td>pvst-plus</td>
<td>Specifies the STP port mode of operation to be PVST+. (6.2)</td>
</tr>
</tbody>
</table>

Default
For ExtremeWare 6.1 (or earlier), the default is N/A.
For ExtremeWare 6.2 (or later), all ports are in emistp mode, except those in STPD s0, whose default setting is dot1d mode.

Usage Guidelines
For version 6.2 or later, this command adds a list of ports within a VLAN to a specified STPD. If no ports are specified, the entire VLAN is added.
For versions up to 6.1, this command adds one or more VLANs to the STPD. All VLANs participating in the STPD elect a Root Bridge and create a loop-free, least-cost path to the bridge.
You must be careful to ensure that ports in overlapping domains do not interfere with the orderly working of each domain’s protocol.
You must create a VLAN to add a VLAN to the STPD. To create a VLAN, use the create vlan command.
You can create STP domains using the create stpd command.
Use the keywords dot1d, emistp, and pvst-plus to specify STP port modes in version 6.2 or later.
- **dot1d**—This mode is reserved for backward compatibility with previous STP versions. BPDUs are sent untagged in 802.1d mode. Because of this, on any given physical interface there can be only one STPD running in 802.1d mode. This mode supports the industry standard implementation, and can be used with non-Extreme devices.
- **emistp**—This mode sends BPDUs with an 802.1Q tag having an STPD instance Identifier (StpdID) in the VLANid field. This is an Extreme proprietary mode, and cannot be used with non-Extreme devices.
• **pvst-plus**—This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.

An StpdID is used to identify each STP domain. You assign the StpdID when configuring the domain. An StpdID must be identical to the VLANid of one of the member VLANs in that STP domain, and that VLAN cannot belong to another STPD.

---

**NOTE**

These port modes are for STP ports, not for physical ports. When a physical port belongs to multiple STPDs, it is associated with multiple STP ports. It is possible for the physical port to run in different modes for different domains for which it belongs.

When the switch boots, it automatically creates a VLAN named default with a tag value of 1, and STPD s0 with an StpdID of 1. The switch associates VLAN default to STPD s0. By default, all ports that belong to this VLAN and STPD are in 802.1d mode.

**Example**

Create a VLAN named marketing and an STPD named STPD1 as follows:

```console
create vlan marketing
create stpd stpd1
```

The following command adds the VLAN named marketing to the STPD STPD1:

```console
configure stpd stpd1 add vlan marketing
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2 to support STP port mode configurations.

This command was added to the Summit "e" series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support STP port mode configurations.

The default port mode also changed from dot1d to emistp in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure stpd delete vlan

configure stpd <spanning tree name> delete vlan <vlan name> {ports <portlist>}

**Description**

Deletes a VLAN from an STPD or one or more ports in the specified VLAN from an STPD. Deleting a VLAN from an STPD does not change the configuration. Only the ports that belong to the VLAN are also deleted from the STPD.

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>ports</td>
<td>Specifies the port or ports to be removed from the STPD.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

N/A

**Example**

The following command deletes a VLAN named Marketing from the STPD STPD1:

```
configure stpd stpd1 delete vlan marketing
```

**History**

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

The default mode was changed from dot1d to emistp in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure stpd forwarddelay

configure stpd <spanning tree name> forwarddelay <seconds>

Description
Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the switch is the Root Bridge.

Syntax Description

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the forward delay time in seconds.</td>
</tr>
</tbody>
</table>

Default
15 seconds

Usage Guidelines
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The range for the <seconds> parameter is 4 – 30 seconds.

Example
The following command sets the forward delay from STPD1 to 20 seconds:

```
configure stpd stpd1 forwarddelay 20
```

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure stpd hellotime

configure stpd <spanning tree name> hellotime <seconds>

Description
Specifies the time delay (in seconds) between transmissions of Bridge Protocol Data Units (BPDUs) from this STPD when it is the Root Bridge.

Syntax Description

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the hello time in seconds.</td>
</tr>
</tbody>
</table>

Default
2 seconds

Usage Guidelines
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The range for the <seconds> parameter is 1 – 10 seconds.

Example
The following command sets the time delay from STPD1 to 10 seconds:

```
configure stpd stpd1 hellotime 10
```

History
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure stpd maxage

configure stpd <spanning tree name> maxage <seconds>

Description
Specifies the maximum age of a BPDU in the specified STPD.

Syntax Description

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the maxage time in seconds.</td>
</tr>
</tbody>
</table>

Default
20 seconds

Usage Guidelines
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The range for the <seconds> parameter is 6 – 40 seconds.

Note that the time must be greater than or equal to 2 * (Hello Time + 1) and less than or equal to 2 * (Forward Delay –1).

Example
The following command sets the maximum age of STPD1 to 30 seconds:
configure stpd stpd1 maxage 30

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit "e" series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure stpd mode

configure stpd <spanning tree name> mode [dot1d | dot1w]

Description
Configures the operational mode for the specified STP domain.

Syntax Description

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1d</td>
<td>Specifies the STPD mode of operation to be 802.1d.</td>
</tr>
<tr>
<td>dot1w</td>
<td>Specifies the STPD mode of operation to be 802.1w, and rapid configuration is enabled.</td>
</tr>
</tbody>
</table>

Default
Operates in 802.1d mode.

Usage Guidelines
If you configure the STP domain in 802.1d mode, the rapid reconfiguration mechanism is disabled.

If you configure the STP domain in 802.1w mode, the rapid reconfiguration mechanism is enabled.

Example
The following command configures STPD s1 to enable the rapid reconfiguration mechanism and operate in 802.1w mode:

```
configure stpd s1 mode dot1w
```

History
This command was first available in ExtremeWare 7.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure stpd ports cost

configure stpd <spanning tree name> ports cost <cost> <portlist>

Description
Specifies the path cost of the port in the specified STPD.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a numerical port cost value. The range is 1 through 65,535.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*; 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
The switch automatically assigns a default path cost based on the speed of the port, as follows:

- For a 10Mbps port, the default cost is 100.
- For a 100Mbps port, the default cost is 19.
- For a 1000Mbps port, the default cost is 4.

Usage Guidelines
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The range for the cost parameter is 1 through 65,535. The switch automatically assigns a default path cost based on the speed of the port.

Example
The following command configures a cost of 100 to ports 1 through 5 in STPD s0 on a stand-alone switch:

configure stpd s0 ports cost 100 1-5

The following command configures a cost of 100 to slot 2, ports 1 through 5 in STPD s0 on a modular switch:

configure stpd s0 ports cost 100 2:1-2:5

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.
This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and 7.1e.

**Platform Availability**
This command is available on all platforms.
configure stpd ports link-type

configure stpd <spanning tree name> ports link-type [auto | edge | broadcast | point-to-point] <portlist>

Description
Configures the ports in the specified STPD as auto, edge, broadcast or point-to-point link types.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>auto</td>
<td>Specifies the switch to automatically determine the port link type. An auto link behaves like a point-to-point link if the link is in full duplex mode or if link aggregation is enabled on the port. Used for 802.1w configurations.</td>
</tr>
<tr>
<td>edge</td>
<td>Specifies a port that does not have a bridge attached. An edge port is placed and held in the STP forwarding state unless a BPDU is received by the port.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Specifies a port attached to a LAN segment with more than two bridges. Used for 802.1d configurations. A port with broadcast link type cannot participate in rapid reconfiguration. By default, all ports are broadcast links.</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Specifies a port attached to a LAN segment with only two bridges. A port with point-to-point link type can participate in rapid reconfiguration. Used for 802.1w configurations.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
All ports are broadcast link types.

Usage Guidelines
The default, broadcast links, supports legacy STP (802.1d) configurations.

If you configure a port to be an edge port, the port immediately enters the forwarding state. Edge ports remain in the forwarding state unless the port receives a BPDU.

RSTP does not send any BPDUs from an edge port, nor does it generate topology change events when an edge port changes its state.

RSTP rapidly moves the designated ports of a point-to-point link type into the forwarding state. This behavior is supported by RSTP only.

An auto link behaves like a point-to-point link if the link is in full-duplex mode or if link aggregation is enabled on the port; otherwise, an auto link behaves like a broadcast link. If a non-802.1w switch exists between several switches operating in 802.1w mode with auto links, the non-802.1w switch may negotiate full-duplex even though the broadcast domain extends over several STP devices. In this situation, an 802.1w port may advance to the “forwarding” state more quickly than desired.

If the switch operates in 802.1d mode, any configured port link type will behave the same as the broadcast link type.
Example

The following command configures ports 1 through 4 to be point-to-point links in STPD s1 on a stand-alone switch:

```
configure stpd s1 ports link-type point-to-point 1-4
```

The following command configures slot 2, ports 1 through 4 to be point-to-point links in STPD s1 on a modular switch:

```
configure stpd s1 ports link-type point-to-point 2:1-2:4
```

History

This command was first available in ExtremeWare 7.1.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
configure stpd ports link-type edge edge-safeguard disable

configure stpd <spanning tree name> ports link-type edge <portlist>
edge-safeguard disable

Description
Disables RSTP on the specified edge port for the specified STPD.

Syntax Description

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*; 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
By default this feature is disabled.

Usage Guidelines
This command applies only to ports that have already been configured edge ports.

Enabling RSTP on edge ports provides a loop detection mechanism (called “edge safeguard”) without preventing rapid network convergence of these ports. Edge ports with RSTP enter the forwarding state within four seconds.

To view the status of the edge safeguard feature, use the show stpd <spanning tree name> ports <portlist> (detail) command. The show stpd command displays information about the STPD configuration on the switch, including the enable/disable state for edge safeguard. To enable or re-enable edge safeguard, use the configure stpd <spanning tree name> ports link-type edge <portlist> edge-safeguard enable command.

Example
The following command disables RSTP on edge port 4 in STPD s1 on a stand-alone switch:
configure stpd s1 ports link-type edge 4 edge-safeguard disable

The following command disables RSTP on slot 2, port 1 in STPD s1 on a modular switch:
configure stpd s1 ports link-type edge 2:1 edge-safeguard disable

History
This command was first available in ExtremeWare 7.5.

Platform Availability
This command is available on all platforms.
configure stpd ports link-type edge edge-safeguard enable

configure stpd <spanning tree name> ports link-type edge <portlist> edge-safeguard enable

**Description**

Enables RSTP on the specified edge port for the specified STPD.

**Syntax Description**

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

**Default**

By default this feature is disabled.

**Usage Guidelines**

This command applies only to ports that have already been configured edge ports.

Enabling RSTP on edge ports provides a loop detection mechanism (called “edge safeguard”) without preventing rapid network convergence of these ports. Edge ports with RSTP enter the forwarding state within four seconds.

To view the status of the edge safeguard feature, use the `show stpd <spanning tree name> ports <portlist> {detail}` command. The `show stpd` command displays information about the STPD configuration on the switch, including the enable/disable state for edge safeguard. To disable edge safeguard, use the `configure stpd <spanning tree name> ports link-type edge <portlist> edge-safeguard disable` command.

**Example**

The following command enables RSTP on edge port 4 in STPD `s1` on a stand-alone switch:

`configure stpd s1 ports link-type edge 4 edge-safeguard enable`

The following command enables RSTP on slot 2, port 1 in STPD `s1` on a modular switch:

`configure stpd s1 ports link-type edge 2:1 edge-safeguard enable`

**History**

This command was first available in ExtremeWare 7.5.

**Platform Availability**

This command is available on all platforms.
configure stpd ports mode

configure stpd <spanning tree name> ports mode [dot1d | emistp | pvst-plus] <portlist>

Description
Configures the STP mode of operation for the specified port list.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>dot1d</td>
<td>Specifies IEEE 802.1d-compliant packet formatting. A physical port can only be a member of one STPD running it dot1d mode.</td>
</tr>
<tr>
<td>emistp</td>
<td>Specifies 802.1d formatting and 802.1q tagging.</td>
</tr>
<tr>
<td>pvst-plus</td>
<td>Specifies PVST+ packet formatting.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Ports in the default STPD (s0) are dot1d mode. Ports in user-created STPDs are in emistp mode.

Usage Guidelines
None.

Examples
The following command configures STPD s1 with PVST+ packet formatting for port 1 on a stand-alone switch:

```
configure stpd s1 ports mode pvst-plus 1
```

The following command configures STPD s1 with PVST+ packet formatting for slot 2, port 1 on a modular switch:

```
configure stpd s1 ports mode pvst-plus 2:1
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure stpd ports priority

configure stpd <spanning tree name> ports priority <priority> <portlist>

Description
Specifies the port priority of the port in the specified STPD.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a numerical port priority value.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2*, 2-5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
The default setting is 16.
For version 6.0 and later, the default setting is 16.
For version 2.0 and 4.0, the default setting is 128.

Usage Guidelines
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

By changing the priority of the port, you can make it more or less likely to become the root port or a designated port.

A setting of 0 (zero) indicates the highest priority.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, the <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

The range for the priority parameter is 0 through 31.
For version 6.0 and later:
• The range for the priority parameter is 0 through 31.
For version 2.0 and 4.0:
• The range for the priority parameter is 0 through 255.

Example
The following command assigns a priority of 1 to ports 1 through 5 in STPD s0 on a stand-alone switch:
configure stpd s0 ports priority 1 1-5
The following command assigns a priority of 1 to slot 2, ports 1 through 5 in STPD s0 on a modular switch:

```
configure stpd s0 ports priority 1 2:1-2:5
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular switches.

This command was modified in ExtremeWare 6.1 to update the *priority* parameter.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
configure stpd priority

configure stpd <spanning tree name> priority <priority>

**Description**
Specifies the bridge priority of the STPD.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the bridge priority of the STPD. The range is 0 – 65,535.</td>
</tr>
</tbody>
</table>

**Default**
The default priority is 32,768.

**Usage Guidelines**
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

By changing the priority of the STPD, you can make it more or less likely to become the root bridge.

The range for the priority parameter is 0 through 65,535. A setting of 0 indicates the highest priority.

**Example**
The following command sets the bridge priority of STPD1 to 16,384:

```
configure stpd stpd1 priority 16384
```

**History**
This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure stpd tag

configure stpd <spanning tree name> tag <vlan tag>

Description
Assigns an StpdID to an STPD.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>vlan tag</td>
<td>Specifies the VLANid of a VLAN that is owned by the STPD.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

An STPD identifier (StpdID) is used to identify each STP domain. You assign the StpdID when configuring the domain. An StpdID must be identical to the VLANid of one of the member VLANs in that STP domain, and that VLAN cannot belong to another STPD. Unless all ports are running in 802.1d mode, an STPD must be configured with an StpdID.

You must create and configure the VLAN, along with the tag, before you can configure the STPD tag. To create a VLAN, use the `create vlan` command. To configure the VLAN, use the `configure vlan` command.

In addition to the VLAN attributes that you will use in the STPD, you must first create an STPD. To create an STPD, use the `delete stpd` command.

Example
The following command assigns an StpdID to the STPD called purple_st:

```bash
configure stpd purple_st tag 200
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure vlan add ports stpd

configure vlan <vlan name> add ports [all | <portlist>] stpd <spanning tree name> {{dot1d | emistp | pvst-plus}}

**Description**

Adds a list of ports within a VLAN to a specified STPD.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all of the ports to be included in the STPD.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port or ports to be included in the STPD.</td>
</tr>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD name on the switch.</td>
</tr>
<tr>
<td>dot1d</td>
<td>Specifies the STP port mode of operation to be 802.1d.</td>
</tr>
<tr>
<td>emistp</td>
<td>Specifies the STP port mode of operation to be limited EMISTP.</td>
</tr>
<tr>
<td>pvst-plus</td>
<td>Specifies the STP port mode of operation to be limited PVST+.</td>
</tr>
</tbody>
</table>

**Default**

All ports are in *emistp* mode, except those in STPD s0, whose default setting is *dot1d* mode.

**Usage Guidelines**

This command performs the same function as the `configure stpd add vlan` command with the ports option included.

This command adds a list of ports within a VLAN to a specified STPD, and specifies one of the following modes for those ports.

- **dot1d**—In this mode, BPDUs are sent untagged in 802.1d mode. Because of this, on any given physical interface there can be only one STPD running in 802.1d mode. This mode supports the industry standard implementation, and can be used with non-Extreme devices. It can also be used for backward compatibility with previous STP versions.

- **emistp**—This mode sends BPDUs with an 802.1Q tag having an STPD instance identifier (StpdID) in the VLANid field. This is an Extreme proprietary mode, and cannot be used with non-Extreme devices.

- **pvst-plus**—This mode implements PVST+ in compatibility with third-party switches running this version of STP. The STPDs running in this mode have a one-to-one relationship with VLANs, and send and process packets in PVST+ format.
Example
The following command adds ports 2 and 3, members of a VLAN named Marketing, to the STPD named STPD1, and specifies that they be in EMISTP mode:

```
configure vlan marketing add ports 2-3 stpd stpd1 emistp
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
create stpd

    create stpd <name>

Description
Creates a user-defined STPD.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies a user-defined STPD name.</th>
</tr>
</thead>
</table>

Default
The default device configuration contains a single STPD called s0.

When an STPD is created, the STPD has the following default parameters:
- State—disabled
- StpdID—none
- Assigned VLANs—none
- Bridge priority—32,768
- Max age—20 seconds
- Hello time—2 seconds
- Forward delay—15 seconds
- Operational mode—802.1d
- Rapid Root Failover—disabled state
- Port mode—Ports in the default STPD (s0) are 802.1d mode. Ports in user-created STPDs are in emistp mode.

Usage Guidelines
Each STPD name must be unique, and cannot duplicate any other named elements on the switch (such as VLANs, QoS profiles, Access profiles, or route maps). If you are uncertain about the VLAN profile names on the switch, use the show vlan command to view the VLAN profiles. If you are uncertain about QoS profile names on the switch, use the show qosprofile command to view the QoS profiles.

Each STPD has its own Root Bridge and active path. After the STPD is created, one or more VLANs can be assigned to it.

Example
The following example creates an STPD named purple_st:

create stpd purple_st

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
delete stpd

delete stpd <spanning tree name>

Description
Removes a user-defined STPD from the switch.

Syntax Description

| spanning tree name | Specifies a user-defined STPD name on the switch. |

Default
N/A

Usage Guidelines
If you remove an STPD, the VLANs that were members of that STPD are also deleted. An STPD can only be removed if all VLANs have been deleted from it.

The default STPD, s0, cannot be deleted.

Example
The following command deletes an STPD named purple_st:

delete stpd purple_st

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ignore-bpdu vlan

    disable ignore-bpdu vlan <vlan name>

Description
Allows the switch to recognize STP BPDUs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
By default, STP processes all of the BPDUs received on a VLAN.

Use the enable ignore-bpdu vlan <vlan name> command to allow a BPDU to traverse a VLAN without being processed by STP, even if STP is enabled on the port. If you have a known topology and have switches outside of your network within your STPD, use this feature to keep the root bridge within your network.

Example
The following command disables the ignore-bpdu option on the VLAN accounting:

disable ignore-bpdu accounting

History
This command was first available in ExtremeWare 2.0.

Platform Availability
This command is available on the “i” series platforms only.
disable ignore-stp vlan

    disable ignore-stp vlan <vlan name>

Description
Allows a VLAN to use STP port information.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
The `vlan` keyword is optional. To configure the switch to ignore the STP protocol and not block traffic for the VLAN(s), see the following command: `enable ignore-stp vlan <vlan name>`.

Example
The following command disables the ignore-stp option on the VLAN `accounting`:

disable ignore-stp accounting

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable stpd

disable stpd {<spanning tree name>}

Description
Disables the Spanning Tree Protocol on a particular STPD or for all STPDs.

Syntax Description

| spanning tree name | Specifies an STPD name on the switch. |

Default
Disabled

Usage Guidelines
All VLANs belong to an STPD. If you do not want to run STP on a VLAN, you must add the VLAN to an STPD that is disabled.

The spanning tree name keyword is optional. You do not need to indicate an STPD name if you disable STP for all STPDs.

To enable or re-enable STP on a particular STPD or on all STPDs, use the enable stpd {<spanning tree name>} command.

Example
The following command disables an STPD named purple_st:

disable stpd purple_st

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable stpd ports

disable stpd <spanning tree name> {ports <portlist>|vlan <vlan name>}

Description
Disables STP on one or more ports for a given STPD.

Syntax Description

<table>
<thead>
<tr>
<th>spanning tree name</th>
<th>Specifies an STPD name on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Disabling STP on one or more ports puts those ports in forwarding state; all Bridge Protocol Data Units (BPDUs) received on those ports will be disregarded and dropped.

The portlist keyword is optional. You do not need to indicate a list of ports if you want to disable STP on all ports in the STPD.

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, the <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

You must create one or more STP domains, configure, and enable an STPD before you can use the disable stpd ports command.

To enable STP on one or more ports for a given STPD, use the enable stpd ports command.

Example
The following command disables port 4 on an STPD named Backbone_st on a stand-alone switch:

disable stpd backbone_st ports 4

The following command disables slot 2, port 4 on an STPD named Backbone_st on a modular switch:

disable stpd backbone_st ports 2:4

History
This command was first available in ExtremeWare 2.0.

This command was modified in ExtremeWare 4.0 to support modular devices.

This command was added to the Summit “e” series of switches ExtremeWare 6.2a and ExtremeWare 7.1e.
Platform Availability
This command is available on all platforms.
disable stpd rapid-root-failover

disable stpd <spanning tree name> rapid-root-failover

Description
Disables rapid root failover for STP recovery times.

Syntax Description

| spanning tree name | Specifies an STPD name on the switch. |

Default
Disabled

Usage Guidelines
This command is used if there is a link failure. The port that is in FORWARDING state moves to BLOCKING state, and it may take a long time to recover. If the port is a root port, it needs to recover quickly, and this command is used for that purpose.

To view the status of rapid root failover on the switch, use the show stpd command. The show stpd command displays information about the STPD configuration on the switch, including the enable/disable state for rapid root failover. To enable or re-enable rapid root failover for STP recovery times, use the enable stpd <spanning tree name> rapid-root-failover command.

Example
The following command disables rapid root fail over on STPD Backbone_st:

disable stpd backbone_st rapid-root-failover

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable ignore-bpdu vlan

   enable ignore-bpdu vlan <vlan name>

Description
Configures the switch to ignore the STP BPDUs, which prevents ports in the VLAN from becoming part of an STPD.

NOTE
This command is available only on the "i" series switches.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Use this command to allow a BPDU to traverse a VLAN without being processed by STP, even if STP is enabled on the port. If you have a known topology and have switches outside your network that are within your STPD, use this feature to keep the root bridge within your network.

Use the disable ignore-bpdu vlan <vlan name> command to allow the switch to recognize STP BPDUs.

Example
The following command configures the switch to ignore STP BPDUs on the VLAN accounting:

```
enable ignore-bpdu vlan accounting
```

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on the “i” series platforms only.
enable ignore-stp vlan

    enable ignore-stp vlan <vlan name>

Description
Configures the switch to ignore the STP protocol and not block traffic for the VLAN(s).

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
This command is useful when multiple VLANs share the same physical ports, but only some of the VLANs require STP protection.

To allow a VLAN to use STP port information, use the `disable ignore-stp vlan` command.

Example
The following command enables the ignore-stp option on the VLAN accounting:
```
enable ignore-stp accounting
```

History
This command was first available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable stpd

    enable stpd {<spanning tree name>}

**Description**

Enables the STP protocol for one or all STPDs.

**Syntax Description**

| spanning tree name | Specifies an STPD name on the switch. |

**Default**

Disabled

**Usage Guidelines**

You must create one or more STP domains and configure an STPD before you can use the enable stpd command. Use the create stpd command to create an STPD.

The spanning tree name keyword is optional. You do not need to indicate an STPD name if you enable the STP protocol for all STPDs.

To disable the STP protocol on a particular STPD or on all STPDs, use the disable stpd command.

The default port mode is emistp, which requires an StpdID. When using 802.1d mode, configure the mode of all the ports to dot1d before enabling the domain.

**Example**

The following command enables an STPD named Backbone_st:

```
enable stpd backbone_st
```

**History**

This command was first available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable stpd ports

    enable stpd <spanning tree name> {ports <portlist>|vlan <vlan name>}

**Description**

Enables the STP protocol on one or more ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

Enabled

**Usage Guidelines**

If STPD is enabled for a port, Bridge Protocol Data Units (BPDUs) will be generated on that port if STP is enabled for the associated STPD.

You must create and configure one or more STP domains before you can use the `enable stpd ports` command. Use the `delete stpd <name>` command to create an STP domain. If you have considerable knowledge and experience with STP, you can configure the STPD using the `configure stpd` commands. However, the default STP parameters are adequate for most networks.

On a modular switch, `<portlist>` can be a list of slots and ports. On a stand-alone switch, `<portlist>` can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

**Example**

The following command enables port 4 on an STPD named *Backbone_st* on a stand-alone switch:

```shell
enable stpd backbone_st ports 4
```

The following command enables slot 2, port 4 on an STPD named *Backbone_st* on a modular switch:

```shell
enable stpd backbone_st ports 2:4
```

**History**

This command was first available in ExtremeWare 2.0.

Support for modular switches was introduced in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
enable stpd rapid-root-failover

    enable stpd <spanning tree name> rapid-root-failover

**Description**
Enables rapid root failover for faster STP recovery times.

**Syntax Description**

| spanning tree name | Specifies an STPD name on the switch. |

**Default**
Disabled

**Usage Guidelines**
This command is used if there is a link failure. The port that is in FORWARDING state moves to BLOCKING state, and it may take a long time to recover. If the port is a root port, it needs to recover quickly, and this command is used for that purpose.

To view the status of rapid root failover on the switch, use the `show stpd` command. The `show stpd` command displays information about the STPD configuration on the switch including the enable/disable state for rapid root failover.

**Example**
The following command enables rapid root failover on the STPD called Backbone_st:
`enable stpd backbone_st rapid-root-failover`

**History**
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
show stpd

    show stpd {<spanning tree name> | detail}

Description
Displays STPD settings on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>spanning tree name</td>
<td>Specifies an STPD on the switch.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that STPD settings should be shown for each STPD.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is available only on the “i” series switches.</td>
</tr>
<tr>
<td>domain</td>
<td>Specifies an STPD on the switch. Supported on e platform switches.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The command displays the following STPD information:

- STPD name
- STPD state
- STPD mode of operation
- Rapid Root Failover
- Tag
- Ports
- Active VLANs
- Bridge Priority
- Bridge ID
- Designated root
- STPD configuration information

You can create, configure, and enable one or more STP domains and use the show stpd command to display STP configurations. Use the create stpd command to create an STP domain. Use the enable stpd command to enable an STPD. If you have considerable knowledge and experience with STP, you can configure the STPD using the configure stpd commands. However, the default STP parameters are adequate for most networks.

Examples
The following command displays STPD settings on an STPD named Backbone_st in an Alpine 3804 switch:

    show stpd backbone_st
The results for this command are as follows:

```
* Alpine3804:47 # show stpd Backbone_st
Stpd: Backbone_st Stp: ENABLED            Number of Ports: 0
Rapid Root Failover: Disabled
Operational Mode: 802.1W
802.1Q Tag: (none)
8:3,4:4
Active Vlans:  Default
Bridge Priority: 32768
BridgeID:               80:00:00:01:30:23:c1:00
Designated root:        80:00:00:01:30:23:c1:00
RootPathCost: 0         Root Port: ----
MaxAge: 20s             HelloTime: 2s           ForwardDelay: 15s
CfgrMaxAge: 20s         CfgBrHelloTime: 2s      CfgBrForwardDelay: 15s
Topology Change Time: 35s Hold time: 1s
Topology Change Detected: FALSE                 Topology Change: FALSE
Number of Topology Changes: 0
Time Since Last Topology Change: 5192295s
```

The following command displays STPD settings on an STPD named *Backbone_st* in a Summit 200 switch:

```
show stpd backbone_st
```

The results for this command are as follows:

```
* Summit200:47 # show stpd Backbone_st
Stpd: Backbone_st Stp: ENABLED            Number of Ports: 14
Rapid Root Failover: Disabled
Operational Mode: 802.1W
802.1Q Tag: (none)
8:3,4:4
Active Vlans:  Default
Bridge Priority: 32768
BridgeID:               80:00:00:01:30:23:c1:00
Designated root:        80:00:00:01:30:23:c1:00
RootPathCost: 0         Root Port: ----
MaxAge: 20s             HelloTime: 2s           ForwardDelay: 15s
CfgrMaxAge: 20s         CfgBrHelloTime: 2s      CfgBrForwardDelay: 15s
Topology Change Time: 35s Hold time: 1s
Topology Change Detected: FALSE                 Topology Change: FALSE
Number of Topology Changes: 1
Time Since Last Topology Change: 134s
```

**History**

This command was first available in ExtremeWare 2.0.

Support for the *detail* keyword was introduced in ExtremeWare 6.2.

Support for displaying RSTP data was introduced in ExtremeWare 7.1.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.
**Platform Availability**

This command is available on all platforms.
show stpd ports

    show stpd <spanning tree name> ports <portlist> {detail}

Description
Displays the STP state of a port.

Syntax Description

<table>
<thead>
<tr>
<th>spannning tree name</th>
<th>Specifies an STPD name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that STPD state information should be displayed for all ports, or for the ports in the port list.</td>
</tr>
</tbody>
</table>

NOTE: This option is available only on the “i” series switches.

| vlan name | Specifies a VLAN name. |

NOTE: This option is available only on the “e” series switches.

Default
N/A

Usage Guidelines
This command displays the following:

- STPD port configuration
- STPD port mode of operation
- STPD path cost
- STPD priority
- STPD state (root bridge, and so on)
- Port role (root port, edge port, and so on.)
- STPD port state (forwarding, blocking, and so on)
- Configured port link type
- Operational port link type
- Status of edge port safeguard (enabled or disabled)

On a modular switch, <portlist> can be a list of slots and ports. On a stand-alone switch, <portlist> can be one or more port numbers. For a detailed explanation of port specification, see “Modular Switch Numerical Ranges” or “Stand-alone Switch Numerical Ranges” in Chapter 1.

Examples
The following command displays the state of port 4 on an STPD named Backbone_st on a stand-alone switch:

```
show stpd Backbone_st ports 4
```
The following command displays the state of slot 3, ports 1 through 3 on an STPD named `s0` on a modular switch:

```
show stpd S0 ports 3:1-3:3
```

The results for this command are as follows:

```
* Alpine3804:4 # show stpd s0 ports 3:1-3:3
Port Mode   State     Cost   Flags Priority Port ID Designated Bridge
3:1  802.1D FORWARDING 100    e------- 16    16641   00:00:00:00:00:00:00:00
3:2  802.1D FORWARDING 100    e------- 16    16642   00:00:00:00:00:00:00:00
3:3  802.1D FORWARDING 100    e------- 16    16643   00:00:00:00:00:00:00:00

Total Ports: 14
```

The following command displays the state of port 20 on an STPD named `rstp_domain` on a standalone switch:

```
show stpd rstp_domain port 20 detail
```

The results for this command are as follows:

```
Partner STP version: Dot1w
Stpd: rstp_domain Port: 20 PortId: 4014 Stp: ENABLED Path Cost: 19
Port Mode: EMISTP
Port State: BLOCKING   Topology Change Ack: FALSE
Port Priority: 16   Loopback Port: FALSE
Designated Root: 80:00:00:04:96:05:00:30 Designated Cost: 0
Designated Bridge: 80:00:00:04:96:05:00:30 Designated Port Id: 400a
Edge Port SafeGuard: Enable
```

**History**

This command was first available in ExtremeWare 2.0.

Support for modular switches was introduced in ExtremeWare 4.0.

Support for the `all` keyword was introduced in ExtremeWare 4.0.

Support for the `detail` keyword was introduced in ExtremeWare 6.2 and replaced the `all` keyword.

Support for displaying RSTP data was introduced in ExtremeWare 7.1.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

Support for the `detail` keyword was introduced in ExtremeWare 7.2e.

Support for the edge safeguard feature was introduced in ExtremeWare 7.5.
Platform Availability

This command is available on all platforms.
show vlan stpd

    show vlan <vlan name> stpd

Description
Displays the STP configuration of the ports assigned to a specific VLAN. It is an alternate syntax to the show stpd <spanning tree name> ports vlan <vlan name> command.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

If you have a VLAN that spans multiple STPDs, use this command to display the STP configuration of the ports assigned to that specific VLAN.

This command displays the following:

- STPD port configuration
- STPD port mode of operation
- STPD path cost
- STPD priority
- STPD state (root bridge, and so on)
- Port role (root bridge, edge port, and so on)
- STPD port state (forwarding, blocking, and so on)
- Configured port link type
- Operational port link type

Example

The following command displays the spanning tree configurations for the vlan Default:

```
show vlan default stpd
```

The results for this command are as follows:

```
* Summit1iTx:30 # show vlan "Default" stpd
s0(enabled)  Tag: (none)  Ports: 8  Root/P/C: 80:00:00:01:30:1d:48:30/2/4

<table>
<thead>
<tr>
<th>Port</th>
<th>Mode</th>
<th>State</th>
<th>Cost</th>
<th>Flags</th>
<th>Priority</th>
<th>Port ID</th>
<th>Designated Bridge</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>802.1D</td>
<td>FORWARDING</td>
<td>19</td>
<td>e-Dbb-d-</td>
<td>16</td>
<td>16385</td>
<td>80:00:00:01:30:b6:99:10</td>
</tr>
<tr>
<td>2</td>
<td>802.1D</td>
<td>FORWARDING</td>
<td>4</td>
<td>e-Rbb-w-</td>
<td>16</td>
<td>16386</td>
<td>80:00:00:01:30:1d:48:30</td>
</tr>
<tr>
<td>3</td>
<td>802.1D</td>
<td>DISABLED</td>
<td>4</td>
<td>e-------</td>
<td>16</td>
<td>16387</td>
<td>00:00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>4</td>
<td>802.1D</td>
<td>DISABLED</td>
<td>4</td>
<td>e-------</td>
<td>16</td>
<td>16388</td>
<td>00:00:00:00:00:00:00:00</td>
</tr>
<tr>
<td>5</td>
<td>802.1D</td>
<td>FORWARDING</td>
<td>19</td>
<td>e-Dbb-w-</td>
<td>16</td>
<td>16389</td>
<td>80:00:00:01:30:b6:99:10</td>
</tr>
</tbody>
</table>
```
show vlan stpd

6  802.1D DISABLED  4      e------- 16    16390   00:00:00:00:00:00:00:00
7  802.1D DISABLED  4      e------- 16    16391   00:00:00:00:00:00:00:00
8  802.1D DISABLED  4      e------- 16    16392   00:00:00:00:00:00:00:00

------------------------- Flags: ----------------------------
1:                e=Enable, d=Disable
2:                L = Loopback port
3: (Port role)    R=Root, D=Designated, A=Alternate, B=Backup
4: (Config type)  b=broadcast, p=point-to-point, e=edge, a=auto
5: (Oper. type)   b=broadcast, p=point-to-point, e=edge
6:                p=proposing, a=agree
7: (partner mode) d = 802.1d, w = 802.1w
8:                i = edgeport inconsistency

The following command displays the detailed spanning tree configurations for s0:
show stpd s0 ports detail

The results for this command are as follows:

* Summit400-48t:4 # show stpd s0 ports detail
Stpd: s0        Port: 13        PortId: 400d    Stp: ENABLED    Path Cost: 4
Port Mode: 802.1D
Port State: FORWARDING          Topology Change Ack: FALSE
Port Priority: 16               Loopback Port: FALSE
Designated Root:   00:00:00:00:00:00:00:00      Designated Cost: 0
Designated Bridge: 00:00:00:00:00:00:00:00      Designated Port Id: 0
Partner STP version: Dot1d
Stpd: s0        Port: 14        PortId: 400e    Stp: ENABLED    Path Cost: 4
Port Mode: 802.1D
Port State: FORWARDING          Topology Change Ack: FALSE
Port Priority: 16               Loopback Port: FALSE
Designated Root:   00:00:00:00:00:00:00:00      Designated Cost: 0
Designated Bridge: 00:00:00:00:00:00:00:00      Designated Port Id: 0
Partner STP version: Dot1d

* Summit400-48t:5 #

History

This command was first available in ExtremeWare 6.2.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
unconfigure stpd

    unconfigure stpd {<spanning tree name>}

Description
Restores default STP values to a particular STPD or all STPDs.

Syntax Description

| spanning tree name | Specifies an STPD name on the switch. |

Default
N/A

Usage Guidelines
Use this command to restore default STP values to a particular STPD. If you want to restore default STP values on all STPDs, do not specify a spanning tree name.

For version 2.0 on “i” series switches:
- You can use the all parameter to specify all STPDs.

Example
The following command restores default values to an STPD named Backbone_st:

unconfigure stpd backbone_st

History
This command was first available in ExtremeWare 2.0.

Support for the all parameter was discontinued in ExtremeWare 7.0.

This command was added to the Summit “e” series of switches in ExtremeWare 6.2a and ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
This chapter describes the following commands:

- Commands for enabling and disabling ESRP
- Commands for performing basic ESRP configuration
- Commands for enabling and disabling port restart and failure tracking for ESRP
- Commands for displaying ESRP configuration information
- Commands for enabling and disabling ELRP in an ESRP environment
- Commands for enabling, disabling, configuring, and monitoring the Extreme Link Status Monitoring (ELSM) protocol

ESRP is a feature of ExtremeWare that allows multiple switches to provide redundant layer 3 routing services to users. In addition to providing layer 3 routing redundancy, ESRP also provides for layer 2 redundancy. These “layered” redundancy features can be used in combination or independently. The layer 2 redundancy features of ESRP offer fast failure recovery and provide for dual-homed system design. In some instances, depending on network system design, ESRP can provide better resiliency than using the Spanning Tree Protocol (STP) or Virtual Router Redundancy Protocol (VRRP).

Extreme switches that are not running ESRP, but are connected on a network that has other Extreme switches running ESRP are ESRP-aware. This means that when Extreme switches are attached to the ESRP-enabled switches, the non-ESRP switches reliably perform fail-over and fail-back scenarios in the prescribed recovery times. No configuration of this feature is necessary.

**NOTE**

If you disable EDP on the switch, the switch is no longer ESRP-aware.

ESRP is configured on a per-VLAN basis on each switch. A maximum of four switches can participate in providing redundant layer 3 or layer 2 services to a single VLAN. The switches exchange keep-alive packets for each VLAN independently. Only one switch can actively provide layer 3 routing and/or layer 2 switching for each VLAN. The switch performing the forwarding for a particular VLAN is considered the “master” for that VLAN. Other participating switches for the VLAN are in slave mode.

To have two or more switches participate in ESRP, the following must be true:

- For each VLAN to be made redundant, the switches must have the ability to exchange packets on the same layer 2 broadcast domain for that VLAN. Multiple paths of exchange can be used.
ESRP Commands

- For a VLAN to be recognized as participating in ESRP, the assigned IP address or the IPX NETid for the separate switches must be identical. Other aspects of the VLAN, including its name, are ignored.
- ESRP must be enabled on the desired VLANs for each switch. ESRP cannot be enabled on the VLAN “default.”
- Extreme Discovery Protocol (EDP) must be enabled on the ports that are members of the ESRP VLANs. (The default setting is enabled.)

ESRP can also be enabled on super-VLANs. The super-VLAN must be configured with all the ports as the sub-VLANs.

It is highly recommended that all switches participating in ESRP run the same version of ExtremeWare. Not all ESRP features are available in all ExtremeWare software releases.

Extreme Loop Recovery Protocol (ELRP) is a feature of ExtremeWare that allows you to prevent, detect, and recover from layer 2 loops in the network. You can use ELRP with other protocols such as ESRP.

With ELRP, each switch, except for the sender, treats the ELRP PDU as a layer 2 multicast packet. The sender uses the source and destination MAC addresses to identify the packet it sends and receives. When the sender receives its original packet back, that triggers loop detection and prevention. Once a loop is detected, the loop recovery agent is notified of the event and takes the necessary actions to recover from the loop. ELRP operates only on the sending switch; therefore, ELRP operates transparently across the network.

**NOTE**

Because ELRP introduces the pre-master state to ESRP, you must upgrade all ESRP-enabled switches within an ESRP domain to ExtremeWare 6.2.2b134 (or later) for ESRP to operate correctly. Earlier ExtremeWare releases do not recognize the pre-master state.
clear elrp stats

clear elrp stats {vlan <vlan name>}

**Description**
Clears the transmitted and received ELRP packet counters.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
If you do not specify the optional `vlan name` parameter, you clear the system level ELRP counters, the VLAN counters, and the global counters.

If you specify the optional `vlan name` parameter, you clear the counters for a specific VLAN.

**Example**
The following command clears the ELRP system counters:
```
clear elrp stats
```

The following command clears the VLAN counters on VLAN `elrp1`:
```
clear elrp stats elrp1
```

**History**
This command was first available in ExtremeWare 6.2.2.b134.
This command was not supported in ExtremeWare 7.0.
This command was not supported in ExtremeWare 7.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
clear elsm auto-restart ports

    clear elsm auto-restart ports <portlist>

Description
Clears the Extreme Link Status Monitoring (ELSM) Down-Stuck receive state and enters the Down receive state for the specified ports.

Syntax Description

| portlist          | Specifies the ports or slots and ports for which ELSM auto-start is being cleared. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default
Uncleared.

Usage Guidelines
If you have ELSM automatic restart enabled and the port goes down, ELSM automatically brings up the port if it receives the Hello packets from its neighbor.

If you do not have automatic restart enabled, the port goes through the Up, Down, Down-Wait process once. When you first enable ELSM or if you reboot the switch, it goes through the process twice. After it is done with the cycle (or cycles), the port enters the Down-Stuck state.

To enable automatic restart, use the following command:

    enable elsm auto-restart ports <portlist>

To disable automatic restart, use the following command:

    enable elsm auto-restart ports <portlist>

To get out of the Down-Stuck state and enter the Down state, you can use one of the following commands:

    clear elsm auto-restart ports <portlist>
    enable elsm auto-restart ports <portlist>

Example
The following command clears ELSM automatic restart for ports 1-3 on the switch:

    clear elsm auto-restart ports 1-3

History
This command was first available in ExtremeWare 6.2.2b134.
Platform Availability

This command is available on "i" series platforms only.
clear elsm counters ports

clear elsm counters ports <portlist>

Description
Clears the statistics gathered by Extreme Link Status Monitoring (ELSM) for selected ports.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies the ports or slots and ports for which statistics gathered by ELSM are being cleared. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</th>
</tr>
</thead>
</table>

Default
None.

Usage Guidelines
To clear the statistics gathered by ELSM, use the following command:

clear elsm counters ports <portlist>

Example
The following command clears the statistics gathered by Extreme Link Status Monitoring (ELSM) for ports 1-6 on the switch:

clear elsm counters ports 1-6

History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on "i" series platforms only.
configure debug elsm-port

configure debug elsm-port <level> <port number>

Description
Configures debug tracing for Extreme Link Status Monitoring (ELSM) ports.

Syntax Description

<table>
<thead>
<tr>
<th>level</th>
<th>Specifies the level of debug tracing:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Level 0 disables debug tracing.</td>
</tr>
<tr>
<td>1</td>
<td>Level 1 is information.</td>
</tr>
<tr>
<td>2</td>
<td>Level 2 is trace, and is used to trace the path of code execution.</td>
</tr>
<tr>
<td></td>
<td>Levels 3 and above are not used. To disable debug tracing, set the level to 0.</td>
</tr>
<tr>
<td>port number</td>
<td>Specifies the ports or slots and ports for which ELSM debug tracing is being configured. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
To configure debug tracing for ELSM ports, use the following command:

configure debug elsm-port <level> <port number>

The levels provide the following information:

- Level 1 is information.
- Level 2 is trace, and is used to trace the path of code execution.
- Levels 3 and above are not used.

To disable debug tracing, set the level to 0.

To configure ELSM debug tracing for the entire system, use the following command:

configure debug elsm-system <level>

Example
The following command configures debug tracing of code execution (Level 2) for ELSM port 3 on the switch:

configure debug elsm-port 2 3

History
This command was first available in ExtremeWare 6.2.2b134.
Platform Availability

This command is available on “i” series platforms only.
configure debug elsm-system

configure debug elsm-system <level>

Description
Configures Extreme Link Status Monitoring (ELSM) debug tracing for the entire system.

Syntax Description

<table>
<thead>
<tr>
<th>level</th>
<th>Specifies the level of debug tracing:</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Level 0 disables debug tracing.</td>
</tr>
<tr>
<td>1</td>
<td>Level 1 is information.</td>
</tr>
<tr>
<td>2</td>
<td>Level 2 is trace, and is used to trace the path of code execution. Levels 3 and above are not used. To disable debug tracing, set the level to 0.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
To configure ELSM debug tracing for the entire system, use the following command:

configure debug elsm-system <level>

The levels provide the following information:

- Level 1 is information.
- Level 2 is trace, and is used to trace the path of code execution.
- Levels 3 and above are not used.

To disable debug tracing, set the level to 0.

To configure debug tracing for ELSM ports, use the following command:

configure debug elsm-port <level> <port number>

Example
The following command configures ELSM debug tracing of code execution (Level 2) for the entire system:

configure debug elsm-system 2

History
This command was first available in ExtremeWare 6.2.2b134.
Platform Availability

This command is available on “i” series platforms only.
configure elrp-client one-shot

configure elrp-client one-shot <vlan name> timeout <interval> retry <count> ports <port-mask> action [log | print | print-and-log]

Description
Starts one-time, non-periodic Extreme Loop Recovery Protocol (ELRP) packet transmission on the specified ports of the VLAN using the specified count and interval.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>timeout &lt;interval&gt;</td>
<td>Specifies the interval (in seconds) between consecutive packet transmissions. The valid range for the time out is from 1 to 10 seconds.</td>
</tr>
<tr>
<td>retry &lt;count&gt;</td>
<td>Specifies the number of times ELRP packets must be transmitted. The valid range for retry is from 1 to 3.</td>
</tr>
<tr>
<td>ports &lt;port-mask&gt;</td>
<td>Specifies the set of VLAN ports for packet transmission.</td>
</tr>
<tr>
<td>action log</td>
<td>Specifies that a message should be logged in the system log file when ELRP packets are received back indicating detection of network loop, or no packets are received within the specified duration.</td>
</tr>
<tr>
<td>action trap</td>
<td>Specifies that a message should be printed to the console when ELRP packets are received back indicating detection of network loop, or no packets are received within the specified duration.</td>
</tr>
<tr>
<td>action log-and-trap</td>
<td>Specifies that a message should be logged in the system log file and printed to the console when ELRP packets are received back indicating detection of network loop, or no packets are received within the specified duration.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines

This command starts one-time, non-periodic ELRP packet transmission on the specified ports of the VLAN using the specified count and interval. If any of these transmitted packets is returned, indicating loopback detection, the ELRP client can perform a configured action such as logging a message in the system log file or printing a log message to the console. There is no need to trap to the SNMP manager for non-periodic requests.

Use the configure elrp-client periodic command to configure periodic transmission of ELRP packets.

The ELRP client must be enabled globally in order for it to work on any VLANs. Use the enable elrp-client command to globally enable the ELRP client.

The ELRP client can be disabled globally so that none of the ELRP VLAN configurations take effect. Use the disable elrp-client command to globally disable the ELRP client.
Example
The following example configures a non-periodic ELRP client on VLAN \textit{v1} with a timeout interval of 2 seconds and a retry every 2 seconds. It also prints a log message to the console.

\texttt{configure elrp-client one-shot v1 timeout 2 retry 2 ports <1:5> print}

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on all platforms.
configure elrp-client periodic

configure elrp-client periodic <vlan name> interval <seconds> ports <port-mask> action [log | log-and-trap | trap]

Description
Starts periodic Extreme Loop Recovery Protocol (ELRP) packet transmission on the specified ports of the VLAN using the specified interval.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>interval &lt;seconds&gt;</td>
<td>Specifies the interval (in seconds) between consecutive packet transmissions.</td>
</tr>
<tr>
<td>ports &lt;port-mask&gt;</td>
<td>Specifies the set of VLAN ports for packet transmission.</td>
</tr>
<tr>
<td>action log</td>
<td>Specifies that a message should be logged in the system log file when ELRP packets are received back indicating detection of network loop, or no packets are received within the specified duration.</td>
</tr>
<tr>
<td>action trap</td>
<td>Specifies that a trap message should be sent to the SNMP manager when ELRP packets are received back indicating detection of network loop, or no packets are received within the specified duration.</td>
</tr>
<tr>
<td>action log-and-trap</td>
<td>Specifies that a message should be logged in the system log file and a trap message should be sent to the SNMP manager when ELRP packets are received back indicating detection of network loop, or no packets are received within the specified duration.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
This command starts periodic ELRP packet transmission on the specified ports of the VLAN using the specified interval. If any of these transmitted packets is returned, indicating loopback detection, the ELRP client can perform a configured action such as logging a message in the system log file and/or sending a trap to the SNMP manager.

Use the `configure elrp-client one-shot` command to configure non-periodic, one-time transmission of ELRP packets.

The ELRP client must be enabled globally in order for it to work on any VLANs. Use the `enable elrp-client` command to globally enable the ELRP client.

The ELRP client can be disabled globally so that none of the ELRP VLAN configurations take effect. Use the `disable elrp-client` command to globally disable the ELRP client.

Example
The following example configures a periodic request on VLAN v1, writes to the log file, and sends a trap to the SNMP manager.
configure elrp-client periodic v1 interval 10 ports 5 log-and-trap

**History**
This command was first available in ExtremeWare 7.3.0

**Platform Availability**
This command is available on all platforms.
configure elsm hellotime

configure elsm hellotime <1-128> ports <portlist>

Description
Configures the Extreme Link Status Monitoring (ELSM) hello timer by specifying the time between consecutive ELSM hellos for the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hellotime &lt;1-128&gt;</td>
<td>Specifies the time, in seconds between consecutive hellos. Use the same value for the hello interval on peer ports. The default is 1. The range is 1 to 128.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports or slots and ports for which the ELSM hello timer should be configured. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
1.

Usage Guidelines
The Extreme Link Status Monitoring (ELSM) protocol allows you to detect remote CPU failures in the network. A software or hardware fault might prevent the CPU from transmitting or receiving, leading to the sudden failure of the CPU. If the CPU cannot process or send packets, ELSM isolates the connections to the faulty switch from the rest of the network. If the switch fabric continues to send packets during a CPU failure, the switch may appear to be healthy when it is not.

An Extreme Networks device with ELSM enabled can detect remote CPU failures by exchanging hello packets between two ELSM peers. When ELSM detects a CPU failure as a result of not hearing from its neighbor, it brings down the connection to the neighbor. ELSM operates on a point-to-point basis; you only configure ELSM on the ports that connect to other devices within the network, but you must configure ELSM on both sides of the peer connections.

ELSM ports use hello packets to communicate information about the health of the network to peer ports. The hello packets are received and transmitted by an ELSM-enabled port. The port expects a response from its neighbor after it sends a hello packet.

When you enable ELSM on the specified ports, the ports participate in ELSM with their peers and begin exchanging ELSM hellos. Use the following command to enable ELSM:

disable elsm ports <portlist>

ELSM works between two connected ports, and each ELSM instance is based on a single port.

When you disable ELSM on the specified ports, the ports no longer send ELSM hellos to its peer and no longer maintain ELSM states.

When you disable ELSM on the specified ports, the ports no longer send ELSM hellos to its peer and no longer maintain ELSM states. Use the following command to disable ELSM:

disable elsm ports <portlist>
ESRP Commands

ESLM uses two types of hello packets to communicate the health of the network to other ELSM ports.

- **Hello+** — The device receives a hello from the neighbor device, and no problem is detected
- **Hello-** — The device does not receive a hello from the neighbor device, or the device has experienced a critical event.

**Example**
The following command specifies 5 seconds between consecutive ELSM hellos for ports 1-7 on the switch:

```
configure elsm helloTime 5 ports 1-7
```

**History**
This command was first available in ExtremeWare 6.2.2b134.

**Platform Availability**
This command is available on the “i” series platform only.
configure elsm hold-threshold

configure elsm hold-threshold <1-3> ports <portlist>

Description
Configures the Extreme Link Status Monitoring (ELSM) hold threshold by specifying the number of packets to transition out of the Down-Wait receive state to the Up receive state for the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hold-threshold &lt;1-3&gt;</td>
<td>Specifies the number of packets required to transition out of the Down-Wait state to the Up state. A threshold of 1 means the ELSM port must receive at least one Hello+ packet to transition from the Down-Wait state to the Up state. The default is 2. The range is 1 to 3.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the ports or slots and ports for which the ELSM hold threshold should be configured. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
2.

Usage Guidelines
The Extreme Link Status Monitoring (ELSM) protocol allows you to detect remote CPU failures in the network. A software or hardware fault might prevent the CPU from transmitting or receiving, leading to the sudden failure of the CPU. If the CPU cannot process or send packets, ELSM isolates the connections to the faulty switch from the rest of the network. If the switch fabric continues to send packets during a CPU failure, the switch may appear to be healthy when it is not.

An Extreme Networks device with ELSM enabled can detect remote CPU failures by exchanging hello packets between two ELSM peers. When ELSM detects a CPU failure as a result of not hearing from its neighbor, it brings down the connection to the neighbor. ELSM operates on a point-to-point basis; you only configure ELSM on the ports that connect to other devices within the network, but you must configure ELSM on both sides of the peer connections.

ELSM ports use hello packets to communicate information about the health of the network to peer ports. The hello packets are received and transmitted by an ELSM-enabled port. The port expects a response from its neighbor after it sends a hello packet.

When you enable ELSM on the specified ports, the ports participate in ELSM with their peers and begin exchanging ELSM hellos. Use the following command to enable ELSM:

disable elsm ports <portlist>

ELSM works between two connected ports, and each ELSM instance is based on a single port.

When you disable ELSM on the specified ports, the ports no longer send ELSM hellos to its peer and no longer maintain ELSM states.

When you disable ELSM on the specified ports, the ports no longer send ELSM hellos to its peer and no longer maintain ELSM states. Use the following command to disable ELSM:

disable elsm ports <portlist>
ESRP Commands

ELSM uses two types of hello packets to communicate the health of the network to other ELSM ports.

- **Hello+** — The device receives a hello from the neighbor device, and no problem is detected
- **Hello-** — The device does not receive a hello from the neighbor device, or the device has experienced a critical event.

Use the following command to specify the time, in seconds, between consecutive ELSM hellos:

```
configure elsm hellotime <1-128> ports <portlist>
```

Table 28 describes the ELSM timers that are derived from other timers and are not user-configurable.

**Table 28: Derived timers**

<table>
<thead>
<tr>
<th>Timer</th>
<th>Description</th>
</tr>
</thead>
</table>
| Down   | Specifies the time it takes for the ELSM receive port to cycle through the following states:  
- Down  
- Down-Wait  
- Up  
  If the Hello timer is set to 1 seconds, it takes 4 seconds for the ELSM receive port to cycle through the states.  
  After the timer expires, the port checks the number of Hello+ packets against the hold threshold. If the number of Hello+ packets received is greater than or equal to the configured hold threshold, the ELSM receive port moves from the Down-Wait state to the Up state.  
  If the number of Hello+ packets received is less than the configured hold threshold, the ELSM receive port moves from the Down-Wait state to the Down state.  
  The down timer is 4 times the Hello timer. |
| Up     | When an ELSM-enabled port enters the Up state, the Up timer begins. The timer restarts each time the port receives a Hello+ packet. The Up timer is 6 times the Hello timer. |
| HelloRx| Specifies the time in which a Hello packet is expected, otherwise the ELSM transmit state changes from HelloRx+ to HelloRx-. The HelloRx timer is 6 times the Hello timer. |

The ELSM receive port receives hello messages from its peer. The ELSM receive states are:

- **Down**—Port is down.  
  When you enable ELSM, the starting state is Up. If it does not receive a Hello message from its neighbor before the Up timeout, it transitions to the Down state. When ELSM is down, data packets are neither received nor transmitted out of that port.

- **Down-Wait**—Transitional state.  
  When the port enters the Down-Wait state, the Down timer begins. After the timer expires, the port checks the number of Hello+ packets received against the configured down threshold. If the Hello+ packets are greater than or equal to the threshold, the port transitions to the Up state. If the Hello+ packets are less than the threshold, the port returns to the Down state and begins the process again.

- **Up**—Beginning state, port is up.  
  If ELSM is enabled and the port enters the Up state, the Up timer begins. Each time the port receives a Hello+ packet, the timer restarts and remains in the Up state.  
  If the port no longer receives hello packets for Up-timer seconds, or receives a hello- packet, the port transitions to either the Down or Down-Stuck state.
configure elsm hold-threshold

- **Down-Stuck** —Port stays down and requires manual intervention.

If you have ELSM automatic restart enabled and the port goes down, ELSM automatically brings up the port if it receives the Hello packets from its neighbor.

If you do not have automatic restart enabled, the port goes through the Up, Down, Down-Wait process once. When you first enable ELSM or if you reboot the switch, it goes through the process twice. After it is done with the cycle (or cycles), the port enters the Down-Stuck state.

To enable automatic restart, use the following command:

```
enable elsm auto-restart ports <portlist>
```

To disable automatic restart, use the following command:

```
enable elsm auto-restart ports <portlist>
```

To get out of the Down-Stuck state and enter the Down state, you can use one of the following commands:

```
clear elsm auto-restart ports <portlist>
enable elsm auto-restart ports <portlist>
```

The ELSM transmit port sends hello messages to its peer. The ELSM transmit states are.

- **Init** —No ELSM activity, the initial transmit state. The port remains in this state until ELSM is enabled on the port.

- **HelloRx-** —Transitions from Init when ELSM is enabled.

  When you enable ELSM, the port transitions from the Init state to the HelloRx- state. During the HelloRx- state, the port waits to receive neighbor hello messages. Depending on what happens to the port, the following occurs:
  - Hello+ packet received: The port actively receives hello messages from its neighbor and the network is healthy. The port transitions to the Hello Rx+ state.
  - Hello- packet received: The neighbor has not received the Hello packet sent by this switch. The switch transitions to the HelloRx+ state.

- **HelloRx+** —Up and receives hello messages.

  In this state, the port receives hello messages from its neighbor and the following occurs:
  - Hello+ packet received: The port actively receives hello messages from its neighbor and the network is healthy. The port remains in the Hello Rx+ state and the HelloRx timer is restarted.
  - Hello- packet received: The neighbor has not received the Hello sent by this switch. The switch stays in the HelloRx+ state.
  - HelloRX timer: If the HelloRx timer expires, the port returns to the HelloRx- state.

- **CriticalEvent** —A critical event occurs in the software.

  A critical event occurs when a critical task crash occurs in the software. When the critical event clears, the port returns to the HelloRx- state. As long as the port is in the CriticalEvent state, Hello -packets are sent to the neighboring device.

**Example**

The following command specifies that 2 packets are required to transition out of the Down-Wait receive state to the Up receive state for ports 1-4 on the switch:

```
configure elsm hold-threshold 2 ports 1-4
```
History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on “i” series platforms only.
configure esrp port-mode ports

configure esrp port-mode [host | normal] ports <portlist> {don’t-count}

Description
Configures the ESRP port mode for ESRP host attach.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>host</td>
<td>Specifies that the ports should be configured as host ports.</td>
</tr>
<tr>
<td>normal</td>
<td>Specifies that the ports should be configured as normal ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be</td>
</tr>
<tr>
<td></td>
<td>a list of slots and ports. On a stand-alone switch, can be one or more port</td>
</tr>
<tr>
<td></td>
<td>numbers. May be in the form 1, 2, 3-5, 2:*; 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>don’t-count</td>
<td>Specifies that ports should not be counted as active ports.</td>
</tr>
</tbody>
</table>

Default
Normal.

Usage Guidelines
This feature is useful in dual-homed server environments in conjunction with high availability server load-balancing (SLB) configurations.

Ports configured as normal ports do not accept or transmit layer 2 or layer 3 traffic when the local ESRP device is a slave.

Ports configured as host ports allow configured ports that do not represent loops to the network to continue operation independent of ESRP status. The command sets the port to forward, allowing those ports directly attached to the slave’s hosts to communicate with other hosts that are connected to the master. If you use load sharing with the host attach feature, configure all ports in the same load sharing groups as host attach ports.

don’t-count has the effect of not counting the host ports and normal ports as active ports. This has the convenience of minimal ESRP state changes due to frequent client activities like reboots and unplugging laptops. If you use load sharing with the don’t count feature, configure all ports in the same load sharing group as don’t count ports.

An L2 connection for VLANs between ESRP switches is required.

Example
The following command configures ports 1 through 5 as host ports, and prevents them from being counted as active ports:

```bash
configure esrp port-mode host ports 1-5 don’t-count
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure msm-failover esrp-failover-mode

configure msm-failover esrp-failover-mode [none | rapid-reelection | remain-esrp-master-in-l2-domains {<reelect-timeout>}]

Description
Configures the desired operation of hitless failover when ESRP is in use.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies that ESRP does not participate in hitless failover. The master switch blocks its ports during a failover and performs a full initialization of ESRP. This is the default.</td>
</tr>
<tr>
<td>rapid-reelection</td>
<td>Specifies that ESRP behaves as if none was selected. In addition, if a failover occurs when the switch is the master in an ESRP domain, the switch sends a notification that the standby nodes should elect a new master as soon as possible. This facilitates a faster ESRP master reelection than none.</td>
</tr>
<tr>
<td>remain-esrp-master-in-l2-domains</td>
<td>Specifies that an ESRP master notifies the standby nodes of the failover and wishes to remain the master. Along with the notification, it sends the amount of time in seconds that the standby nodes should wait before beginning reelection.</td>
</tr>
<tr>
<td>reelect-timeout</td>
<td>Specifies the amount of time the standby nodes should wait before beginning reelection. The default is 30 seconds, and the range is 15 - 180 seconds.</td>
</tr>
</tbody>
</table>

For more information about ESRP and ESRP tracking, see the ExtremeWare Software User Guide.

Example
The following command configures the switch to send a notification that the standby nodes should elect a new master as soon as possible:

configure msm-failover esrp-failover-mode rapid-reelection

History
This command was first available in ExtremeWare 7.1.1.

Platform Availability
This command is available on BlackDiamond switches only.
configure vlan add domain-member vlan

configure vlan <super_esrp_vlan> add domain-member vlan <sub_esrp_vlan>

Description
Adds a VLAN to an ESRP domain.

Syntax Description

<table>
<thead>
<tr>
<th>super_esrp_vlan</th>
<th>Specifies the name of an ESRP-enabled domain master-VLAN.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sub_esrp_vlan</td>
<td>Specifies the name of a domain member-VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
ESRP is performed in the domain master VLAN only, and not the other domain members. The domain master VLAN controls member VLANs whether they are in forward or blocked states.

The domain master does not need to have all the ports as the domain members. Domain master VLANs can have their own set of ports and the members can have different ports.

Example
The following command adds the domain member-VLAN sub_esrp1 to ESRP-enabled domain master-VLAN esrp-super:

configure vlan esrp-super add domain-member vlan sub_esrp1

History
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan add elrp-poll ports

configure vlan <vlan name> add elrp-poll ports [portlist | all]

**Description**
Configures the ports of a VLAN where ELRP packet transmission is requested by ESRP.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports in the VLAN.</td>
</tr>
</tbody>
</table>

**Default**
All ports of an ESRP-enabled VLAN have ELRP transmission enabled.

**Usage Guidelines**
This command allows you to configure the ports in your network that might experience loops, such as ports that connect to master, slave, or ESRP-aware switches, to receive ELRP packets. You do not need to send ELRP packets to host ports.

**Example**
The following command enables ELRP packet transmission for ports 3-5 on VLAN esrp1:

```
configure vlan esrp1 add elrp-poll ports 3-5
```

**History**
This command was first available in ExtremeWare 6.2.2b134.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vlan add ports no-restart

configure vlan <vlan name> add ports [<portlist> | all] no-restart

**Description**
Disables port restart for a port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be</td>
</tr>
<tr>
<td></td>
<td>a list of slots and ports. On a stand-alone switch, can be one or more port</td>
</tr>
<tr>
<td></td>
<td>numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
To disable port restart, you either delete the ports and then add them again with the **no-restart** option, or directly add the ports with the **no-restart** option.

**Example**
The following command disables port restart for ports 7-9 on VLAN esrp1:

```bash
configure vlan esrp1 add ports 7-9 no-restart
```

**History**
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vlan add ports restart

configure vlan <vlan name> add ports [<portlist> | all] restart

Description
Configures ESRP to restart ports if there is a state change and the downstream switch is from another vendor.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If a VLAN becomes a slave, ESRP disconnects member ports that have port restart enabled. The disconnection of these ports causes downstream devices to remove the ports from their FDB tables. After 3 seconds the ports re-establish connection with the ESRP-enabled device. This feature allows you to use ESRP in networks that include equipment from other vendors.

Example
The following command enables port restart for ports 7-9 on VLAN esrp1:

```
configure vlan esrp1 add ports 7-9 restart
```

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan add track-bgp

    configure vlan <vlan name> add track-bgp failover <priority>

Description
Configures an ESRP-enabled VLAN to track any available BGP route.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a number between 0 and 255.</td>
</tr>
</tbody>
</table>

Default
No BGP route tracking.

Usage Guidelines
If no BGP routes are detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and makes it ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example
The following command enables BGP failure tracking, and specifies that the ESRP priority for VLAN esrp-1 be set to 10 when no BGP routes are reachable.

configure vlan esrp-1 add track-bgp failover 10

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series platforms only.
configure vlan add track-diagnostic

configure vlan <vlan name> add track-diagnostic failover <priority>

Description
Configures backplane diagnostics failure tracking for an ESRP-enabled VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a number between 0 and 255.</td>
</tr>
</tbody>
</table>

Default
No diagnostic tracking.

Usage Guidelines
If a diagnostic failure is detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and makes it ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example
The following command enables diagnostic failure tracking, and specifies that the ESRP priority for VLAN esrp-1 be set to 10 upon a diagnostic failure.

```
configure vlan esrp-1 add track-diagnostic failover 10
```

History
This command was first available in ExtremeWare 6.1.5.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan add track-environment

configure vlan <vlan name> add track-environment failover <priority>

**Description**
Configures an ESRP-enabled VLAN to track environmental failures.

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a number between 0 and 255.</td>
</tr>
</tbody>
</table>

**Default**
No environmental tracking.

**Usage Guidelines**
Environmental tracking tracks fan, power supply, and chassis temperature status.

If a failure is detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

**Example**
The following command enables diagnostic failure tracking, and specifies that the ESRP priority for VLAN esrp-1 be set to 10 upon a diagnostic failure.

```
configure vlan esrp-1 add track-environment failover 10
```

**History**
This command was first available in ExtremeWare 6.1.5.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vlan add track-iproute

configure vlan <vlan name> add track-iproute <ip address>/<masklength>

Description
Configures an ESRP-enabled VLAN or a VRRP VLAN to track a route entry in the kernel route table.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled or VRRP VLAN name.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the route entry to be tracked.</td>
</tr>
</tbody>
</table>

Default
No route tracking.

Usage Guidelines

If the specified routes are not reachable, the device automatically relinquishes master status and remains in slave mode (for ESRP) or backup mode (for VRRP).

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example

The following command enables IP route failure tracking for routes to the specified subnet:

```bash
configure vlan esrp-1 add track-iproute 192.168.46.0/24
```

History

This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability

This command is available on all platforms.
configure vlan add track-ospf

configure vlan <vlan name> add track-ospf failover <priority>

**Description**
Configures an ESRP-enabled VLAN to track any available OSPF route.

**Syntax Description**

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a number between 0 and 255.</td>
</tr>
</tbody>
</table>

**Default**
No OSPF route tracking.

**Usage Guidelines**
The switch cannot be the ESRP master if none of the specified routes are reachable.

If no OSPF routes are detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

**Example**
The following command enables OSPF route failure tracking, and specifies that the ESRP priority for VLAN esrp-1 be set to 10 when all OSPF routes become unreachable:

```
configure vlan esrp-1 add track-ospf failover 10
```

**History**
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vlan add track-ping

configure vlan <vlan name> add track-ping <ip address> frequency <seconds> miss <number>

Description
Configures an ESRP-enabled VLAN or VRRP VLAN to track an external gateway using ping.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled or VRRP VLAN name.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the external gateway.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the interval in seconds between ping requests.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the number of consecutive ping failures that will initiate failover to an ESRP slave or VRRP backup router.</td>
</tr>
</tbody>
</table>

Default
No ping tracking. Default miss number for VRRP is 3 consecutive missed ping responses.

Usage Guidelines
If the external gateway is not reachable as indicated by consecutive ping failures, the device automatically relinquishes master status and remains in slave mode (for ESRP) or backup mode (for VRRP).

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example
The following command enables ping tracking for the external gateway at 10.207.29.17, pinging every 10 seconds, and considering the gateway to be unreachable if no response is received to 5 consecutive pings:

configure vlan esrp-1 add track-ping 10.207.29.17 frequency 10 miss 5

History
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan add track-rip

configure vlan <vlan name> add track-rip failover <priority>

Description
Configures an ESRP-enabled VLAN to track any available RIP route.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a number between 0 and 255.</td>
</tr>
</tbody>
</table>

Default
No RIP route tracking.

Usage Guidelines
If no RIP routes are detected, the ESRP VLAN priority steps to the failover-priority value specified. By setting the failover priority to be lower than the normal priority of the VLAN, it will cause the affected VLAN to go into standby.

The range of the priority value is 0 to 254. Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master.

To make effective use of this feature, the following should be true:

- The priority field should be given precedence over the other election factors by assigning the priority-ports-track-mac election algorithm to the VLAN.
- The normal priority of the ESRP-enabled VLANs must be higher than the failover priority of this command.

Example
The following command enables RIP route tracking, and specifies that the ESRP priority for VLAN esrp-1 be set to 10 upon a diagnostic failure:

```
cfg@switch(config)#configure vlan esrp-1 add track-rip failover 10
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan add track-vlan

configure vlan <vlan name> add track-vlan <vlan_tracked>

Description
Configures an ESRP-enabled VLAN or a VRRP VLAN to track port connectivity to a specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled or VRRP VLAN name.</td>
</tr>
<tr>
<td>vlan_tracked</td>
<td>Specifies the VLAN to be tracked.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
If no active ports remain on the specified VLANs, the device automatically relinquishes master status and remains in slave mode (for ESRP) or backup mode (for VRRP).

An ESRP or VRRP VLAN can track one VLAN.

This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example
The following command enables ESRP-enabled VLAN esrp-1 to track port connectivity to VLAN engineering:

```
configure vlan esrp-1 add track-vlan engineering
```

History
This command was first available in ExtremeWare 4.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete domain-member vlan

    configure vlan <super_esrp_vlan> delete domain-member vlan <sub_esrp_vlan>

**Description**

Deletes a VLAN from an ESRP domain.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>super_esrp_vlan</td>
<td>Specifies a domain master-VLAN name.</td>
</tr>
<tr>
<td>sub_esrp_vlan</td>
<td>Specifies a domain member-VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

The domain master does not need to have all the ports as the domain members. Domain master VLANs can have their own set of ports and the members can have different ports.

**Example**

The following command deletes the domain member-VLAN `sub_esrp1` from ESRP-enabled domain master-VLAN `esrp-super`:

```
cfg> configure vlan esrp-super delete domain-member vlan sub_esrp1
```

**History**

This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure vlan delete elrp-poll ports

configure vlan <vlan name> delete elrp-poll ports [portlist] all

Description
Disables ELRP packet transmission on ports of an ESRP-enabled VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a</td>
</tr>
<tr>
<td></td>
<td>list of slots and ports. On a stand-alone switch, can be one or more port</td>
</tr>
<tr>
<td></td>
<td>numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ports in the VLAN.</td>
</tr>
</tbody>
</table>

Default
All ports of an ESRP-enabled VLAN have ELRP transmission enabled.

Usage Guidelines
If you have host ports on an ESRP-enabled VLAN, you do not need to send ELRP packets to those ports.

If you change your network configuration, and a port no longer connects to a master, slave, or ESRP-aware switch, you can disable ELRP transmission on that port.

Example
The following command disables ELRP packet transmission for ports 3-5 on VLAN esrp1:

configure vlan esrp1 delete elrp-poll ports 3-5

History
This command was first available in ExtremeWare 6.2.2b134.

This command was not supported ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete track-bgp

configure vlan <vlan name> delete track-bgp

**Description**
Disables BGP route tracking for an ESRP-enabled VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command disables BGP tracking for VLAN esrp-1:
configure vlan esrp-1 delete track-bgp

**History**
This command was first available in ExtremeWare 6.2.

**Platform Availability**
This command is available on “i” series platforms only.
configure vlan delete track-diagnostic

configure vlan <vlan name> delete track-diagnostic

Description
Disables diagnostics failure tracking for an ESRP-enabled VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command disables diagnostic failure tracking for VLAN esrp-1:

```
configure vlan esrp-1 delete track-diagnostic
```

History
This command was first available in ExtremeWare 6.1.5.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete track-environment

configure vlan <vlan name> delete track-environment

Description
Disables environmental failure tracking.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command disables environmental failure tracking for VLAN esrp-1:

```bash
configure vlan esrp-1 delete track-environment
```

History
This command was first available in ExtremeWare 6.1.5.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete track-iproute

configure vlan <vlan name> delete track-iproute <ipaddress>/<masklength>

**Description**
Disables route table entry tracking for an ESRP-enabled VLAN or a VRRP VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled or VRRP VLAN name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the route entry to be tracked.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

**Example**
The following command disables tacking of routes to the specified subnet for VLAN esrp-1:

configure vlan esrp-1 delete track-iproute 192.168.46.0/24

**History**
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vlan delete track-ospf

configure vlan <vlan name> delete track-ospf

Description
Disables OSPF route tracking for an ESRP-enabled VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command disables OSPF route tracking for VLAN esrp-1:
configure vlan esrp-1 delete track-ospf

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete track-ping

configure vlan <vlan name> delete track-ping <ipaddress>

Description
Disables the tracking of an external gateway using ping.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled or VRRP VLAN name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the external gateway.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

Example
The following command disables ping tracking for the external gateway at 10.207.29.17:
configure vlan esrp-1 delete track-ping 10.207.29.17

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete track-rip

configure vlan <vlan name> delete track-rip

Description
Disables RIP route tracking for an ESRP-enabled VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

Default
No RIP route tracking.

Usage Guidelines
None.

Example
The following command disables RIP route failure tracking for VLAN esrp-1:

```
configure vlan esrp-1 delete track-rip
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan delete track-vlan

configure vlan <vlan name> delete track-vlan <vlan_tracked>

**Description**
Disables the tracking of port connectivity to a specified VLAN.

**Syntax Description**
- **vlan name**: Specifies an ESRP-enabled or VRRP VLAN name.
- **vlan_tracked**: Specifies the VLAN to be tracked.

**Default**
N/A.

**Usage Guidelines**
This command can be used with both ESRP-enabled VLANs and VRRP VLANs.

**Example**
The following command disables the tracking of port connectivity to VLAN *engineering*:
```
configure vlan esrp-1 delete track-vlan engineering
```

**History**
This command was first available in ExtremeWare 4.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vlan esrp elrp-master-poll disable

configure vlan <vlan name> esrp elrp-master-poll disable

Description
Disables the use of ELRP by ESRP in the master state.

Syntax Description

+-----------------+--------------------------------------------------+
|   vlan name      | Specifies an ESRP-enabled VLAN name.             |
+-----------------+--------------------------------------------------+

Default
Disabled.

Usage Guidelines
Use this command to disable the use of ELRP by ESRP in the master state. When you disable ELRP, the ESRP master switch no longer transmits ELRP PDUs to detect network loops.

Example
The following command disables the use of ELRP in the master state on the ESRP-enabled VLAN elrp1:

configure vlan elrp1 esrp elrp-master poll disable

History
This command was first available in ExtremeWare 6.2.2b134.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan esrp elrp-master-poll enable

configure vlan <vlan name> esrp elrp-master-poll enable {interval <seconds>}

Description
Enables the use of ELRP by ESRP in the master state, and configures how often the master checks for loops in the network.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies how often, in seconds, successive ELRP packets are sent. The default is 1 second. The range is 1 to 32 seconds.</td>
</tr>
</tbody>
</table>

Default
- Use of ELRP in the master state—disabled
- Interval—1 second

Usage Guidelines
Use this command to enable the use of ELRP by ESRP in the master state. When an ESRP-enabled switch is in the master state, and you enable elrp-master-poll, the switch periodically sends ELRP PDUs at the configured interval level. If a loop is detected in the network, the transmitted PDUs are received by the switch. The ESRP master switch then transitions to the slave state to break the network loop.

Specify the interval parameter to configure how often successive ELRP PDUs are sent while in the master state. If you do not specify an interval value, the default value is used.

Example
The following command enables the use of ELRP in the master state on the ESRP-enabled VLAN elrp1:

```
configure vlan elrp1 esrp elrp-master-poll enable
```

The following command configures the ESRP master to check for loops in the network every 3 seconds:

```
configure vlan elrp1 esrp elrp-master-poll enable interval 3
```

History
This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
Platform Availability

This command is available on all platforms.
configure vlan esrp elrp-premaster-poll disable

    configure vlan <vlan name> esrp elrp-premaster-poll disable

Description
Disables the use of ELRP by ESRP in the pre-master state.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
Use this command to disable the use of ELRP by ESRP in the pre-master state. When you disable ELRP in the pre-master state, the ESRP pre-master switch no longer transmits ELRP PDUs to detect network loops prior to changing to the master state.

Example
The following command disables the use of ELRP in the pre-master state on the ESRP-enabled VLAN elrp1:

```
configure vlan elrp1 esrp elrp-premaster poll disable
```

History
This command was first available in ExtremeWare 6.2.2b134.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan esrp elrp-premaster-poll enable

configure vlan <vlan name> esrp elrp-premaster-poll enable {count <number> | interval <seconds>}

Description
Enables the use of ELRP by ESRP in the pre-master state, and configures how many times the switch sends ELRP PDUs and how often the switch sends ELRP PDUs in the pre-master state.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the number of times the switch sends ELRP PDUs. The default is 3.</td>
</tr>
<tr>
<td></td>
<td>The range is 1 to 32.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies how often, in seconds, the ELRP PDUs are sent. The default is 1</td>
</tr>
<tr>
<td></td>
<td>second. The range is 1 to 32 seconds.</td>
</tr>
</tbody>
</table>

Default
- Use of ELRP in the pre-master state—disabled
- Count—3 times
- Interval—1 second

Usage Guidelines
Use this command to enable the use of ELRP by ESRP in the pre-master state to prevent network loops from occurring. When an ESRP-enabled switch is in the pre-master state (waiting to become the master), and you enable elrp-premaster-poll, the switch periodically sends ELRP PDUs at the configure level for a specified number of times. If there is a loop in the network, the transmitted PDUs are received by the switch. If this happens, the ESRP pre-master switch does not transition to the master state; rather, the switch transitions to the slave state.

If you do not specify the optional count or interval parameters, the default values are used.

If no packets are received by the sender, there is no loop in the network.

Example
The following command enables the use of ELRP in the pre-master state on the ESRP-enabled VLAN elrp1:

configure vlan elrp1 esrp elrp-premaster poll enable

History
This command was first available in ExtremeWare 6.2.2b134.
This command was not supported in ExtremeWare 7.0.
This command is supported in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure vlan esrp esrp-election


Description

Configures the election algorithm on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>ports-track-priority</td>
<td>Specifies that this VLAN should consider election factors in the following order: Active ports, tracking information, ESRP priority.</td>
</tr>
<tr>
<td>ports-track-priority-mac</td>
<td>Specifies that this VLAN should consider election factors in the following order: Active ports, tracking information, ESRP priority, MAC address. This is the default election algorithm.</td>
</tr>
<tr>
<td>track-ports-priority</td>
<td>Specifies that this VLAN should consider election factors in the following order: Tracking information, active ports, ESRP priority.</td>
</tr>
<tr>
<td>track-ports-priority-mac</td>
<td>Specifies that this VLAN should consider election factors in the following order: Tracking information, active ports, ESRP priority, MAC address.</td>
</tr>
<tr>
<td>priority-ports-track-mac</td>
<td>Specifies that this VLAN should consider election factors in the following order: ESRP priority, active ports, tracking information, MAC address.</td>
</tr>
<tr>
<td>priority-track-ports-mac</td>
<td>Specifies that this VLAN should consider election factors in the following order: ESRP priority, tracking information, active ports, MAC address.</td>
</tr>
<tr>
<td>priority-mac-only</td>
<td>Specifies that this VLAN should consider election factors in the following order: ESRP priority, MAC address.</td>
</tr>
</tbody>
</table>

Default

`ports_track_priority_mac` election algorithm.

Usage Guidelines

The election algorithm determines the order of precedence of the election factors used to determine the ESRP Master. The election factors are:

- **Active Ports** (*ports*): the number of active ports (the switch with the highest number takes priority)
- **Tracking Information** (*track*): whether the switch is using ESRP tracking. A switch using tracking has priority.
- **ESRP Priority** (*priority*): a user-defined priority number between 0 and 254. A higher number has higher priority. The default priority setting is 0. A priority setting of 255 makes an ESRP switch remain in slave mode and is the recommended setting for system maintenance. A switch with a priority setting of 255 will never become the master.
- **MAC address** (*mac*): the switch MAC address. A higher-number address has priority.

The election algorithm must be the same on all switches for a particular VLAN.
The `ports-track-priority` or `track-ports-priority` options can be used to ensure that there is no failback if the original Master recovers (the Master will have the same ports, tracks and priority, but a higher MAC).

If a switch is master, it actively provides layer 3 routing services to other VLANs, and layer 2 switching between all the ports of that VLAN. Additionally, the switch exchanges ESRP packets with other switches that are in slave mode.

If a switch is in slave mode, it exchanges ESRP packets with other switches on that same VLAN. When a switch is in slave mode, it does not perform layer 3 routing or layer 2 switching services for the VLAN.

**Example**

The following command configures the election algorithm to use tracking information as the first criteria for determining the ESRP master switch for VLAN `esrp-1`:

```
configure vlan esrp-1 esrp esrp-election track-ports-priority-mac
```

**History**

This command was first available in ExtremeWare 6.0.

The `ports-track-priority` and `track-ports-priority` election algorithms were added in ExtremeWare 6.2.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
configure vlan esrp esrp-premaster-timeout

configure vlan <vlan name> esrp esrp-premaster-timeout <premaster-timer (0-512, 0 restores df1t)>

Description
Configures the ESRP pre-master timeout value.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>premaster-timer</td>
<td>Specifies the maximum length of time, in seconds, that the transitioning master VLAN remains in the pre-master state. The range is 0 to 512.</td>
</tr>
</tbody>
</table>

Default
The default timeout is 6 seconds (three times the hello timer).

Usage Guidelines
The premaster-timer range is 0 - 512. If you set the premaster-timer to 0, ESRP uses the default. To see the premaster-timer settings, use the show esrp vlan command.

⚠️ CAUTION
Configure the pre-master state timeout only with guidance from Extreme Networks personnel. Misconfiguration can severely degrade the performance of ESRP and your switch.

Example
The following command configures the pre-master timeout to 10 seconds for the VLAN esrp-1:

configure vlan esrp-1 esrp esrp-premaster-timeout 10

History
This command was first available in ExtremeWare 7.1.0, and replaced the configure vlan esrp esrp-neutral-timeout command.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan esrp group

    configure vlan <vlan name> esrp group <number>

Description
Configures the group number to be used for the ESRP VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the ESRP group to which this VLAN should be added.</td>
</tr>
</tbody>
</table>

Default
The default group number is 0.

Usage Guidelines
Each group runs an instance of ESRP within the same VLAN or broadcast domain. A maximum of four ESRP groups can be defined within the same networked broadcast domain. In addition, a maximum of four distinct ESRP groups can be supported on a single ESRP switch. You can configure a maximum of 32 ESRP groups in a network.

The most typical application for multiple ESRP groups is when two or more sets of ESRP switches are providing fast-failover protection within a common subnet for two or more groups of users. An additional use for ESRP groups is ESRP Host Attach; ESRP VLANs that share ESRP HA ports must be members of different ESRP groups.

Example
The following command configures VLAN esrp-1 to be a member of ESRP group 2:

```bash
configure vlan esrp-1 esrp group 2
```

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan esrp group add esrp-aware-ports

configure vlan <vlan name> esrp group <number> add esrp-aware-ports [all | <portlist>]

Description
Enables selective forwarding on an ESRP-aware VLAN.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-aware VLAN name.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the ESRP group to which this ESRP-aware VLAN belongs.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all of the ports to be configured.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
An ESRP-aware switch floods ESRP PDUs to all ports in an ESRP-aware VLAN and the CPU. This flooding increases the amount of network traffic because all ports receive ESRP PDUs, whether or not they are connected to switches running the same ESRP group. To reduce the amount of traffic, you can select the ports that receive ESRP PDUs by configuring selective forwarding on an ESRP-aware VLAN. By configuring selective forwarding, you create a portlist for the ESRP groups associated with an ESRP-aware VLAN, and that portlist is used for forwarding ESRP PDUs on the relevant ports only.

The ESRP group number must be the same as the ESRP-aware VLAN number.

If you specify the all or portlist options, the ports must be connected to switches running ESRP, and the ports must connect to the ESRP master and slave switches.

When an ESRP-aware switch receives an ESRP PDU, the software will lookup the group to which the PDU belongs and will forward the ESRP PDU to the group’s portlist and the CPU.

Example
The following command configures ESRP-aware VLAN purple to receive ESRP PDUs on ports 1, 2, 3, and 4:

```
configure vlan purple esrp group 1 add esrp-aware-ports 1-4
```

History
This command was first available in ExtremeWare 6.2.2b81.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
Platform Availability

This command is available on all platforms.
configure vlan esrp group delete esrp-aware-ports

configure vlan <vlan name> esrp group <group_number> delete esrp-aware-ports [all | <portlist>]

Description
Disables selective forwarding on an ESRP-aware VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-aware VLAN name.</td>
</tr>
<tr>
<td>group_number</td>
<td>Specifies the ESRP group to which this ESRP-aware VLAN belongs.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all of the ports to be disabled.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
An ESRP-aware switch floods ESRP PDUs to all ports in an ESRP-aware VLAN and the CPU. This flooding increases the amount of network traffic because all ports, regardless if they are connected to switches running the same ESRP group or not, receive ESRP PDUs. To reduce the amount of traffic, you can select the ports that receive ESRP PDUs by configuring selective forwarding on an ESRP-aware VLAN. By configuring selective forwarding, you create a portlist for the ESRP groups associated with an ESRP-aware VLAN, and that portlist is used for forwarding ESRP PDUs on the relevant ports only.

If all ports are removed from the esrp-aware-ports list, selective forwarding is disabled.

Example
The following command disables selective forwarding for ESRP-aware VLAN purple:
configure vlan purple esrp group 1 delete esrp-aware-ports 1-4

History
This command was first available in ExtremeWare 6.2.2b81.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan esrp priority

configure vlan <vlan name> esrp priority <value>

Description
Configures the ESRP priority.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>value</td>
<td>Specifies a number between 0 and 255.</td>
</tr>
</tbody>
</table>

Default
Priority = 0.

Usage Guidelines
The ESRP priority is one of the factors used by the ESRP election algorithm in determining which switch is the Master switch.

The range of the priority value is 0 to 254, with 0 being the lowest priority, 254 being the highest. If the ESRP priority is the determining criteria for the election algorithm, the highest priority value determines which switch will act as master for a particular VLAN.

Setting the priority to 255 configures the switch to slave mode, and to be ineligible to become the master. The switch will remain in slave mode even when the VLAN fails over from the current master. This feature is typically used to ensure a switch cannot become the ESRP master while it is offline for servicing.

Example
The following command configures the ESRP priority to the highest priority on VLAN esrp-1:

```
configure vlan esrp-1 esrp priority 254
```

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vlan esrp timer

configure vlan <vlan name> esrp timer <timervalue> {esrp-nbr-timeout <timeoutvalue>}

Description
Configures the ESRP timer values.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>timervalue</td>
<td>Specifies the number of seconds between keep-alive packets. The range is 1 to 255 seconds.</td>
</tr>
<tr>
<td>esrp-nbr-timeout</td>
<td>Specifies the number of seconds after which an ESRP neighbor times out. The range is 3 to 7650 seconds.</td>
</tr>
</tbody>
</table>

Default
The default timervalue is 2 seconds.
The default neighbor timeout is 3 times the timervalue.

Usage Guidelines
The timer specifies the interval, in seconds, for exchanging keep-alive packets between the ESRP switches for this VLAN. A lower value specifies a more frequent exchange of keep-alive messages, resulting in the faster detection of a failover condition. The timer setting must be configured identically for the VLAN across all participating switches. If your configuration contains more than 2,500 ESRP VLANs and 256,000 FDB entries, we recommend a timer setting greater than 3 seconds.
The neighbor timeout specifies the amount of time that ESRP waits before considering the neighbor down. The timeout value must be at least 3 times, but not more than 30 times the timervalue. Entering a value outside of that range generates an error message.

In a large ESRP configuration, the slave ESRP VLAN might inadvertently become the master ESRP VLAN. This can occur when FDB entries are flushed during a master-slave transition. To avoid this we recommend the general neighbor timeout guidelines listed in Table 29.

Table 29: General neighbor timeout

<table>
<thead>
<tr>
<th>Number of Domains</th>
<th>Number of VLANs</th>
<th>Number of Active ports</th>
<th>Suggested Neighbor Timeout</th>
</tr>
</thead>
<tbody>
<tr>
<td>64</td>
<td>1000</td>
<td>6 or more</td>
<td>&gt; 8</td>
</tr>
<tr>
<td>48 or more</td>
<td>1500</td>
<td>4 or more</td>
<td>&gt; 10</td>
</tr>
<tr>
<td>48 or more</td>
<td>2000</td>
<td>4 or more</td>
<td>&gt; 11</td>
</tr>
</tbody>
</table>

Example
The following command configures the ESRP timer to 3 seconds and the ESRP neighbor timeout to 12 seconds:

configure vlan esrp-1 esrp timer 3 esrp-nbr-timeout 12
**History**

This command was first available in ExtremeWare 4.0.

This command was modified to include the `esrp-nbr-timeout` option in ExtremeWare 6.2.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
disable elrp-client

disable elrp-client

Description
Disables the Extreme Loop Recovery Protocol (ELRP) client (standalone elrp) globally.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
This command disables the ELRP globally so that none of the ELRP VLAN configurations take effect.

The ELRP client must be enabled globally in order for it to work on any VLANs. Use the enable elrp-client command to globally enable the ELRP client.

Example
The following command globally disables the ELRP client:

disable elrp-client

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on all platforms.
disable elsm auto-restart ports

    disable elsm auto-restart ports <portlist>

Description
Disable Extreme Link Status Monitoring (ELSM) auto-restart for the specified ports.

Syntax Description

| portlist | Specifies the ports or slots and ports for which ELSM auto-start is being disabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default
Disabled.

Usage Guidelines
If you have ELSM automatic restart enabled and the port goes down, ELSM automatically brings up the port if it receives the Hello packets from its neighbor.

If you do not have automatic restart enabled, the port goes through the Up, Down, Down-Wait process once. When you first enable ELSM or if you reboot the switch, it goes through the process twice. After it is done with the cycle (or cycles), the port enters the Down-Stuck state.

To enable automatic restart, use the following command:

    enable elsm auto-restart ports <portlist>

To disable automatic restart, use the following command:

    disable elsm auto-restart ports <portlist>

To get out of the Down-Stuck state and enter the Down state, you can use one of the following commands:

    clear elsm auto-restart ports <portlist>
    enable elsm auto-restart ports <portlist>

Example
The following command disables ELSM automatic restart for ports 1-5 on the switch:

    disable elsm auto-restart ports 1-5

History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on “i” series platforms only.
disable elsm ports

    disable elsm ports <portlist>

Description
Disables Extreme Link Status Monitoring (ELSM) protocol for the specified ports.

Syntax Description

| Portlist | Specifies the ports or slots and ports for which ELSM should be disabled. May be in the form 1, 2, 3-5.

Default
Disabled.

Usage Guidelines

The Extreme Link Status Monitoring (ELSM) protocol allows you to detect remote CPU failures in the network. A software or hardware fault might prevent the CPU from transmitting or receiving, leading to the sudden failure of the CPU. If the CPU cannot process or send packets, ELSM isolates the connections to the faulty switch from the rest of the network. If the switch fabric continues to send packets during a CPU failure, the switch may appear to be healthy when it is not.

An Extreme Networks device with ELSM enabled can detect remote CPU failures by exchanging hello packets between two ELSM peers. When ELSM detects a CPU failure as a result of not hearing from its neighbor, it brings down the connection to the neighbor. ELSM operates on a point-to-point basis; you only configure ELSM on the ports that connect to other devices within the network, but you must configure ELSM on both sides of the peer connections.

ELSM ports use hello packets to communicate information about the health of the network to peer ports. The hello packets are received and transmitted by an ELSM-enabled port. The port expects a response from its neighbor after it sends a hello packet.

When you enable ELSM on the specified ports, the ports participate in ELSM with their peers and begin exchanging ELSM hellos. Use the following command to enable ELSM:

    enable elsm ports <portlist>

ELSM works between two connected ports, and each ELSM instance is based on a single port.

When you disable ELSM on the specified ports, the ports no longer send ELSM hellos to its peer and no longer maintain ELSM states.

Example
The following command disables ELSM for ports 1-6 on the switch:

    disable elsm ports 1-6

History
This command was first available in ExtremeWare 6.2.2b1347.3e.
Platform Availability

This command is available on “i” series platforms only.
disable esrp vlan

    disable esrp vlan <vlan name>

**Description**
Disables ESRP on a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
Disabled.

**Usage Guidelines**
None.

**Example**
The following command disables ESRP on the VLAN accounting:

disable esrp vlan accounting

**History**
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
enable elrp-client

Description
Enables the Extreme Loop Recovery Protocol (ELRP) client (standalone elrp) globally.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
The ELRP client must be enabled globally in order for it to work on any VLANs.
The ELRP client can be disabled globally so that none of the ELRP VLAN configurations take effect. Use the disable elrp-client command to globally disable the ELRP client.

Example
The following command globally enables the ELRP client:

```
enable elrp-client
```

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on all platforms.
enable elsm auto-restart ports

    enable elsm auto-restart ports <portlist>

Description
Enable Extreme Link Status Monitoring (ELSM) auto-restart for the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
If you have ELSM automatic restart enabled and the port goes down, ELSM automatically brings up the port if it receives the Hello packets from its neighbor.

If you do not have automatic restart enabled, the port goes through the Up, Down, Down-Wait process once. When you first enable ELSM or if you reboot the switch, it goes through the process twice. After it is done with the cycle (or cycles), the port enters the Down-Stuck state.

To enable automatic restart, use the following command:

    enable elsm auto-restart ports <portlist>

To disable automatic restart, use the following command:

    enable elsm auto-restart ports <portlist>

To get out of the Down-Stuck state and enter the Down state, you can use one of the following commands:

    clear elsm auto-restart ports <portlist>
    enable elsm auto-restart ports <portlist>

Example
The following command enables ELSM automatic restart for ports 1-5 on the switch:

    enable elsm auto-restart ports 1-5

History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on “i” series platforms.
**enable elsm ports**

```
enable elsm ports <portlist>
```

**Description**

Enables Extreme Link Status Monitoring (ELSM) protocol for the specified ports.

**Syntax Description**

| portlist | Specifies the ports or slots and ports for which ELSM should be enabled. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

**Default**

Disabled.

**Usage Guidelines**

The Extreme Link Status Monitoring (ELSM) protocol allows you to detect remote CPU failures in the network. A software or hardware fault might prevent the CPU from transmitting or receiving, leading to the sudden failure of the CPU. If the CPU cannot process or send packets, ELSM isolates the connections to the faulty switch from the rest of the network. If the switch fabric continues to send packets during a CPU failure, the switch may appear to be healthy when it is not.

An Extreme Networks device with ELSM enabled can detect remote CPU failures by exchanging hello packets between two ELSM peers. When ELSM detects a CPU failure as a result of not hearing from its neighbor, it brings down the connection to the neighbor. ELSM operates on a point-to-point basis; you only configure ELSM on the ports that connect to other devices within the network, but you must configure ELSM on both sides of the peer connections.

ELSM ports use hello packets to communicate information about the health of the network to peer ports. The hello packets are received and transmitted by an ELSM-enabled port. The port expects a response from its neighbor after it sends a hello packet.

When you enable ELSM on the specified ports, the ports participate in ELSM with their peers and begin exchanging ELSM hellos.

ELSM works between two connected ports, and each ELSM instance is based on a single port.

When you disable ELSM on the specified ports, the ports no longer send ELSM hellos to its peer and no longer maintain ELSM states. Use the following command to disable ELSM:

```
disable elsm ports <portlist>
```

**Example**

The following command enables ELSM for ports 1-6 on the switch:

```
enable elsm ports 1-6
```
History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on “i” series platforms only.
enable esrp vlan

    enable esrp vlan <vlan name>

Description
Enables ESRP on a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
EDP must be enabled on all ports participating in ESRP.
ESRP cannot be enabled on the VLAN default.

Example
The following command enables ESRP on the VLAN esrp-1:

```
enable esrp vlan esrp-1
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show elrp

    show elrp {<vlan name> | detail}

Description
Displays ESRP information.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies detail for each switch in the ESRP VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If you enter the show elrp command without a keyword, the command displays the:

- Total number of clients registered with ESRP
- ESRP packets transmitted
- ESRP packets received

If you enter the detail keyword, more detailed status information for VLANs in the master and pre-master states is displayed. If you enter a vlan name, the command displays ESRP information for that specific VLAN.

The additional table output for the detail keyword or a specific VLAN name includes the following:

<table>
<thead>
<tr>
<th>Client name</th>
<th>Displays the name of the ESRP client.</th>
</tr>
</thead>
<tbody>
<tr>
<td>VLAN</td>
<td>Displays the name of the VLAN with ESRP enabled.</td>
</tr>
<tr>
<td>Interval</td>
<td>Displays the configured interval. An interval of 3 indicates that ESRP PDUs are transmitted every 3 seconds.</td>
</tr>
<tr>
<td>Count</td>
<td>Lists the configured number of ESRP PDUs that are transmitted. The PDUs are transmitted at the configured interval. This method of ESRP PDU transmission is used by ESRP in the pre-master state. A count of 0 indicates continuous PDU transmission. If the Cyclic value is Yes, the count is always 0.</td>
</tr>
<tr>
<td>Cyclic</td>
<td>Indicates whether ESRP PDUs are being continuously sent. The column shows Yes for the master VLAN because that VLAN is continuously sending ESRP PDUs for loop detection. When a VLAN is in the pre-master state, it only sends three ESRP PDUs before changing to master or slave. During this time the column shows No for that VLAN.</td>
</tr>
<tr>
<td>Pkts-Xmit</td>
<td>Displays the number of ESRP PDUs transmitted.</td>
</tr>
<tr>
<td>Pkts-Rcvd</td>
<td>Displays the number of ESRP PDUs received.</td>
</tr>
</tbody>
</table>
**Example**

The following command displays summary ELRP status information on the switch:

```
show elrp
```

The following sample output is displayed:

```
Number of ELRP Clients          = 1
Number of ELRP pkts transmitted = 69345
Number of ELRP pkts Received    = 150
```

The following command displays detailed ELRP status information on the switch:

```
show elrp detail
```

The following sample output is displayed:

```
Number of ELRP Clients          = 1
Number of ELRP pkts transmitted = 70305
Number of ELRP pkts Received    = 150

<table>
<thead>
<tr>
<th>Client</th>
<th>VLAN</th>
<th>Interval</th>
<th>Count</th>
<th>Cyclic</th>
<th>Pkts-Xmit</th>
<th>Pkts-Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>tEsrpTask</td>
<td>uj-mas64</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas63</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas62</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas61</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas60</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas59</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas58</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas57</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas56</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas55</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas54</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas53</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas52</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas51</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas50</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
<tr>
<td>tEsrpTask</td>
<td>uj-mas49</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
</tbody>
</table>
```

The following command displays the ELRP status information for VLAN *uj-mas*:

```
show elrp uj-mas
```

The following sample output is displayed:

```
<table>
<thead>
<tr>
<th>Client</th>
<th>VLAN</th>
<th>Interval</th>
<th>Count</th>
<th>Cyclic</th>
<th>Pkts-Xmit</th>
<th>Pkts-Rcvd</th>
</tr>
</thead>
<tbody>
<tr>
<td>tEsrpTask</td>
<td>uj-mas</td>
<td>3</td>
<td>0</td>
<td>Yes</td>
<td>1095</td>
<td>0</td>
</tr>
</tbody>
</table>
```

**History**

This command was first available in ExtremeWare 6.2.2b134.

This command was not supported in ExtremeWare 7.0.

This command is supported in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
show elsm

Description
Displays the operational state of the Extreme Link Status Monitoring (ELSM) for all ports on a switch.

Syntax Description
This command has no arguments or variables.

Default
All.

Usage Guidelines
This command displays the following ELSM data for all ports on the switch:

- Port
- Receive State—up, down, down-wait, or down-stuck for each listed port
- Hello time for each listed port

Use the following command to display ELSM data for selected ports on the switch:

```
show elsm ports <portlist>
```

To clear the statistics gathered by ELSM, use the following command:

```
clear elsm counters ports <portlist>
```

Example
The following command displays the operational state of the Extreme Link Status Monitoring (ELSM) for all ports on the switch:

```
show elsm
```

Following is the output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Rx State</th>
<th>Hello Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>9</td>
<td>Up</td>
<td>1</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on “i” series platforms only.
show elsm ports

    show elsm ports <portlist>

Description
Displays the operational state of the Extreme Link Status Monitoring (ELSM) for selected ports on a switch.

Syntax Description

| portlist | Specifies the ports or slots and ports for which the ELSM operational state is being displayed. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8. |

Default
None.

Usage Guidelines
This command displays the following ELSM data for selected ports on the switch:

- Admin state—enabled or disabled
- Upper layer link status—up or down
- Receive State—up, down, down-wait, or down-stuck
- Transmit state—HelloRx+, HelloRx-, Critical Event, Init
- Hello time
- Hold threshold
- Auto-restart
- Receive Hello and Transmit Hello packet counters
- ELSM up/down count

Use the following command to display ELSM data for all ports on the switch:

    show elsm

If ELSM is disabled, only the admin (enabled/disabled) information is displayed.

To clear the statistics gathered by ELSM, use the following command:

    clear elsm counters ports <portlist>

Example
The following command displays the operational state of the Extreme Link Status Monitoring (ELSM) for port 9 on the switch:

    show elsm ports 9

Following is the output from this command:
show elsm ports

ELSM Info Port 9

Admin : Enabled
Upper Layer Link Status : Down
Rx State : Down
Tx State : HelloRx(-)
Hello Time : 1 (second)
Hold Threshold : 2
Auto Restart : Enabled
Rx Hello+ : 0
Rx Hello- : 0
Tx Hello+ : 0
Tx Hello- : 0
ELSM Up/Down Count : Up 0 Down 0

History
This command was first available in ExtremeWare 6.2.2b134.

Platform Availability
This command is available on “i” series platform only.
show esrp

    show esrp {detail}

Description
Displays ESRP configuration information.

Syntax Description

| detail | Specifies detail for each switch in the ESRP VLAN. |

Default
Shows summary ESRP information.

Usage Guidelines
This command shows information about the state of an ESRP VLAN and its neighbors. This includes information about tracked devices.

In addition to ESRP information, ELRP status information is also displayed. This includes information about the master and pre-master states, number of transitions to the pre-master state, and the ports where ELRP is disabled.

This command also displays ESRP hitless failover statistics.

The output varies depending upon the configuration and the state of the switch. The following output applies to all platforms:

- **Standby switch**—Information about the impending failover and the timeout is displayed
- **none**—Information about not participating in hitless failover is displayed

The following output applies only to “i” series platforms:

- **Layer 3 tracking in use and the failover mode is remain-esrp-master-in-l2-domain**—Information about rapid reelection and layer 3 tracking is displayed
- **Layer 3 tracking is not in use and the failover mode is remain-esrp-master-in-l2-domain**—Information about remaining the master is displayed
- **rapid-reelection**—Information about rapid reelection is displayed

Example
The following command displays summary ESRP status information for the VLANs on the switch:

```
show esrp
```

It produces output similar to the following:

```
VLAN Name VID Virtual IP/IPX  State Master MAC Addr NbrPri/Gr/Prt/In/TR/TP/T
uj-mas1 0001 192.169.1.1  Master  00:E0:2B:80:E6:00  1
070/10/004/00/01/00/02
```

Nbr - Number of Neighbors, Pri - Priority In Use, Gr - Group
Prt - Number of ActivePorts, In - Internal Ports, TR - Tracked Rt/Ping/LSP
TP - Tracked Ports, T - Hello Time.

The following command displays detailed ESRP status information for the VLANs on the switch:

```
show esrp detail
```

It produces output similar to the following:

```
VLAN Interface(Layer 2): demo_esrp
  Priority:               0 (Priority In Use: 0)
  Active Ports:           2
  Internal Ports:         0
  Tracked Rt/Ping/LSP:    0
  Tracked Ports:          0
  Tracked Diag:           -
  Tracked Env:            -
  Tracked RIP:            -
  Tracked OSPF:           -
  Tracked BGP:            -
  Tracked LSP:            None
  ELRP in Premaster(Int, Cnt): Enabled(1, 3)
  ELRP in Master(Int):    Enabled(1)
  Election Algorithm:     ports-track-priority-mac
  Group:                  0
  Hello Timer:            2
  Esrp Nbr Timeout:       6
  Premaster Timeout:      6
  State:                  Enabled(Slave) on Mon Jun 2 10:09:48 2003
  State Trans Counters:   ToMaster:(1)    ToPremaster:(1) ToSlave:(2)

  Host (Direct-Attach) ports : None
  No-count ports: None
  Restart Ports: None
  Tracked VLANs: None
  Tracked Ip Routes: None
  Tracked Pings/Freq/N_miss:
    192.12.1.1/5/2*
  Neighbours:
    [1]  Nbr Active Ports:          3
         Nbr Internal Ports:        0
         Nbr Tracked Rt/Ping/LSP:   0
         Nbr Tracked Ports:         0
         Nbr Priority:              0
         Nbr MacID:                  00:01:30:33:28:00
         Nbr HelloTimer:             2
         Nbr ESRP State:             Master
```

**History**

This command was first available in ExtremeWare 4.0.

This command was updated to support ELRP data in ExtremeWare 6.2.2b134 and ExtremeWare 7.1.0. ELRP data is not displayed in ExtremeWare 7.0.

This command was updated to support ESRP hitless failover statistics in ExtremeWare 7.1.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
show esrp vlan

    show esrp vlan <vlan name> {counters}

Description
Displays ESRP configuration information for a specific VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>counters</td>
<td>Displays ESRP counters.</td>
</tr>
</tbody>
</table>

Default
Displays summary ESRP and ELRP information for the VLAN.

Usage Guidelines
None.

Example
The following command displays ESRP status information for ESRP-enabled VLAN demo-esrp:

    show esrp vlan demo-esrp

It produces output similar to the following:

VLAN Interface(Layer 2): demo_esrp
    Priority: 0 (Priority In Use: 0)
    Active Ports: 2
    Internal Ports: 0
    Tracked Rt/Ping/LSP: 0
    Tracked Ports: 0
    Tracked Diag: -
    Tracked Env: -
    Tracked RIP: -
    Tracked OSPF: -
    Tracked BGP: -
    Tracked LSP: None
    ELRP in Premaster(Int, Cnt):Enabled(1, 3)
    ELRP in Master(Int): Enabled(1)
    Election Algorithm: ports-track-priority-mac
    Group: 0
    Hello Timer: 2
    Esrp Nbr Timeout: 6
    Premaster Timeout: 6
    State: Enabled(Slave) on Mon Jun 2 10:09:48 2003
    State Trans Counters: ToMaster:(1) ToPremaster:(1) ToSlave:(2)

    Host (Direct-Attach) ports : None
    No-count ports: None
    Restart Ports: None
Tracked VLANs: None
Tracked Ip Routes: None
Tracked Pings/Freq/N_miss: 192.12.1.1/5/2*
Neighbours:
[1] Nbr Active Ports: 3
    Nbr Internal Ports: 0
    Nbr Tracked Rt/Ping/LSP: 0
    Nbr Tracked Ports: 0
    Nbr Priority: 0
    Nbr MacID: 00:01:30:33:28:00
    Nbr HelloTimer: 2
    Nbr ESRP State: Master

The following command displays the ESRP counters for ESRP-enabled VLAN demo-esrp:
show esrp vlan demo-esrp counters

It produces output similar to the following:

VLAN=demo_esrp Current-time: Mon Jun 2 08:40:15 2003
Rx-Esrp-Pkts=0  Tx-Esrp-Pkts=0
Rx-Aware-Esrp-Pkts=0, Rx-Elrp-Pkts=0

History
This command was first available in ExtremeWare 6.0.
This command was updated to support ELRP data in ExtremeWare 6.2b134 and ExtremeWare 7.1.0. ELRP data is not displayed in ExtremeWare 7.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show esrp-aware vlan

    show esrp-aware vlan <vlan name>

**Description**
Displays ESRP-aware information for a specific VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
Displays summary information for the VLAN.

**Usage Guidelines**
The display includes the group number, MAC address for the master of the group, and age of the information.

**Example**
The following command displays ESRP-aware status information for ESRP-aware VLAN demo-esrp-aware:

```
show esrp-aware vlan demo-esrp-aware
```

On an ESRP-aware switch, it produces output similar to the following:

```
Summit48i:24 # sh esrp-aware
VLAN Interface: [demo-esrp-aware]. DisableLearnTimeout=0 secs, Total-Fdb-Flushes=6
    Last EsrpAware Fdb-Flush on Mon Nov 18 05:22:26 2002
    Esrp-Group:0  Esrp-Master-Mac=00:01:30:08:36:00,  Age=1 secs
```

**History**
This command was first available in ExtremeWare 6.2.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
show esrp-aware-ports

    show esrp-aware-ports {vlan <vlan name>}

Description
Displays the ESRP-aware VLAN(s), the ESRP group(s), and the ESRP-aware port(s) that receive ESRP PDUs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
To reduce the amount of traffic, you can select the ports that receive ESRP PDUs by configuring selective forwarding on ESRP-aware VLANs. By configuring selective forwarding, you create a portlist of the ESRP groups associated with an ESRP-aware VLAN, and that portlist is used for forwarding ESRP PDUs on the relevant ports only. Use the `show esrp-aware-ports` command to view the ESRP group portlist that forwards ESRP PDUs.

Example
The following command displays selective forwarding statistics:

```
show esrp-aware-ports
```

The `show esrp-aware-ports` command produces output similar to the following:

```
VLAN tt
-------
ESRP Group 0: 1:2 1:1
```

History
This command was first available in ExtremeWare 6.2.2b81.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
unconfigure elrp-client

    unconfigure elrp-client <vlan name>

Description
Disables a pending one-shot or periodic ELRP request for the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>vlan name</th>
<th>Specifies a VLAN name.</th>
</tr>
</thead>
</table>

Default
None.

Usage Guidelines
This command disables a pending one-shot or periodic ELRP request for the specified VLAN.

Use the configure elrp-client one-shot command to configure non-periodic, one-time transmission of ELRP packets. Use the configure elrp-client periodic command to configure periodic transmission of ELRP packets.

The ELRP client must be enabled globally in order for it to work on any VLANs. Use the enable elrp-client command to globally enable the ELRP client.

The ELRP client can be disabled globally so that none of the ELRP VLAN configurations take effect. Use the disable elrp-client command to globally disable the ELRP client.

Example
The following command disables a pending ELRP request on VLAN elrp1:

    unconfigure elrp-client elrp1

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on all platforms.
19 VRRP Commands

This chapter describes the following commands:

- Commands for enabling and disabling Virtual Router Redundancy Protocol (VRRP)
- Commands for performing basic VRRP configuration

**NOTE**

Commands for enabling and disabling port restart and enabling and disabling failure tracking for VRRP are described in Chapter 14, covering ESRP commands.

Like ESRP, VRRP is a protocol that allows multiple switches to provide redundant routing services to users. A virtual router is a group of one or more physical devices that acts as the default gateway for hosts on the network. The virtual router is identified by a virtual router identifier (VRID) and an IP address. All of the VRRP routers that participate in the virtual router are assigned the same VRID.

The Extreme Networks VRRP implementation is compliant with RFC 2338, Virtual Router Redundancy Protocol.

The following points pertain to VRRP:

- VRRP packets are encapsulated IP packets.
- The VRRP multicast address is 224.0.0.18.
- The virtual router MAC address is 00 00 5E 00 01 <vrid>
- An interconnect link between VRRP routers should not be used, except when VRRP routers have hosts directly attached.
- A maximum of 64 VRID instances are supported on the “e” series switches and a maximum of 128 VRID instances are supported on the “i” series switches.
- Up to 4 unique VRIDs can be configured on an interface. VRIDs can be re-used, but not on the same interface.
- VRRP and Spanning Tree can be simultaneously enabled on the same switch.
- On “e” series switches, VRRP and ESRP cannot be simultaneously enabled on the same switch.

VRRP uses an election algorithm to dynamically assign responsibility for the master router to one of the VRRP routers on the network. A VRRP router is elected master if one of the following is true:

- The router is the IP address owner (router that has the IP address of the virtual router configured as its real interface address).
• The router is configured with the highest priority (the range is 1 - 255).

If the master router becomes unavailable, the election process provides dynamic failover and the backup router that has the highest priority assumes the role of master.

A new master is elected when one of the following things happen:
• VRRP is disabled on the master router.
• Communication is lost between master and backup router(s). The master router sends periodic advertisements to the backup routers to indicate that it is alive.

VRRP also supports the following tracking options:
• VRRP VLAN tracking
• VRRP route table tracking
• VRRP ping tracking

If a tracking option is enabled, and the object being tracked becomes unreachable, the master device will fail over. These tracking features are documented in the chapter on ESRP.

VRRP also supports port restart. Like the tracking features, the commands to enable and disable this feature are described in the chapter on ESRP.
configure vrrp add vlan

    configure vrrp add vlan <vlan name>

Description
Enables VRRP on a particular VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None.

Example
The following enables VRRP on VLAN vrrp-1:
configure vrrp add vlan vrrp-1

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vrrp delete

configure vrrp delete [vlan <vlan name> | all]

Description
Disables VRRP on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN on which to disable VRRP.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that VRRP should be disabled on all VLANs on this device.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command disables VRRP on VLAN vrrp-1:

configure vrrp delete vlan vrrp-1

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vrrp vlan add

```bash
configure vrrp vlan <vlan name> add [master | backup] vrid <number> <ip address>
```

**Description**
Configures the VRID instance on the VRRP VLAN as master or backup.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VRRP VLAN.</td>
</tr>
<tr>
<td>master</td>
<td>Specifies that this device is the master router for the virtual router.</td>
</tr>
<tr>
<td>backup</td>
<td>Specifies that this device is a backup router for this VLAN.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a Virtual Router ID (VRID). Value can be in the range of 1-255.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the virtual router in which this device participates.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
The IP address must be the same on all VRRP routers that make up the virtual router for this VLAN. If the IP address is the same as the actual interface address of the device, this device is the IP address owner, and is automatically elected as the master router as long as it remains functional.

**Example**
The following command sets up this device as the master router for VLAN `vrrp-1`, using IP address 192.168.1.3 as the virtual router IP address:

```
configure vrrp vlan vrrp-1 add master vrid 1 192.168.1.3
```

**History**
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available on all platforms.
configure vrrp vlan authentication

configure vrrp vlan <vlan name> authentication [none | simple-password <simple password>]

Description
Configures VRRP authentication.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VRRP VLAN.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no password is required.</td>
</tr>
<tr>
<td>simple password</td>
<td>Specifies the password for VRRP authentication. The maximum password length is eight characters.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
VRRP authentication occurs when VRRP protocol exchanges are authenticated using the configured password. VRRP authentication can be used in networks with the high risk of local attacks to protect against accidental misconfiguration of routers in a local area network (LAN).

Example
The following command configures authentication for VRRP VLAN vrrp-1 with the password newvrrp:

configure vrrp vlan vrrp-1 authentication simple-password newvrrp

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
configure vrrp vlan delete vrid

configure vrrp vlan <vlan name> delete vrid [<number> | all]

Description
Deletes one or all VRIDs.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VRRP VLAN.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a Virtual Router ID (VRID). Value can be in the range of 1-255.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all virtual routers should be deleted for this VLAN on this device.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command deletes the virtual router identified by VRID 2:

```
configure vrrp vlan vrrp-1 delete vrid 2
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
**configure vrrp vlan vrid**

configure vrrp vlan <vlan name> vrid <number> [priority <priority_number> | advertisement-interval <ad_interval_number> | dont_preempt | preempt]

**Description**
Configures VRRP parameters.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VRRP VLAN.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a Virtual Router ID (VRID). Value can be in the range of 1-255.</td>
</tr>
<tr>
<td>priority_number</td>
<td>Specifies the priority value to be used by this VRRP router in the master election process. Value is 1 - 254. The default value is 100.</td>
</tr>
<tr>
<td>ad_interval_number</td>
<td>Specifies the time interval between advertisements, in seconds. Value is 1 - 255. The default value is 1 second.</td>
</tr>
<tr>
<td>dont_preempt</td>
<td>Specifies that this router, as master, may not be preempted by a higher priority backup router.</td>
</tr>
<tr>
<td>preempt</td>
<td>Specifies that this router, as master, may be preempted by a higher-priority backup router. This is the default.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command may be used to configure a VRRP router priority, advertisement interval, and preempt mode.

The priority is used to determine which VRRP router takes over when the master fails over. A value of 255 is reserved for the router that is configured with the virtual router IP address (the IP address owner). A value of 0 is reserved for the master router’s use to indicate it is releasing responsibility for the virtual router.

The advertisement interval specifies the interval between advertisements sent by the master router to inform the backup routers that it is alive. The master down interval is the interval that a backup router waits after the last received advertisement before it determines that the master router is down.

If you have an extremely busy CPU, a short dual master situation can occur. To avoid this, increase the advertisement interval.

The preempt mode controls whether a higher priority backup router preempts a lower priority master. preempt allows preemption. dont_preempt prohibits preemption. The default setting is preempt. The router that owns the virtual router IP address always preempts, independent of the setting of this parameter.

**Example**
The following commands set a priority and advertisement interval for the VRRP router on VLAN vrrp-1, and sets the preempt mode to disallow preemption:
configure vrrp vlan vrrp-1 vrid 2 priority 200
configure vrrp vlan vrrp-1 vrid 2 advertisement-interval 15
configure vrrp vlan vrrp-1 vrid 2 dont_preempt

**History**

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on all platforms.
disable vrrp

disable vrrp

Description
Disables VRRP on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This disables VRRP on the device. All virtual routers defined on this device will also be disabled. If you enable VRRP again, it is not necessary to enable virtual routers again individually.

Example
The following command disables VRRP on the device:

disable vrrp

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
enable vrrp

Description
Enables VRRP on the switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
IGMP snooping must be enabled for VRRP to operate correctly. Use the following command to enable IGMP snooping:

```
enable igmp snooping
```

Example
The following command enables VRRP on this device:

```
enable vrrp
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show vrrp

    show vrrp [vlan <vlan name> | all] {detail}

Description
Displays VRRP configuration information for one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Specifies the name of a VRRP VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that information should be displayed for all VLANs.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies detail information.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use the detail option for detailed tracking information and the VRRP state transition counters.

Example
The following command displays summary status information for VRRP:

    show vrrp

It produces output similar to the following:

VRRP Router: Enabled
    VLAN Name VRID Pri Virtual IP Addr State Master Mac Addr Prt/TR/TPr/W/M/T
demo_vr(En) 0001 100 192.168.1.1      MSTR 00:00:5E:00:01:01   1  0 0 Y Y 1
En-Enabled, Ds-Disabled, Pri-Priority, T-Advert Timer, M-Preempt
    Prt-Active Ports, TR-Tracked Routes/Pings, TPr-Tracked Ports, W-TrackWinner

The following command displays detail status information for VRRP:

    show vrrp detail

It produces output similar to the following:

VRRP Router: Enabled
    Vlan:demo_vrrp IpAddress Owner=192.168.1.2 Vrrp:ENABLED Router:ENABLED
    Authentication: None
    Tracked VLANs: -
    Tracked Ip Routes: -
    Tracked Pings/Freq/N_miss: -
    Tracked Diag: -
    Tracked Env: -
    Track Winner: Yes
1) Backup-Vrid:1 Virtual-IP:192.168.1.1 Priority:100
    Active Ports:1, Advert-Interval:1, Preempt:Yes
    State:MASTER on Wed Jan 23 10:17:42 2002
    Transition Counters: ToMaster:1 ToBackup:1
    Skew:0.609375 Master-Dn-Int:3.60938
History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
show vrrp vlan stats

    show vrrp vlan <vlan name> stats

Description
Displays VRRP statistics for a particular VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VRRP VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to show the statistics or counters for the VRRP protocol for a VLAN.

Example
The following command displays statistics for VLAN v1:

```
show vrrp vlan v1 stats
```

It produces output similar to the following:

```
VLAN v1
    Chksum Err:0, Ver Err:0, VRID Err:0, Auth Mismatch:0, Pkt-len Err:0
    Become Master:2, Adv recv:0, Adv Err:0, Auth Fail:0, TTL Err:0
    Pri-0-recv:0, Pri-0-snt:1, Addr-List Err:0, Invalid Auth Err:0
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on all platforms.
Extreme Networks switches provide full layer 3, IP unicast routing. They exchange routing information with other routers on the network using either the Routing Information Protocol (RIP) or the Open Shortest Path First (OSPF) protocol. The switches dynamically build and maintain routing tables and determine the best path for each of its routes.

Each host that uses the IP unicast routing functionality of the switch must have a unique IP address assigned. In addition, the default gateway assigned to the host must be the IP address of the router interface.

The routing software and hardware directs IP traffic between router interfaces. A router interface is simply a VLAN that has an IP address assigned to it.

As you create VLANs with IP addresses belonging to different IP subnets, you can also choose to route between the VLANs. The VLAN switching and IP routing functions occur within the switch.

Each IP address and mask assigned to a VLAN must represent a unique IP subnet. You cannot configure the same IP subnet on different VLANs.

The Extreme Networks switch maintains an IP routing table for network routes and host routes. The table is populated from the following sources:

- Dynamically, by way of routing protocol packets or by ICMP redirects exchanged with other routers
- Statically, by way of routes entered by the administrator
  - Default routes, configured by the administrator
  - Locally, by way of interface addresses assigned to the system
  - By other static routes, as configured by the administrator

Dynamic routes are typically learned by way of RIP or OSPF. Routers that use RIP or OSPF exchange information in their routing tables in the form of advertisements. Using dynamic routes, the routing table contains only networks that are reachable.

Dynamic routes are aged out of the table when an update for the network is not received for a period of time, as determined by the routing protocol.

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure up to 64 static unicast routes on the switch.

Static routes can also be used for security reasons, to control which routes you want advertised by the router. Static routes are never aged out of the routing table.
A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

When there are multiple, conflicting choices of a route to a particular destination, the router picks the route with the longest matching network mask. If these are still equal, the router picks the route using the following criteria (in the order specified):

- Directly attached network interfaces
- ICMP redirects
- Static routes
- Directly attached network interfaces that are not active

If you define multiple default routes, the route that has the lowest metric is used. If there are multiple default routes that have the same lowest metric, the system picks one of the routes.

You can also configure blackhole routes—traffic to these destinations is silently dropped.

Internet Control Message Protocol (ICMP) is used to transmit information needed to control IP traffic. It is used mainly to provide information about routes to destination addresses. ICMP redirect messages inform hosts about more accurate routes to other systems, whereas ICMP unreachable messages indicate problems with a route.

Additionally, ICMP can cause TCP connection to terminate gracefully if the route becomes unavailable.

After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being service by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95.

UDP-forwarding is a flexible and generalized routing utility for handling the directed forwarding of broadcast UDP packets. UDP-forwarding allows applications, such as multiple DHCP relay services from differing sets of VLANs, to be directed to different DHCP servers. The following rules apply to UDP broadcast packets handled by this feature:

- If the UDP profile includes BOOTP or DHCP, the packet is handled according to guidelines in RFC 1542.
- If the UDP profile includes other types of traffic, these packets have the IP destination address modified as configured, and changes are made to the IP and UDP checksums and decrements to the TTL field, as appropriate.

If the UDP-forwarding is used for BOOTP or DHCP forwarding purposes, do not configure or use the existing bootprelay function. However, if the previous bootprelay functions are adequate, you can continue to use them.

To configure UDP-forwarding, you must first create a UDP-forward destination profile. The profile describes the types of UDP packets (by port number) that are used and where they are to be forwarded. You must give the profile a unique name, in the same manner as a VLAN, protocol filter, or Spanning Tree Domain (STD).

Next, configure a VLAN to make use of the UDP-forwarding profile. As a result, all incoming traffic from the VLAN that matches the UDP profile is handled as specified in the UDP-forwarding profile.

A maximum of 10 UDP-forwarding profiles can be defined. Each named profile may contain a maximum of eight “rules” defining the UDP port, and destination IP address or VLAN. A VLAN can
use a single UDP-forwarding profile. UDP packets directed toward a VLAN use an all-ones broadcast on that VLAN.

Proxy Address Resolution Protocol (ARP) was first developed so that ARP-capable devices could respond to ARP Request packets on behalf of ARP-incapable devices. Proxy ARP can also be used to achieve router redundancy and simplify IP client configuration. The Extreme Networks switch supports proxy ARP for this type of network configuration.

Once IP ARP is configured, the system responds to ARP Requests on behalf of the device, as long as the following conditions are satisfied:

- The valid IP ARP Request is received on a router interface.
- The target IP address matches the IP address configured in the proxy ARP table.
- The proxy ARP table entry indicates that the system should always answer this ARP Request, regardless of the ingress VLAN (the `always` parameter must be applied).

After all the proxy ARP conditions have been met, the switch formulates an ARP Response using the configured MAC address in the packet.

In some networks, it is desirable to configure the IP host with a wider subnet than the actual subnet mask of the segment. Proxy ARP can be used so that the router answers ARP Requests for devices outside of the subnet. As a result, the host communicates as if all devices are local. In reality, communication with devices outside of the subnet are proxied by the router.
clear iparp

clear iparp {<ip address> | vlan <vlan name>}

Description
Removes dynamic entries in the IP ARP table.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Permanent IP ARP entries are not affected.

Example
The following command removes a dynamically created entry from the IPARP table:

clear iparp 10.1.1.5/24

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
clear ipfdb

    clear ipfdb {<ip address> <netmask> | vlan <vlan name>}

**Description**
Removes the dynamic entries in the IP forwarding database.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
If no options are specified, all IP FDB entries are removed.

**Example**
The following command removes dynamically created entries in the IP forwarding database:

clear ipfdb 10.1.2.1/24

**History**
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure bootprelay add

configure bootprelay add <ip address>

Description
Configures the addresses to which BOOTP requests should be directed.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   
   ```
   enable bootprelay
   ```
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:
   
   ```
   configure bootprelay add <ip address>
   ```

Example
The following command configures BOOTP requests to be directed to 123.45.67.8:

```
configure bootprelay add 123.45.67.8
```

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure bootprelay delete

configure bootprelay delete [<ip address> | all]

Description
Removes one or all IP destination addresses for forwarding BOOTP packets.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all IP address entries.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   `enable bootprelay`
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:
   `configure bootprelay add <ip address>`

Example
The following command removes the destination address:
`configure bootprelay delete 123.45.67.8`

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure bootprelay dhcp-agent information check

configure bootprelay dhcp-agent information check

Description
Enables the Dynamic Host Configuration Protocol (DHCP) relay agent option (option 82) information checking in the DHCP reply packet.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
After IP unicast routing has been configured, you can configure the switch to forward DHCP or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets.

To configure the relay function and enable relay agent information checking in the DHCP reply packet, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   ```
   enable bootprelay
   ```
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:
   ```
   configure bootprelay add <ip address>
   ```
4. Configure the DHCP relay agent option (option 82), using the following command:
   ```
   configure bootprelay dhcp-agent information option
   ```
5. Configure the option 82 check, using the following command:
   ```
   configure bootprelay dhcp-agent information check
   ```

To disable the DHCP relay agent information checking in the DHCP reply packet, use the following command:

```
unconfigure bootprelay dhcp-agent information check
```

Example
The following command configures DHCP relay agent option check:

```
configure bootprelay dhcp-agent information check
```
This command was added to the “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure bootprelay dhcp-agent information option

configure bootprelay dhcp-agent information option

Description
Enables the Dynamic Host Configuration Protocol (DHCP) relay agent option (option 82).

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
After IP unicast routing has been configured, you can configure the switch to forward DHCP or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets.

To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   ```
   enable bootprelay
   ```
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:
   ```
   configure bootprelay add <ip address>
   ```
4. Configure the DHCP relay agent option (option 82), using the following command:
   ```
   configure bootprelay dhcp-agent information option
   ```

To disable the DHCP relay agent option (option 82), use the following command:

```
unconfigure bootprelay dhcp-agent information option
```

Example
The following command configures the DHCP relay agent option:

```
configure bootprelay dhcp-agent information option
```

History
This command was available in ExtremeWare 7.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.
Platform Availability
This command is available on all platforms.
configure bootprelay dhcp-agent information policy

configure bootprelay dhcp-agent information policy <policy>

**Description**

Configures the Dynamic Host Configuration Protocol (DHCP) relay agent reforwarding policy.

**Syntax Description**

<table>
<thead>
<tr>
<th>policy</th>
<th>Configures the policy according to one of the following values:</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop</td>
<td>Drops the DHCP request if agent information is present in the DHCP request.</td>
</tr>
<tr>
<td>keep</td>
<td>Keeps the agent information if agent information is present in the DHCP request.</td>
</tr>
<tr>
<td>replace</td>
<td>Replaces the existing relay agent information with its own information if agent information is present in the DHCP request.</td>
</tr>
</tbody>
</table>

**Default**

Replace

**Usage Guidelines**

After IP unicast routing has been configured, you can configure the switch to forward DHCP or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets.

To configure the relay function and the relay agent reforwarding policy, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   ```
   enable bootprelay
   ```
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:
   ```
   configure bootprelay add <ip address>
   ```
4. Configure the DHCP relay agent option (option 82), using the following command:
   ```
   configure bootprelay dhcp-agent information option
   ```
5. Configure the DHCP relay agent reforwarding policy, using the following command:
   ```
   configure bootprelay dhcp-agent information policy <policy>
   ```

To disable the DHCP relay agent reforwarding policy, using the following command:

```
unconfigure bootprelay dhcp-agent information policy
```
**History**
This command was available in ExtremeWare 7.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure ip-down-vlan-action

configure ip-down-vlan-action [consume | drop | forward]

Description
Configures the forwarding functionality destined to nonworking IP interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>consume</td>
<td>Specifies the consume function.</td>
</tr>
<tr>
<td>drop</td>
<td>Specifies the drop function.</td>
</tr>
<tr>
<td>forward</td>
<td>Specifies the forwarding function.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command configures the forwarding functionality destined to nonworking IP interfaces:

```
configure ip-down-vlan-action forward
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure iparp add

    configure iparp add <ip address> <mac_address>

Description

Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

Add a permanent IP ARP entry to the system. The ip address is used to match the IP interface address to locate a suitable interface.

Example

The following command adds a permanent IP ARP entry to the switch for IP address 10.1.2.5:

```
configure iparp add 10.1.2.5 00:11:22:33:44:55
```

History

This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability

This command is available on all platforms.
configure iparp add proxy

    configure iparp add proxy <ip address> {<mask>} {<mac_address>} {always}

Description

Configures the switch to respond to ARP Requests on behalf of devices that are incapable of doing so. Up to 64 proxy ARP entries can be configured.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address.</td>
</tr>
<tr>
<td>always</td>
<td>Specifies all ARP Requests.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

When mask is not specified, an address with the mask 255.255.255.255 is assumed. When mac_address is not specified, the MAC address of the switch is used in the ARP Response. When always is specified, the switch answers ARP Requests without filtering requests that belong to the same subnet of the receiving router interface and specifying a MAC address becomes optional.

After IP ARP is configured, the system responds to ARP Requests on behalf of the device as long as the following conditions are satisfied:

- The valid IP ARP Request is received on a router interface.
- The target IP address matches the IP address configured in the proxy ARP table.
- The proxy ARP table entry indicates that the system should always answer this ARP Request, regardless of the ingress VLAN (the always parameter must be applied).

After all the proxy ARP conditions have been met, the switch formulates an ARP Response using the configured MAC address in the packet.

Example

The following command configures the switch to answer ARP Requests for all devices with the address range of 100.101.45.1 to 100.101.45.255:

```
configure iparp add proxy 100.101.45.0/24
```

History

This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
configure iparp delete

configure iparp delete <ip address>

Description
Deletes an entry from the ARP table. Specify the IP address of the entry.

Syntax Description

| ip address | Specifies an IP address. |

Default
N/A

Usage Guidelines
Removes any IP ARP entry (dynamic or permanent) from the table. The ip address is used to match the IP interface address to locate a suitable interface.

Example
The following command deletes an IP address entry from the ARP table:
configure iparp delete 10.1.2.5

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iparp delete proxy

configure iparp delete proxy [<ip address> {<mask>} | all]

**Description**

Deletes one or all proxy ARP entries.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ARP entries.</td>
</tr>
</tbody>
</table>

**Default**

Not Always.

**Usage Guidelines**

Proxy ARP can be used for two purposes:

1. To support host that cannot process ARP traffic. In this case, the switch answers the ARP Request for that host.

2. To hide the IP topology from the host. The network administrator can configure a large network on the host machine (16-bit mask) and a smaller network on each router interface (for example, 22-bit mask). When the host sends ARP Request for another host on another subnet, the switch answers the ARP Request and all subsequent traffic will be sent directly to the router.

You can configure up to 64 proxy ARP entries. When the mask is not specified, then software will assume a host address (that is, a 32-bit mask). When the MAC address is not specified, then the software uses the switch’s MAC address as the proxy host. Always should be specified for type-1 usage, not always is the default (type-2).

**Example**

The following command deletes the IP ARP proxy entry 100.101.45.0/24:

```
configure iparp delete proxy 100.101.45.0/24
```

**History**

This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
configure iparp max-entries

configure iparp max-entries <number>

Description
Configures the maximum allowed IP ARP entries.

Syntax Description

| number | Specifies a number of maximum IP ARP entries. |

Default
4096

Usage Guidelines
Range: 1 - 20480. The maximum IP ARP entries include dynamic, static, and incomplete IP ARP entries.

Example
The following command sets the maximum IP ARP entries to 2000 entries:

```configure iparp max-entries 2000```

History
This command was first available in ExtremeWare 6.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure iparp max-pending-entries

configure iparp max-pending-entries <number>

Description
Configures the maximum allowed incomplete IP ARP entries.

Syntax Description

| number | Specifies a number of maximum IP ARP entries. |

Default
256

Usage Guidelines
Range: 1 - 20480, but cannot be greater than the configured IP ARP max-entries value.

Example
The following command sets the maximum IP ARP entries to 500 entries:
configure iparp max-pending-entries 500

History
This command was first available in ExtremeWare 6.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure iparp timeout

configure iparp timeout <minutes>

**Description**

Configures the IP ARP timeout period.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>minutes</td>
<td>Specifies a time in minutes.</td>
</tr>
</tbody>
</table>

**Default**

20 minutes

**Usage Guidelines**

A setting of 0 disables ARP aging.

**Example**

The following command sets the IP ARP timeout period to 10 minutes:

```
configure iparp timeout 10
```

**History**

This command was first available in ExtremeWare 4.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
configure ipfdb route-add

    configure ipfdb route-add [clear-all | clear-subnet]

**Description**
Specifies which routes are deleted and reinstalled with a new gateway.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>clear-all</td>
<td>Clears all IPFDB entries associated with a route if a more specific route is installed.</td>
</tr>
<tr>
<td>clear-subnet</td>
<td>Clears only the IPFDB entries associated with the new route’s subnet.</td>
</tr>
</tbody>
</table>

**Default**
The default is clear-all.

**Usage Guidelines**
To see the current setting, use the `show ipconfig` command.

**Example**
The following command clears only the IPFDB entries associated with the new route’s subnet:

```
configure ipfdb route-add clear-subnet
```

**History**
This command was first available in ExtremeWare 7.0.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure iproute add

    configure iproute add <ip address> <mask> <gateway> <metric>

Description
Adds a static address to the routing table.

Syntax Description

| ip address | Specifies an IP address. |
| mask       | Specifies a subnet mask. |
| gateway    | Specifies a VLAN gateway. |
| metric     | Specifies a cost metric. |

Default
N/A

Usage Guidelines
Use a value of 255.255.255.255 for mask to indicate a host entry.

Example
The following command adds a static address to the routing table:

    configure iproute add 10.1.1.1/24 123.45.67.1 5

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iproute add blackhole

configure iproute add blackhole <ip address> <mask>

Description
Adds a blackhole address to the routing table. All traffic destined for a configured blackhole IP address is silently dropped, and no Internet Control Message Protocol (ICMP) message is generated.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
A blackhole entry configures packets with a specified MAC destination address to be discarded. Blackhole entries are useful as a security measure or in special circumstances where a specific destination address must be discarded. Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged out of the forwarding database (FDB).

Example
The following command adds a blackhole address to the routing table for packets with a destination address of 100.101.145.4:

```
configure iproute add blackhole 100.101.145.4
```

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iproute add blackhole default

configure iproute add blackhole default

Description
Adds a default blackhole route to the routing table. All traffic destined for an unknown IP destination is silently dropped, and no Internet Control Message Protocol (ICMP) message is generated.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
While a default route is for *forwarding* traffic destined to an unknown IP destination, and a blackhole route is for *discarding* traffic destined to a specified IP destination, a *default blackhole* route is for *discarding* traffic to the unknown IP destination.

Using this command, all traffic with an unknown destination is discarded. If there is another static default route existing in the routing table, the blackhole default route takes higher route priority.

The default blackhole route is treated like a permanent entry in the event of a switch reset or power off/on cycle. The default blackhole route’s origin is “b” or “blackhole” and the gateway IP address for this route is 0.0.0.0.

Example
The following command adds a blackhole default route into the routing table:

```command
configure iproute add blackhole default
```

History
This command was first available in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure iproute add default

configure iproute add default <gateway> {<metric>}

Description
Adds a default gateway to the routing table.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway</td>
<td>Specifies a VLAN gateway</td>
</tr>
<tr>
<td>metric</td>
<td>Specifies a cost metric. If no metric is specified, the default of 1 is used.</td>
</tr>
</tbody>
</table>

Default
If no metric is specified, the default metric of 1 is used.

Usage Guidelines
Default routes are used when the router has no other dynamic or static route to the requested destination. A default gateway must be located on a configured IP interface. Use the unicast-only or multicast-only options to specify a particular traffic type. If not specified, both unicast and multicast traffic uses the default route.

Example
The following command configures a default route for the switch:

```plaintext
configure iproute add default 123.45.67.1
```

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iproute delete

configure iproute delete <ip address> <mask> <gateway>

**Description**
 Deletes a static address from the routing table.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>gateway</td>
<td>Specifies a VLAN gateway.</td>
</tr>
</tbody>
</table>

**Default**
 N/A

**Usage Guidelines**
 Use a value of 255.255.255.255 for mask to indicate a host entry.

**Example**
The following command deletes an address from the gateway:
configure iproute delete 10.101.0.250/24 10.101.0.1

**History**
 This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
 This command is available on all platforms.
configure iproute delete blackhole

   configure iproute delete blackhole <ip address> <mask>

Description
Deletes a blackhole address from the routing table.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes a blackhole address from the routing table:
configure iproute delete blackhole 100.101.145.4

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iproute delete blackhole default

configure iproute delete blackhole default

Description
Deletes a default blackhole route from the routing table.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command deletes a blackhole default route from the routing table:
configure iproute delete blackhole default

History
This command was first available in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure iproute delete default

    configure iproute delete default <gateway>

Description
Deleting a default gateway from the routing table.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>gateway</td>
<td>Specifies a VLAN gateway.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Default routes are used when the router has no other dynamic or static route to the requested destination. A default gateway must be located on a configured IP interface.

Example
The following command deletes a default gateway:

    configure iproute delete default 123.45.67.1

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iproute priority

configure iproute priority [rip | bootp | icmp | static | ospf-intra | ospf-inter | ospf-as-external | ospf-extern1 | ospf-extern2] <priority>

Description
Changes the priority for all routes from a particular route origin.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rip</td>
<td>Specifies RIP.</td>
</tr>
<tr>
<td>bootp</td>
<td>Specifies BOOTP.</td>
</tr>
<tr>
<td>icmp</td>
<td>Specifies ICMP.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies OSPFIntra routing.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies OSPFInter routing.</td>
</tr>
<tr>
<td>ospf-as-external</td>
<td>Specifies OSPF as External routing.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies OSPF External 1 routing.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies OSPF External 2 routing.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a priority number.</td>
</tr>
</tbody>
</table>

Default
Table 30 lists the relative priorities assigned to routes depending upon the learned source of the route.

Table 30: Relative Route Priorities

<table>
<thead>
<tr>
<th>Route Origin</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct</td>
<td>10</td>
</tr>
<tr>
<td>Blackhole</td>
<td>50</td>
</tr>
<tr>
<td>Static</td>
<td>1100</td>
</tr>
<tr>
<td>ICMP</td>
<td>1200</td>
</tr>
<tr>
<td>OSPFIntra</td>
<td>2200</td>
</tr>
<tr>
<td>OSPFInter</td>
<td>2300</td>
</tr>
<tr>
<td>RIP</td>
<td>2400</td>
</tr>
<tr>
<td>OSPF External 1</td>
<td>3200</td>
</tr>
<tr>
<td>OSPF External 2</td>
<td>3300</td>
</tr>
<tr>
<td>BOOTP</td>
<td>5000</td>
</tr>
</tbody>
</table>

Usage Guidelines
Although these priorities can be changed, do not attempt any manipulation unless you are expertly familiar with the possible consequences.
Example
The following command sets IP route priority for static routing to 1200:
configure iproute priority static 1200

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure iproute route-map

configure iproute route-map [bgp | direct | e-bgp | i-bgp | ospf |
ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | rip | static]
[<route map> | none]

Description
Configures the contents of the IP routing table.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Specifies BGP routing.</td>
</tr>
<tr>
<td>direct</td>
<td>Specifies direct routing.</td>
</tr>
<tr>
<td>e-bgp</td>
<td>Specifies E-BGP routing.</td>
</tr>
<tr>
<td>i-bgp</td>
<td>Specifies I-BGP routing.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies OSPF routing.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies OSPF External 1 routing.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies OSPF External 2 routing.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies OSPFInter routing.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies OSPFIntra routing.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routing.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routing.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies not to use a route map.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Route maps for IP routing can be configured based on the route origin. When routes are added to the IP routing table from various sources, the route map configured for the origin of the route is applied to the route. After matching on specified characteristics, the characteristics for the route can be modified using the route maps. The characteristics that can be matched and modified are dependent on the origin of the route. Route maps for IP routing can be dynamically changed. In the case of direct and static route origins, the changes are reflected immediately. In the case of routes that are sourced from other origin, the changes are reflected within 30 seconds.

MPLS uses route map-based filters for controlling label advertisement and label propagation. The implementation of the delete route-map <route-map> command has been augmented to support the MPLS module.

Example
The following command configures the IP routing table bgp_out to BGP routing:

configure iproute route-map bgp_out bgp
**History**

This command was first available in ExtremeWare 6.1.5.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

**Platform Availability**

This command is available on the “i” series platforms only.
configure irdp

    configure irdp <mininterval> <maxinterval> <lifetime> <preference>

Description

Configures the router advertisement message timers, using seconds.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mininterval</td>
<td>Specifies the minimum amount of time between router advertisements in seconds. The default setting is 450 seconds.</td>
</tr>
<tr>
<td>maxinterval</td>
<td>Specifies the maximum amount of time between router advertisements in seconds. The default setting is 600 seconds.</td>
</tr>
<tr>
<td>lifetime</td>
<td>Specifies the client aging time. The default setting is 1,800 seconds.</td>
</tr>
<tr>
<td>preference</td>
<td>Specifies the preference level of the router. The default setting is 0.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

All arguments need to be specified. All time intervals are in seconds.

An ICMP Router Discover Protocol (IRDP) client always uses the router with the highest preference level. Change the preference setting to encourage or discourage the use of this router. The default setting is 0.

Example

The following command configures the router advertisement message timers:

    configure irdp 30 40 300 1

History

This command was first available in ExtremeWare 4.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
configure irdp

    configure irdp [multicast | broadcast]

Description
Configures the destination address of the router advertisement messages.

Syntax Description

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>multicast</td>
<td>Specifies multicast setting.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Specifies broadcast setting.</td>
</tr>
</tbody>
</table>

Default
Multicast (224.0.0.1)

Usage Guidelines
None

Example
The following command sets the address of the router advertiser messages to multicast:

```
configure irdp multicast
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure udp-profile add

configure udp-profile <profile_name> add <udp_port> [vlan <vlan name> | ip address <dest_ipaddress>]

**Description**
Configures a UDP-forwarding profile.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>Specifies a UDP profile name.</td>
</tr>
<tr>
<td>udp_port</td>
<td>Specifies a UDP port number.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>dest_ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
A maximum of 10 UDP-forwarding profiles can be defined. Each named profile may contain a maximum of eight “rules” defining the UDP port, and destination IP address or VLAN. A VLAN can make use of a single UDP-forwarding profile. UDP packets directed toward a VLAN use an all-ones broadcast on that VLAN.

**Example**
The following command adds port 34 to UDP profile `port_34_to_server`:
```
configure udp-profile port_34_to_server add 34 ip address 10.1.1.1
```

**History**
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure udp-profile delete

configure udp-profile <profile_name> delete <udp_port> [vlan <vlan name> | ip address <dest_ipaddress>]

Description
Deletes a forwarding entry from the specified UDP-profile.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>Specifies a UDP profile name.</td>
</tr>
<tr>
<td>udp_port</td>
<td>Specifies a UDP port number.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>dest_ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes port 34 from UDP profile port_34_to_server:
configure udp-profile port_34_to_server delete 34 ip address 10.1.1.1

History
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure vlan secondary-ip

configure vlan <super-vlan name> [add | delete] secondary-ip <ip address> {<mask>}

Description
Adds or deletes a secondary IP address to the super-VLAN for responding to ICMP ping requests.

Syntax Description

<table>
<thead>
<tr>
<th>super-vlan name</th>
<th>Specifies a super-VLAN name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Specifies to add a secondary IP address.</td>
</tr>
<tr>
<td>delete</td>
<td>Specifies to delete a secondary IP address.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a netmask.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

- All broadcast and unknown traffic remains local to the sub-VLAN and does not cross the sub-VLAN boundary. All traffic within the sub-VLAN is switched by the sub-VLAN, allowing traffic separation between sub-VLANs (while using the same default router address among the sub-VLANs).
- Hosts are located on the sub-VLAN. Each host can assume any IP address within the address range of the super-VLAN router interface. Hosts on the sub-VLAN are expected to have the same network mask as the super-VLAN and have their default router set to the IP address or the super-VLAN.
- All traffic (IP unicast and IP multicast) between sub-VLANs is routed through the super-VLAN. For example, no ICMP redirects are generated for traffic between sub-VLANs, because the super-VLAN is responsible for sub-VLAN routing. Unicast IP traffic across the sub-VLANs is facilitated by the automatic addition of an ARP entry (similar to a proxy ARP entry) when a sub-VLAN is added to a super-VLAN. This feature can be disabled for security purposes.

IP multicast traffic between sub-VLANs is routed when an IP multicast routing protocol is enabled on the super-VLAN.

Example
The following command adds a secondary IP address to the super-VLAN vsuper for responding to ICMP ping requests:

configure vlan vsuper add secondary-ip 10.1.1.1

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on the “i” series platforms only.
configure vlan subvlan

configure vlan <super-vlan name> [add | delete] subvlan <sub-vlan name>

Description
Adds or deletes a sub-VLAN to a super-VLAN.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>super-vlan name</td>
<td>Specifies a super-VLAN name</td>
</tr>
<tr>
<td>add</td>
<td>Specifies to add the sub-VLAN to the super-VLAN</td>
</tr>
<tr>
<td>delete</td>
<td>Specifies to delete the sub-VLAN from the super-VLAN</td>
</tr>
<tr>
<td>sub-vlan name</td>
<td>Specifies a sub-VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

- All broadcast and unknown traffic remains local to the sub-VLAN and does not cross the sub-VLAN boundary. All traffic within the sub-VLAN is switched by the sub-VLAN, allowing traffic separation between sub-VLANs (while using the same default router address among the sub-VLANs).
- Hosts are located on the sub-VLAN. Each host can assume any IP address within the address range of the super-VLAN router interface. Hosts on the sub-VLAN are expected to have the same network mask as the super-VLAN and have their default router set to the IP address or the super-VLAN.
- All traffic (IP unicast and IP multicast) between sub-VLANs is routed through the super-VLAN. For example, no ICMP redirects are generated for traffic between sub-VLANs, because the super-VLAN is responsible for sub-VLAN routing. Unicast IP traffic across the sub-VLANs is facilitated by the automatic addition of an ARP entry (similar to a proxy ARP entry) when a sub-VLAN is added to a super-VLAN. This feature can be disabled for security purposes.

IP multicast traffic between sub-VLANs is routed when an IP multicast routing protocol is enabled on the super-VLAN.

Example

The following command adds the sub-VLAN \texttt{vsub1} to the super-VLAN \texttt{vsuper}:

```
configure vlan vsuper add subvlan vsub1
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on the “i” series platforms only.
configure vlan subvlan-address-range

```
  configure vlan <vlan name> subvlan-address-range <ip address1> - <ip address2>
```

**Description**
Configures sub-VLAN address ranges on each sub-VLAN to prohibit the entry of IP addresses from hosts outside of the configured range.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a super-VLAN name.</td>
</tr>
<tr>
<td>ip address1</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>ip address2</td>
<td>Specifies another IP address.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
There is no error checking to prevent the configuration of overlapping sub-VLAN address ranges between multiple sub-VLANs. Doing so can result in unexpected behavior of ARP within the super-VLAN and associated sub-VLANs.

**Example**
The following command configures the super-VLAN vsuper to prohibit the entry of IP addresses from hosts outside of the configured range of IP addresses:

```
  configure vlan vsuper subvlan-address-range 10.1.1.1 - 10.1.1.255
```

**History**
This command was available in ExtremeWare 6.1.5.

**Platform Availability**
This command is available on the “i” series platforms only.
configure vlan upd-profile

configure vlan <vlan name> udp-profile <profile_name>

Description
Assigns a UDP-forwarding profile to the source VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>profile_name</td>
<td>Specifies a UDP profile name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
After the UDP profile has been associated with the VLAN, the switch picks up any broadcast UDP packets that match the user-configured UDP port number, and forwards those packets to the user-defined destination. If the UDP port is the DHCP/BOOTP port number, appropriate BOOTP/DHCP proxy functions are invoked.

Example
The following command assigns a UDP profile to VLAN accounting:

configure vlan accounting udp-profile port_34_to_server

History
This command was first available in ExtremeWare 4.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
create udp-profile

create udp-profile <profile_name>

Description
Creates a UDP-forwarding destination profile that describes the types of UDP packets (by port number) that are used, and where they are to be forwarded.

Syntax Description

| profile_name | Specifies a UDP profile name. |

Default
N/A

Usage Guidelines
You must give the profile a unique name, in the same manner as a VLAN, protocol filter, or Spanning Tree Domain (STD). A maximum of 10 UDP-forwarding profiles can be defined.

Example
The following command creates a UPD profile named backbone:
create udp-profile backbone

History
This command was first available in ExtremeWare 4.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
delete udp-profile

delete udp-profile <profile_name>

Description
Deletes a UDP-forwarding profile.

Syntax Description

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Specifies a UDP profile name.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command deletes a UDP profile named backbone:
delete udp-profile backbone

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable bootp vlan

    disable bootp vlan [<vlan name> | all]

Description
Disables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Enabled for all VLANs

Usage Guidelines
None

Example
The following command disables the generation and processing of BOOTP packets on a VLAN named accounting:

disable bootp vlan accounting

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable bootprelay

disable bootprelay

Description
Disables the BOOTP relay function.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   
```plaintext
   enable bootprelay
   ```
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

```plaintext
   configure bootprelay add <ip address>
```

Example
The following command disables the forwarding of BOOTP requests:

```plaintext
   disable bootprelay
```

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable icmp access-list

disable icmp access-list (slot <slot number>)

**Description**
Disables software forwarding of ICMP packets and enables hardware forwarding of ICMP packets at wire speed on selected models of “i” series switches.

**Syntax Description**

| slot number | Specifies the physical location in the chassis of the module. |

**Default**
Enabled

**Usage Guidelines**
Switches capable of hardware ICMP forwarding include the Summit 48si, Alpine 3804 and Alpine 3808, and BlackDiamond modules MSM-3, G16X3, G24T3, G8Xi, 10GX3 and F48Ti. For further information regarding specific models and ASIC part numbers, see the Release Notes.

Use this command to disable software forwarding and to enable hardware forwarding of ICMP packets. When ICMP hardware forwarding is used, ICMP access lists are not permitted and ICMP no longer uses ICMP filter rules.

When modules are mixed in the same chassis, the module continues to follow the configuration for the slot. That is, those slots that are incapable of hardware forwarding continue to forward packets by the CPU; slots capable and configured for hardware forwarding no longer use the CPU and handle the forwarding through the hardware.

**Example**
The following command disables software forwarding of ICMP packets:

disable icmp access-list slot 5

**History**
This command was available in ExtremeWare 7.3.0.

**Platform Availability**
This command is only applicable to selected modules of BlackDiamond, selected models of Alpine, and the Summit 48si. See the Release Notes for further information regarding the models and applicable ASIC part numbers.
disable icmp address-mask

disable icmp address-mask {vlan <vlan name>}

Description
Disables the generation of an ICMP address-mask reply on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Disables the generation of an ICMP address-mask reply (type 18, code 0) when an ICMP address mask request is received. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example
The following command disables the generation of an ICMP address-mask reply on VLAN accounting:

disable icmp address-mask vlan accounting

History
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable icmp parameter-problem

    disable icmp parameter-problem {vlan <vlan name>}

**Description**
Disables the generation of an ICMP parameter-problem message on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
Enabled

**Usage Guidelines**
Disables the generation of an ICMP parameter-problem message (type 12) when the switch cannot properly process the IP header or IP option information. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

**Example**
The following command disables the generation of an ICMP parameter-problem message on VLAN accounting:
```
disable icmp parameter-problem vlan accounting
```

**History**
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
disable icmp port-unreachables

disable icmp port-unreachables {vlan <vlan name>}

Description
Disables the generation of ICMP port unreachable messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Disables the generation of ICMP port unreachable messages (type 3, code 3) when a TPC or UDP request is made to the switch, and no application is waiting for the request, or access policy denies the request. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example
The following command disables ICMP port unreachable messages on VLAN accounting:

disable icmp port-unreachables vlan accounting

History
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable icmp redirects

    disable icmp redirects (vlan <vlan name>)

**Description**
Disables generation of ICMP redirect messages on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
Enabled

**Usage Guidelines**
This option only applies to the switch when the switch is not in routing mode.

**Example**
The following command disables ICMP redirects from VLAN accounting:

disable icmp redirects vlan accounting

**History**
This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
disable icmp time-exceeded

disable icmp time-exceeded {vlan <vlan name>}

Description
Disables the generation of ICMP time exceeded messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Disables the generation of an ICMP time exceeded message (type 11) when the TTL field expires during forwarding. IP multicast packets do not trigger ICMP time exceeded messages. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example
The following command disables the generation of ICMP time exceeded messages on VLAN accounting:

disable icmp time-exceeded vlan accounting

History
This command was first available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable icmp timestamp

   disable icmp timestamp {vlan <vlan name>}

Description
Disables the generation of an ICMP timestamp response on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Disables the generation of an ICMP timestamp response (type 14, code 0) when an ICMP timestamp request is received. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example
The following command disables the generation of an ICMP timestamp response on VLAN accounting:

disable icmp timestamp vlan accounting

History
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable icmp unreachables

disable icmp unreachables {vlan <vlan name>}

Description
Disables the generation of ICMP unreachable messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
None

Example
The following command disables the generation of ICMP unreachable messages on all VLANs:

disable icmp unreachables

History
This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
**disable icmp useredirects**

```disable icmp useredirects```

**Description**
Disables the modification of route table information when an ICMP redirect message is received.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled

**Usage Guidelines**
This option only applies to the switch when the switch is not in routing mode.

**Example**
The following command disables the changing of routing table information:
```
disable icmp useredirects
```

**History**
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
disable ip-option loose-source-route

Description
Disables the loose source route IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command disables the loose source route IP option:

disable ip-option loose-source-route

History
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ip-option record-route

    disable ip-option record-route

Description
Disables the record route IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command disables the record route IP option:
    disable ip-option record-route

History
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ip-option record-timestamp

    disable ip-option record-timestamp

**Description**
Disables the record timestamp IP option.

**Syntax Description**
This command has no arguments or variables.

**Default**
Enabled

**Usage Guidelines**
None

**Example**
The following command disables the record timestamp IP option:

disable ip-option record-timestamp

**History**
This command was first available in ExtremeWare 6.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
disable ip-option strict-source-route

disable ip-option strict-source-route

Description
Disables the strict source route IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command disables the strict source route IP option:
disable ip-option strict-source-route

History
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ip-option use-router-alert

    disable ip-option use-router-alert

Description
Disables the generation of the router alert IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command disables generation of the router alert IP option:
    disable ip-option use-router-alert

History
This command was first available in ExtremeWare 6.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable iparp checking

disable iparp checking

Description
Disable checking if the ARP Request source IP address is within the range of the local interface or VLAN domain.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command disables IP ARP checking:

disable iparp checking

History
This command was first available in ExtremeWare 6.2.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable iparp refresh

disable iparp refresh

Description
Disables IP ARP to refresh its IP ARP entries before timing out.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
IP ARP refresh can only be disabled if IP forwarding is disabled. The purpose of disabling ARP refresh is to reduce ARP traffic in a high node count layer 2 switching only environment.

Example
The following command disables IP ARP refresh:

disable iparp refresh

History
This command was first available in ExtremeWare 6.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable ipforwarding

For “i” series switches:

disable ipforwarding {
    [broadcast | fast-direct-broadcast |
    ignore-broadcast] } {vlan <vlan name>}

For “e” series switches:

disable ipforwarding {
    [broadcast | ignore-broadcast] } {vlan <vlan name>}

Description
Disables routing (or routing of broadcasts) for one or all VLANs. If no argument is provided, disables routing for all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Specifies broadcast IP forwarding.</td>
</tr>
<tr>
<td>fast-direct-broadcast</td>
<td>Specifies fast direct broadcast forwarding.</td>
</tr>
<tr>
<td></td>
<td>NOTE: This option is only available on the “i” series of switches.</td>
</tr>
<tr>
<td>ignore-broadcast</td>
<td>Specifies to ignore broadcast forwarding.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Disabling IP forwarding also disables broadcast forwarding. Broadcast forwarding can be disabled without disabling IP forwarding. When new IP interfaces are added, IP forwarding (and IP broadcast forwarding) is disabled by default. Other IP related configuration is not affected.

Example
The following command disables forwarding of IP broadcast traffic for a VLAN named accounting:

disable ipforwarding broadcast vlan accounting

History
This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support broadcast IP forwarding.
Platform Availability

This command is available on all platforms.
disable ipforwarding lpm-routing

    disable ipforwarding lpm-routing {vlan <vlan name>}

Description
Disables Longest Prefix Match (LPM) routing for the specified VLAN. If no argument is provided, disables LPM routing for all VLANs except the management VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Disabling LPM routing does not disable IP forwarding.

Example
The following command disables LPM routing for all configured VLANs:

disable ipforwarding lpm-routing

The following command disables LPM routing for a VLAN named *accounting*:

disable ipforwarding lpm-routing accounting

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond series chassis-based systems only.
disable iproute sharing

disable iproute sharing

Description
Disables load sharing if multiple routes to the same destination are available. When multiple routes to
the same destination are available, load sharing can be enabled to distribute the traffic to multiple
destination gateways. Only paths with the same lowest cost is will be shared.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
IP route sharing allows multiple equal-cost routes to be used concurrently. IP route sharing can be used
with static routes or with OSPF routes. In OSPF, this capability is referred to as equal cost multipath
(ECMP) routing. ECMP is not disabled when you disable ip-route sharing. By default, ECMP can
load-balance on up to four next-hops, irrespective of the route-sharing configuration.

Configure static routes and/or OSPF as you would normally. ExtremeWare supports unlimited route
sharing across static routes and up to 12 ECMP routes for OSPF.

Route sharing is useful only in instances where you are constrained for bandwidth. This is typically not
the case using Extreme switches. Using route sharing makes router troubleshooting more difficult
because of the complexity in predicting the path over which the traffic will travel.

Example
The following command disables load sharing for multiple routes:
disable iproute sharing

History
This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.2 to allow support of up to 12 ECMP routes for OSPF.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable irdp

disable irdp {vlan <vlan name>}

Description
Disables the generation of ICMP router advertisement messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
If no optional argument is specified, all the IP interfaces are affected.

Example
The following command disables IRDP on VLAN accounting:

disable irdp vlan accounting

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable loopback-mode vlan

    disable loopback-mode vlan [<vlan name> | all]

**Description**

Disallows a VLAN to be placed in the UP state without an external active port. This allows (disallows) the VLANs routing interface to become active.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan name&gt;</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Use this command to specify a stable interface as a source interface for routing protocols. This decreases the possibility of route flapping, which can disrupt connectivity.

**Example**

The following command disallows the VLAN *accounting* to be placed in the UP state without an external active port:

```
disable loopback-mode vlan accounting
```

**History**

This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
disable multinetting

disable multinetting (proprietary | standard)

Description
Disables multinetting in the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proprietary</td>
<td>Specifies that proprietary multinetting is to be disabled. The proprietary keyword indicates that multinetting operation is done by creating VLANs with dummy protocols and associating IP addresses with them. Proprietary multinetting is the default value.</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies that standard multinetting is to be disabled. The standard keyword indicates that multinetting operation is done by associating multiple IP subnets with a single VLAN without using dummy-protocol based VLANs.</td>
</tr>
</tbody>
</table>

Default
If neither keyword is used, then proprietary multinetting is disabled by default.

Usage Guidelines
This command disables proprietary multinetting or standard multinetting in the switch.
Standard multinetting cannot be disabled if there are secondary IP addresses configured in the switch.

Use the following command to enable multinetting:

```
enable multinetting
```

Example
The following command disables standard multinetting in the switch:

```
disable multinetting standard
```

History
This command was first available in ExtremeWare 2.0.
The proprietary and standard options were made available for this command in ExtremeWare 7.3.0.

Platform Availability
This command is available on the “i” series platforms only.
disable subvlan-proxy-arp vlan

```
disable subvlan-proxy-arp vlan [<super-vlan name> | all]
```

**Description**

Disables the automatic entry of sub-VLAN information in the proxy ARP table.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>super-vlan name</td>
<td>Specifies a super-VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**

Enabled

**Usage Guidelines**

To facilitate communication between sub-VLANs, by default, an entry is made in the IP ARP table of the super-VLAN that performs a proxy ARP function. This allows clients on one sub-VLAN to communicate with clients on another sub-VLAN. In certain circumstances, intra-sub-VLAN communication may not be desired for isolation reasons.

**NOTE**

*The isolation option works for normal, dynamic, ARP-based client communication.*

**Example**

The following command disables the automatic entry of sub-VLAN information in the proxy ARP table of the super-VLAN `vsuper`:

```
disable subvlan-proxy-arp vlan vsuper
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on the “i” series platforms only.
disable udp-echo-server

disable udp-echo-server

Description
Disables UDP echo server support.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
UDP Echo packets are used to measure the transit time for data between the transmitting and receiving end.

Example
The following command disables UDP echo server support:
disable udp-echo-server

History
This command was available in ExtremeWare 6.2.1.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable bootp vlan

    enable bootp vlan [<vlan name> | all]

Description
 Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;vlan name&gt;</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Enabled for all VLANs

Usage Guidelines
None

Example
The following command enables the generation and processing of BOOTP packets on a VLAN named accounting:

    enable bootp vlan accounting

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable bootprelay

Description
Enables the BOOTP relay function.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
After IP unicast routing has been configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95. To configure the relay function, follow these steps:

1. Configure VLANs and IP unicast routing.
2. Enable the DHCP or BOOTP relay function, using the following command:
   ```
   enable bootprelay
   ```
3. Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:
   ```
   configure bootprelay add <ip address>
   ```

Example
The following command enables the forwarding of BOOTP requests:

```
enable bootprelay
```

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable icmp access-list

   enable icmp access-list {slot <slot number>}

Description
Re-enables software forwarding of ICMP packets and disables hardware forwarding of ICMP packets at wire speed on selected models of “i” series switches.

Syntax Description

<table>
<thead>
<tr>
<th>slot number</th>
<th>Specifies the physical location in the chassis of the module.</th>
</tr>
</thead>
</table>

Default
Enabled

Usage Guidelines
Switches capable of hardware ICMP forwarding include the Summit 48si, Alpine 3804 and Alpine 3808, and BlackDiamond modules MSM-3, G16X3, G24T3, G8Xi, 10GX3 and F48Ti. For further information regarding specific models and ASIC part numbers, see the Release Notes.

Use this command to re-enable software forwarding and to disable hardware forwarding of ICMP packets. When ICMP hardware forwarding is used, ICMP access lists are not permitted and ICMP no longer uses ICMP filter rules.

Example
The following command enables software forwarding of ICMP packets:

```
enable icmp access-list slot 5
```

History
This command was available in ExtremeWare 7.3.0.

Platform Availability
This command is only applicable to selected modules of BlackDiamond, selected models of Alpine, and the Summit 48si. See the Release Notes for further information regarding the models and applicable ASIC part numbers.
enable icmp address-mask

    enable icmp address-mask {vlan <vlan name>}

Description
Enables the generation of an ICMP address-mask reply on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Enables the generation of an ICMP address-mask reply (type 18, code 0) when an ICMP address mask request is received. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example
The following command enables the generation of an ICMP address-mask reply on VLAN accounting:

    enable icmp address-mask vlan accounting

History
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable icmp parameter-problem

    enable icmp parameter-problem {vlan <vlan name>}

Description
Enables the generation of an ICMP parameter-problem message on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Enables the generation of an ICMP parameter-problem message (type 12) when the switch cannot properly process the IP header or IP option information. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

Example
The following command enables the generation of an ICMP parameter-problem message on VLAN accounting:

    enable icmp parameter-problem vlan accounting

History
This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable icmp port-unreachables

    enable icmp port-unreachables {vlan <vlan name>}

**Description**

Enables the generation of ICMP port unreachable messages on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

Enabled

**Usage Guidelines**

Enables the generation of ICMP port unreachable messages (type 3, code 3) when a TPC or UDP request is made to the switch, and no application is waiting for the request, or access policy denies the request. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

**Example**

The following command enables ICMP port unreachable messages on VLAN *accounting*:

```
enable icmp port-unreachables vlan accounting
```

**History**

This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable icmp redirects

   enable icmp redirects {vlan <vlan name>}

Description
Enables generation of ICMP redirect messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
This option only applies to the switch when the switch is not in routing mode.

Example
The following command enables the generation of ICMP redirect messages on all VLANs:

```
enable icmp redirects
```

History
This command was available in ExtremeWare 2.0.
This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable icmp time-exceeded

   enable icmp time-exceeded {vlan <vlan name>}

**Description**

Enables the generation of ICMP time exceeded messages on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

Enabled

**Usage Guidelines**

Enables the generation of an ICMP time exceeded message (type 11) when the TTL field expires during forwarding. IP multicast packets do not trigger ICMP time exceeded messages. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

**Example**

The following command enables the generation of ICMP time exceeded messages on VLAN accounting:

```
enable icmp time-exceeded vlan accounting
```

**History**

This command was first available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable icmp timestamp

    enable icmp timestamp {vlan <vlan name>}

**Description**

Enables the generation of an ICMP timestamp response on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

Enabled

**Usage Guidelines**

Enables the generation of an ICMP timestamp response (type 14, code 0) when an ICMP timestamp request is received. If a VLAN is not specified, the command applies to all IP interfaces.

This command only affects the generation of certain ICMP packets. Filtering of ICMP packets usually forwarded by the switch is controlled by the access-list commands.

**Example**

The following command enables the generation of an ICMP timestamp response on VLAN `accounting`:

```
enable icmp timestamp vlan accounting
```

**History**

This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable icmp unreachables

    enable icmp unreachables {vlan <vlan name>}

Description
Enables the generation of ICMP unreachable messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
None

Example
The following command enables the generation of ICMP unreachable messages on all VLANs:

```
enable icmp unreachables
```

History
This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable icmp useredirects

enable icmp useredirects

Description
Enables the modification of route table information when an ICMP redirect message is received.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This option only applies to the switch when the switch is not in routing mode.

Example
The following command enables the modification of route table information:

```
enable icmp useredirects
```

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ip-option loose-source-route

enable ip-option loose-source-route

Description
Enables the loose source route IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command enables the loose source route IP option:

```
enable ip-option loose-source-route
```

History
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ip-option record-route

enable ip-option record-route

**Description**
Enables the record route IP option.

**Syntax Description**
This command has no arguments or variables.

**Default**
Enabled

**Usage Guidelines**
None

**Example**
The following command enables the record route IP option:

```
enable ip-option record-route
```

**History**
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable ip-option record-timestamp

enable ip-option record-timestamp

Description
Enables the record timestamp IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command enables the record timestamp IP option:

```
enable ip-option record-timestamp
```

History
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ip-option strict-source-route

Description
Enables the strict source route IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command enables the strict source route IP option:

```
enable ip-option strict-source-route
```

History
This command was first available in ExtremeWare 6.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ip-option use-router-alert

Description
Enables the generation of the router alert IP option.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
None

Example
The following command enables generation of the router alert IP option:
   enable ip-option use-router-alert

History
This command was first available in ExtremeWare 6.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable iparp checking

enable iparp checking

Description
 Enables checking if the ARP Request source IP address is within the range of the local interface or VLAN domain.

Syntax Description
 This command has no arguments or variables.

Default
 Enabled

Usage Guidelines
 None

Example
 The following command enables IP ARP checking:
 enable iparp checking

History
 This command was first available in ExtremeWare 6.2.
 This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
 This command is available on all platforms.
enable iparp refresh

enable iparp refresh

Description
Enables IP ARP to refresh its IP ARP entries before timing out.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
IP ARP refresh can only be disabled if IP forwarding is disabled. The purpose of disabling ARP refresh is to reduce ARP traffic in a high node count layer 2 switching only environment.

Example
The following command enables IP ARP refresh:
   enable iparp refresh

History
This command was first available in ExtremeWare 6.2.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
enable ipforwarding

For “i” series switches:
   enable ipforwarding {
   broadcast | fast-direct-broadcast |
   ignore-broadcast
   } {vlan <vlan name>}

For “e” series switches:
   enable ipforwarding {
   broadcast | ignore-broadcast
   } {vlan <vlan name>}

Description
Enables IP routing or IP broadcast forwarding for one or all VLANs. If no argument is provided, enables IP routing for all VLANs that have been configured with an IP address.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>broadcast</td>
<td>Specifies broadcast IP forwarding.</td>
</tr>
<tr>
<td>fast-direct-broadcast</td>
<td>Specifies fast direct broadcast forwarding.</td>
</tr>
<tr>
<td>ignore-broadcast</td>
<td>Specifies to ignore broadcast forwarding.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
IP forwarding must first be enabled before IP broadcast forwarding can be enabled. When new IP interfaces are added, IP forwarding (and IP broadcast forwarding) is disabled by default.

Other IP related configuration is not affected.

Example
The following command enables forwarding of IP traffic for all VLANs with IP addresses:
   enable ipforwarding

The following command enables forwarding of IP broadcast traffic for a VLAN named accounting:
   enable ipforwarding broadcast vlan accounting

History
This command was available in ExtremeWare 2.0.
This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.
This command was added to the “e” series of switches in ExtremeWare 7.1e.
This command was modified in an ExtremeWare 7.2e to support the ignore-broadcast keyword.
**Platform Availability**

This command is available on all platforms.
enable ipforwarding lpm-routing

   enable ipforwarding lpm-routing {vlan <vlan name>}

Description
Enables Longest Prefix Match (LPM) routing for the specified VLAN. If no argument is provided, enables LPM routing for all VLANs except the management VLAN.

Syntax Description
<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
This command enables Longest Prefix Match (LPM) routing for a specified VLAN. When either an ARM or MPLS module is installed in a BlackDiamond switch, the module can be configured to forward IP packets for specified VLANs using LPM routing. If no VLAN is specified, LPM routing is enabled for all configured VLANs except the management VLAN.

Example
The following command enables LPM routing for all configured VLANs:
```bash
enable ipforwarding lpm-routing
```

The following command enables LPM routing for a VLAN named **accounting**:
```bash
enable ipforwarding lpm-routing accounting
```

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
enable iproute sharing

enable iproute sharing

Description
Enables load sharing if multiple routes to the same destination are available. When multiple routes to the same destination are available, load sharing can be enabled to distribute the traffic to multiple destination gateways. Only paths with the same lowest cost is will be shared.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
IP route sharing allows multiple equal-cost routes to be used concurrently. IP route sharing can be used with static routes or with OSPF routes. In OSPF, this capability is referred to as equal cost multipath (ECMP) routing.

Configure static routes and/or OSPF as you would normally. ExtremeWare supports unlimited route sharing across static routes and up to 12 ECMP routes for OSPF.

Route sharing is useful only in instances where you are constrained for bandwidth. This is typically not the case using Extreme switches. Using route sharing makes router troubleshooting more difficult because of the complexity in predicting the path over which the traffic will travel.

Example
The following command enables load sharing for multiple routes:

```
enable iproute sharing
```

History
This command was available in ExtremeWare 2.0.

This command was modified in ExtremeWare 6.2.2 to allow support of up to 12 ECMP routes for OSPF.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable irdp

    enable irdp {vlan <vlan name>}

Description
Enables the generation of ICMP router advertisement messages on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
If no optional argument is specified, all the IP interfaces are affected.

Example
The following command enables IRDP on VLAN accounting:

```
enable irdp vlan accounting
```

History
This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable loopback-mode vlan

enable loopback-mode vlan [<vlan name> | all]

**Description**

Allows a VLAN to be placed in the UP state without an external active port. This allows (disallows) the VLANs routing interface to become active.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Use this command to specify a stable interface as a source interface for routing protocols. This decreases the possibility of route flapping, which can disrupt connectivity.

**Example**

The following command allows the VLAN `accounting` to be placed in the UP state without an external active port:

```
enable loopback-mode vlan accounting
```

**History**

This command was first available in ExtremeWare 6.1.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable multinetting

 enable multinetting {proprietary | standard}

Description
Enables multinetting in the switch.

Syntax Description

<table>
<thead>
<tr>
<th>keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>proprietary</td>
<td>Specifies that proprietary multinetting is to be enabled. The proprietary keyword indicates that multinetting operation is done by creating VLANs with dummy protocols and associating IP addresses with them. Proprietary multinetting is the default value.</td>
</tr>
<tr>
<td>standard</td>
<td>Specifies that standard multinetting is to be enabled. The standard keyword indicates that multinetting operation is done by associating multiple IP subnets with a single VLAN without using dummy-protocol based VLANs.</td>
</tr>
</tbody>
</table>

Default
If neither keyword is used, proprietary multinetting is enabled by default.

Usage Guidelines
Use this command to enable proprietary multinetting or standard multinetting in the switch.
Standard multinetting cannot be enabled in the switch when proprietary multinetting is enabled. Proprietary multinetting cannot be enabled in the switch when standard multinetting is enabled.

Use the following command to disable multinetting:

disable multinetting

Example
The following command enables proprietary multinetting in the switch:

enable multinetting proprietary

History
This command was first available in ExtremeWare 2.0.
The proprietary and standard options were made available for this command in ExtremeWare 7.3.0.

Platform Availability
This command is available on the “i” series platforms only.
enable subvlan-proxy-arp vlan

   enable subvlan-proxy-arp vlan [<super-vlan name> | all]

Description
Enables the automatic entry of sub-VLAN information in the proxy ARP table.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>super-vlan name</td>
<td>Specifies a super-VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
To facilitate communication between sub-VLANs, by default, an entry is made in the IP ARP table of the super-VLAN that performs a proxy ARP function. This allows clients on one sub-VLAN to communicate with clients on another sub-VLAN. In certain circumstances, intra-sub-VLAN communication may not be desired for isolation reasons.

![NOTE]

The isolation option works for normal, dynamic, ARP-based client communication.

Example
The following command enables the automatic entry of sub-VLAN information in the proxy ARP table of the super-VLAN vsuper:

   enable subvlan-proxy-arp vlan vsuper

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on the “i” series platforms only.
enable udp-echo-server

    enable udp-echo-server

Description
Enables UDP echo server support.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
UDP Echo packets are used to measure the transit time for data between the transmitting and receiving end.

Example
The following command enables UDP echo server support:

    enable udp-echo-server

History
This command was available in ExtremeWare 6.2.1.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
rtlookup

rtlookup [<ip address> | <hostname>]

Description
Performs a look-up in the route table to determine the best route to reach an IP address or host.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hostname</td>
<td>Specifies a hostname.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The output of the rtlookup command has been enhanced to include information about MPLS LSPs associated with the routes. The flags field displayed by this command has been enhanced to indicate the presence of MPLS next hops. An uppercase L indicates the presence of a direct LSP next hop for the route. A lowercase l indicates the presence of an indirect LSP next hop for the route.

An optional mpls keyword has been added to the rtlookup command. When the mpls keyword is specified, the information displayed is modified; some of the information normally displayed is omitted, and the LSP endpoint and outgoing MPLS label are displayed instead. The LSP endpoint is the IP address/prefix of the FEC associated with the LSP. The LSP endpoint matches the destination for direct LSPs and is a 32-bit prefix address of a proxy router for indirect LSPs.

Example
The following command performs a look up in the route table to determine the best way to reach the specified hostname:

rtlookup berkeley.edu

History
This command was available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
run ipfdb-check

run ipfdb-check [index <bucket> <entry> | <ip-address> {<ip-address>}]
{extended} {detail}

Description
Checks IP FDB entries for consistency.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket</td>
<td>Specifies the bucket portion of the FDB hash index.</td>
</tr>
<tr>
<td>entry</td>
<td>Specifies the entry portion of the FDB hash index.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specifies an IP address. FDB entries with this IP address will be checked.</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specifies a second IP address, for checking bi-directional entries.</td>
</tr>
<tr>
<td>extended</td>
<td>Enables OTP index checking in the MAC entry and VPST of the egress port.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that more detailed debug information should be logged.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The IP FDB error checking function logs the error count into the system log. Use the detail option to log more detailed debug information.

Example
The following command will do consistency checking on IP FDB entries for IP address 10.20.30.55:
run ipfdb-check 10.20.30.55

History
This command was first available in ExtremeWare 6.1.9

Platform Availability
This command is available on all platforms.
The extended option is available on the BlackDiamond switch only.
show iparp

    show iparp {<ip address> | <mac_address> | vlan <vlan name> | permanent}

Description
Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, MAC address, VLAN, or permanent entries.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies a MAC address.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>permanent</td>
<td>Specifies permanent entries.</td>
</tr>
</tbody>
</table>

Default
Show all entries.

Usage Guidelines
Displays the IP ARP table, including:
- IP address
- MAC address
- Aging timer value
- VLAN name, VLAN ID and port number
- Flags

Example
The following command displays the IP ARP table:
show iparp 10.1.1.5/24

History
This command was available in ExtremeWare 2.0.
This command was modified in ExtremeWare 6.2.1 to provide the MAC address option.
This command was added to the “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2.e to provide the MAC address option.

Platform Availability
This command is available on all platforms.
**show iparp proxy**

```
show iparp proxy {<ip address> {<mask>}}
```

**Description**
Displays the proxy ARP table.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
If no argument is specified, then all proxy ARP entries are displayed.

**Example**
The following command displays the proxy ARP table:
```
show iparp proxy 10.1.1.5/24
```

**History**
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show ipconfig

    show ipconfig {vlan <vlan-name>} {detail}

Description
Displays the IP configuration for the given VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Specifies that IP configuration is to be displayed for a selected VLAN. If this optional parameter is not entered, then global IP configuration information is displayed.</td>
</tr>
<tr>
<td>vlan-name</td>
<td>Specifies the name of the VLAN for which the IP configuration is to be displayed.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that IP configuration is to be displayed in detail format.</td>
</tr>
</tbody>
</table>

Default
If no VLAN information is specified, then global IP configuration is displayed by default. Otherwise, information for specific VLAN(s) will be displayed.

Usage Guidelines
This command displays the IP configuration for a given VLAN. If no VLAN information is specified, then global IP configuration is displayed by default. Otherwise, information for specific VLAN(s) will be displayed. Global IP configuration information includes:

- IP address/netmask/etc.
- IP forwarding information / IP multicast forwarding information
- BOOTP configuration
- VLAN name and VLANID
- ICMP configuration (global)
- IGMP configuration (global)
- IRDP configuration (global)

Using the detail option of his command displays secondary IP addresses, which are displayed in the line following the primary IP address output.

Example
The following example shows the secondary IP address configuration for the VLAN named vlantest1:

    show ipconfig vlantest1

Following is sample output from this command:

    inet: 51.0.0.1 netmask 0xffffff00 broadcast 51.0.0.255
    Secondary: inet 53.0.0.1 netmask 0xffffffff broadcast 53.0.0.255

The following example shows global output for the show ipconfig command:

    show ipconfig
Following is sample output from this command:

Router Interface[1] on VLAN test is enable and up.
  UDP Forwarding profile: none.
  inet 11.3.3.4 netmask 0xffffff00 broadcast 11.3.3.255
Secondary: inet 11.4.3.4 netmask 0xffffff00 broadcast 11.4.3.255
  Multicast ttl 1 metric 1 mtu 1500
Locally registered multicast address (Last Querier=11.3.3.4):
  224.0.0.1
Flags:
  AddrMaskRly NO  BOOTP Host NO  DirBcastHwFwd NO  DVMRP NO
  ESRP NO  Fwd Bcast NO  IGMP YES  IGMP Ver V2
  IgnoreBcast NO  IP Fwding NO  IPmc Fwd NO  IRDP Advert NO
  ISIS NO  ISQ NO  LDP NO  LPM-routing NO
  MPLS NO  NAT-Inside NO  NAT-Outside NO  OSPF NO
  PIM NO  RIP NO  RSVP NO  SendParam YES
  SendPortUn YES  Send Redir YES  SendTimxceed YES  SendUnreach YES
  SLB-Cli NO  SLB-Srv NO  SubVLAN Prxy YES  TimeStampRly NO
  VRRP NO

History
This command was first available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

The output for this command was changed to accommodate the multinetting feature by including secondary IP addresses. This modified command was made available in ExtremeWare 7.3.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the detail keyword.

Platform Availability
This command is available on all platforms.
show ipfdb

show ipfdb {<ip address> <netmask> | vlan <vlan name>}

Description
Displays the contents of the IP forwarding database (FDB) table. Used for technical support purposes. If no option is specified, all IP FDB entries are displayed.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Default is to show all IP FDB entries.

Usage Guidelines
Displays IP FDB table content including:

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dest IP Addr</td>
<td>IP address</td>
</tr>
<tr>
<td>TblIdx</td>
<td>IP FDB hash index and entry number</td>
</tr>
<tr>
<td>MacIdx</td>
<td>MAC FDB hash index and entry number</td>
</tr>
<tr>
<td>Flag</td>
<td>Flags</td>
</tr>
<tr>
<td>FlowInfo</td>
<td>This field only appears on the “i” series of switches.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>Next hop router MAC address</td>
</tr>
<tr>
<td>VLAN</td>
<td>Egress VLAN ID</td>
</tr>
<tr>
<td>Port</td>
<td>Egress port number</td>
</tr>
</tbody>
</table>

Example
The following command displays the contents of the IP FDB table on a VLAN named accounting:

show ipfdb vlan accounting

<table>
<thead>
<tr>
<th>Dest IP Addr</th>
<th>TblIdx</th>
<th>MacIdx</th>
<th>Flag</th>
<th>FlowInfo</th>
<th>MAC Address</th>
<th>VLAN Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.205.4.201</td>
<td>00C3.0 9C32.0</td>
<td>0000 00:00:00:00:00:00:00:00</td>
<td>4000</td>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10.205.4.202</td>
<td>01C3.0 9C32.0</td>
<td>0000 00:00:00:00:00:00:00:00</td>
<td>4000</td>
<td>1</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
History

This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability

This command is available on all platforms.
show iproute

For “i” series of switches:

    show iproute {priority | vlan <vlan name> | permanent | <ip address> <netmask> | route-map | origin [direct | static | blackhole | rip | bootp | icmp | ospf-intra | ospf-inter | ospf-as-external | ospf-extern1 | ospf-extern2]} {mpls} {sorted}

For “e” series of switches:

    show iproute {priority | vlan <vlan name> | permanent | <ip address> <netmask> | origin [direct | static | blackhole | rip | bootp | icmp | ospf-intra | ospf-inter | ospf-as-external | ospf-extern1 | ospf-extern2]}} {sorted}

Description
Displays the contents of the IP routing table or the route origin priority.

Syntax Description

- **priority**: Specifies a route priority.
- **vlan name**: Specifies a VLAN name.
- **permanent**: Specifies permanent routing.
- **ip address**: Specifies an IP address.
- **netmask**: Specifies a subnet mask.
- **route-map**: Specifies display of route maps for direct, static, blackhole, RIP, BOOTP, ICMP, OSPF-intra, OSPF-inter, OSPF as External, OSPF External 1, and OSPF External 2 routing.
  - NOTE: This option is only available on the “i” series of switches.
- **origin**: Specifies a display of the route map origin.
- **mpls**: Specifies to display MPLS information.
  - NOTE: This option is only available on the “i” series of switches.
- **sorted**: Specifies to sort the information displayed.

Default
N/A

Usage Guidelines
Route maps for IP routing can be configured based on the route origin. When routes are added to the IP routing table from various sources, the route map configured for the origin of the route is applied to the route. After matching on specified characteristics, the characteristics for the route can be modified using the route maps. The characteristics that can be matched and modified are dependent on the origin of the route. Route maps for IP routing can be dynamically changed. In the case of direct and static route origins, the changes are reflected immediately. In the case of routes that are sourced from other origin, the changes are reflected within 30 seconds.

The output of the `show iproute` command has been enhanced to include information about MPLS LSPs associated with the routes. The flags field displayed by this command has been enhanced to...
indicate the presence of MPLS next hops. An uppercase \( L \) indicates the presence of a direct LSP next hop for the route. A lowercase \( l \) indicates the presence of an indirect LSP next hop for the route.

**On the “I” series of switches only.** An optional \texttt{mpls} keyword has been added to the \texttt{show iproute} command. When the \texttt{mpls} keyword is specified, the information displayed is modified; some of the information normally displayed is omitted, and the LSP endpoint and outgoing MPLS label are displayed instead. The LSP endpoint is the IP address/prefix of the FEC associated with the LSP. The LSP endpoint matches the destination for direct LSPs and is a 32-bit prefix address of a proxy router for indirect LSPs.

The \texttt{mpls} keyword only applies to some of the options available on the \texttt{show iproute} command. The \texttt{mpls} keyword is ignored when specified in conjunction with the following options:

- priority
- route-map
- summary

If a route is active and in use, it is preceded in the display by an “*”. If there are multiple routes to the same destination network, the “*” will indicate which route is the most preferable route.

The \texttt{Use} and \texttt{M-Use} fields indicate the number of times the route table entry is being used for packet forwarding decisions. The \texttt{Use} field indicates a count for unicast routing while the \texttt{M-Use} field indicates a count for multicast routing. If the use count is going up unexpectedly, the software is making route decisions and should be investigated further.

**Example**

The following command displays detailed information about all IP routing:

```
show iproute detail
```

Following is the output from this command:

```
Destination: 10.10.121.111/30
Gateway: 10.10.121.201   VLAN : helium   Origin : *d
Use   : 14409   M-Use : 0   Acct-1 : 0

Destination: 10.11.166.112/29
Gateway: 10.17.0.1   VLAN : helium   Origin : *be
Metric : 2   Flags : UG------um   Time : 01:11:23:49
Use   : 0   M-Use : 0   Acct-1 : 0

Destination: 10.13.105.112/29
Gateway: 10.11.110.123   VLAN : helium   Origin : *be
Metric : 2   Flags : UG------um   Time : 00:29:09:23
Use   : 0   M-Use : 0   Acct-1 : 0
```

**History**

This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare 6.1.8b12 to support MPLS modules.
show iproute

This command was modified to include a timestamp in ExtremeWare 6.2.2.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
show ipstats

    show ipstats {vlan <vlan name>}

Description
Displays IP statistics for the CPU for the switch or for a particular VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command only shows statistics of the CPU-handled packets. Not all packets are handled by the CPU.

The fields displayed in the show ipstats command are defined in Table 31 though Table 35.

Table 31: Global IP Statistics Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>InReceives</td>
<td>Total number of incoming IP packets processed by the CPU.</td>
</tr>
<tr>
<td>InUnicast</td>
<td>Total number of unicast IP packets processed by the CPU.</td>
</tr>
<tr>
<td>InBcast</td>
<td>Total number of broadcast IP packets processed by the CPU.</td>
</tr>
<tr>
<td>InMcast</td>
<td>Total number of multicast IP packets processed by the CPU.</td>
</tr>
<tr>
<td>InHdrEr</td>
<td>Total number of packets with an IP Header Error forwarded to the CPU.</td>
</tr>
<tr>
<td>Bad vers</td>
<td>Total number of packets with a version other than IP v4 in the IP version field.</td>
</tr>
<tr>
<td>Bad chksum</td>
<td>Total number of packets with a bad IP checksum forwarded to the CPU.</td>
</tr>
<tr>
<td>Short pkt</td>
<td>IP packets that are too short.</td>
</tr>
<tr>
<td>Short hdr</td>
<td>IP packets with a header that is too short.</td>
</tr>
<tr>
<td>Bad hdrlen</td>
<td>IP packets with a header length that is less than the length specified.</td>
</tr>
<tr>
<td>Bad length</td>
<td>IP packets with a length less than that of the header.</td>
</tr>
<tr>
<td>InDelivers</td>
<td>IP packets passed to upper layer protocols.</td>
</tr>
<tr>
<td>Bad Proto</td>
<td>IP packets with unknown (not standard) upper layer protocol.</td>
</tr>
<tr>
<td>OutRequest</td>
<td>IP packets sent from upper layers to the IP stack.</td>
</tr>
<tr>
<td>OutDiscard</td>
<td>IP packets that are discarded due to lack of buffer space or the router interface being down, or broadcast packets with broadcast forwarding disabled.</td>
</tr>
<tr>
<td>OutNoRoute</td>
<td>IP packets with no route to the destination.</td>
</tr>
<tr>
<td>Forwards</td>
<td>ForwardOK and Fwd Err aggregate count.</td>
</tr>
<tr>
<td>ForwardOK</td>
<td>Total number of IP packets forwarded correctly.</td>
</tr>
<tr>
<td>Fwd Err</td>
<td>Total number of IP packets that cannot be forwarded.</td>
</tr>
</tbody>
</table>
### Table 31: Global IP Statistics Field Definitions (Continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>NoFwding</td>
<td>Aggregate number of IP packets not forwarded due to errors.</td>
</tr>
<tr>
<td>Redirects</td>
<td>IP packets forwarded on the same network.</td>
</tr>
<tr>
<td>No route</td>
<td>Not used.</td>
</tr>
<tr>
<td>Bad TTL</td>
<td>IP packets with a bad time-to-live.</td>
</tr>
<tr>
<td>Bad MC TTL</td>
<td>IP packets with a bad multicast time-to-live.</td>
</tr>
<tr>
<td>Bad IPdest</td>
<td>IP packets with an address that does not comply with the IP v4 standard.</td>
</tr>
<tr>
<td>Blackhole</td>
<td>IP packets with a destination that is a blackhole entry.</td>
</tr>
<tr>
<td>Output err</td>
<td>Not used. This is the same as Fwd Err.</td>
</tr>
<tr>
<td>MartianSrc</td>
<td>IP packets with an invalid source address.</td>
</tr>
</tbody>
</table>

### Table 32: Global ICMP Statistics Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>OutResp</td>
<td>Echo replies sent from the CPU.</td>
</tr>
<tr>
<td>OutError</td>
<td>Redirect from broadcast or multicast source addresses.</td>
</tr>
<tr>
<td>InBadcode</td>
<td>Incoming ICMP packets with an invalid CODE value.</td>
</tr>
<tr>
<td>InTooshort</td>
<td>Incoming ICMP packets that are too short.</td>
</tr>
<tr>
<td>Bad chksum</td>
<td>Incoming ICMP packets with checksum errors.</td>
</tr>
<tr>
<td>In Badlen</td>
<td>Incoming ICMP packets with length errors.</td>
</tr>
<tr>
<td>echo reply (In/Out):</td>
<td>ICMP “echo reply” packets that are received and transmitted.</td>
</tr>
<tr>
<td>destination unreachable (In/Out):</td>
<td>ICMP packets with destination unreachable that are received and transmitted.</td>
</tr>
<tr>
<td>port unreachable (In/Out):</td>
<td>ICMP packets with port unreachable that are received and transmitted.</td>
</tr>
<tr>
<td>echo (In/Out):</td>
<td>ICMP echo packets that are received and transmitted.</td>
</tr>
</tbody>
</table>

### Table 33: Global IGMP Statistics Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Out Query</td>
<td>Number of IGMP query messages sent by the router.</td>
</tr>
<tr>
<td>Out Report</td>
<td>Number of reports sent on an active multicast route interface for reserved multicast addresses and for regular IGMP reports forwarded by the query router.</td>
</tr>
<tr>
<td>Out Leave</td>
<td>Number of IGMP out leave messages forwarded for IP multicast router interfaces.</td>
</tr>
<tr>
<td>In Query</td>
<td>Number of IGMP query messages received.</td>
</tr>
<tr>
<td>In Report</td>
<td>Number of IGMP report messages received (mostly from hosts).</td>
</tr>
<tr>
<td>In Leave</td>
<td>Number of IGMP leave messages received (mostly from hosts).</td>
</tr>
<tr>
<td>In Error</td>
<td>Number of IGMP packets with bad header fields or checksum failures.</td>
</tr>
</tbody>
</table>
**Table 34:** DHCP/BOOTP Statistics Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received to server</td>
<td>Number of DHCP packets forwarded to server.</td>
</tr>
<tr>
<td>Received to client</td>
<td>Number of DHCP packets received by clients.</td>
</tr>
<tr>
<td>Requests relayed</td>
<td>Number of DHCP request packets relayed.</td>
</tr>
<tr>
<td>Responses relayed</td>
<td>Number of DHCP response packets relayed.</td>
</tr>
<tr>
<td>DHCP Discover</td>
<td>Number of DHCP Discover messages.</td>
</tr>
<tr>
<td>DHCP Offer</td>
<td>Number of DHCP Offer messages.</td>
</tr>
<tr>
<td>DHCP Request</td>
<td>Number of DHCP Request messages.</td>
</tr>
<tr>
<td>DHCP Decline</td>
<td>Number of DHCP Decline responses.</td>
</tr>
<tr>
<td>DHCP Ack</td>
<td>Number of DHCP Ack responses.</td>
</tr>
<tr>
<td>DHCP NAck</td>
<td>Number of DHCP NAck responses.</td>
</tr>
<tr>
<td>DHCP Release</td>
<td>Number of DHCP Release instances.</td>
</tr>
<tr>
<td>DHCP Inform</td>
<td>Not used.</td>
</tr>
</tbody>
</table>

**Table 35:** Router Interface Statistics Field Definitions

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets IN/OUT</td>
<td>Total number of IP packets received or transmitted on a VLAN router interface.</td>
</tr>
<tr>
<td>Octets IN/OUT</td>
<td>Total number of octets received or transmitted on a VLAN router interface.</td>
</tr>
<tr>
<td>Mcast packets IN/OUT</td>
<td>Total number of multicast packets received or transmitted on a VLAN router interface.</td>
</tr>
<tr>
<td>Bcast packets IN/OUT</td>
<td>Total number of broadcast packets received or transmitted on a VLAN router interface.</td>
</tr>
<tr>
<td>Errors IN/OUT</td>
<td>Total number of IP packets with errors received or transmitted on a VLAN router interface.</td>
</tr>
<tr>
<td>Discards IN/OUT</td>
<td>Total number of IP packets that cannot travel up to the CPU due to lack of buffer space.</td>
</tr>
<tr>
<td>Unknown Protocols IN/OUT</td>
<td>Total number of IP packets with unknown upper layer protocols received by the router interface.</td>
</tr>
</tbody>
</table>

**Example**

The following command displays IP statistics for the VLAN *accounting*:

```
show ipstats vlan accounting
```

**History**

This command was available in ExtremeWare 2.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
show udp-profile

  show udp-profile \(<\text{profile\_name}>\)\)

**Description**
Displays the UDP profile information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>Specifies a UDP profile name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Displays the following information:
- Profile names
- Input rules of UDP port, destination IP address, or VLAN
- Source VLANs to which the profile is applied.

**Example**
The following command displays the UDP profile information for the UPD profile named *backbone*:

```
show udp-profile backbone
```

**History**
This command was first available in ExtremeWare 4.0.

This command was added to the “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
unconfigure bootprelay dhcp-agent information check

    unconfigure bootprelay dhcp-agent information check

Description
Disables the Dynamic Host Configuration Protocol (DHCP) relay agent information checking in the
DHCP reply packet.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
The following command configures DHCP relay agent option check:

    configure bootprelay dhcp-agent information check

To disable the DHCP relay agent information check in the DHCP reply packet, use the following
command:

    unconfigure bootprelay dhcp-agent information check

Example
The following command disables DHCP relay agent information checking in the DHCP reply packet:

    unconfigure bootprelay dhcp-agent information check

History
This command was available in ExtremeWare 7.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
unconfigure bootprelay dhcp-agent information option

Description
Disables the Dynamic Host Configuration Protocol (DHCP) relay agent option (option 82).

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
The following command configures the DHCP relay agent option:

configure bootprelay dhcp-agent information option

To disable the DHCP relay agent option (option 82), use the following command:

unconfigure bootprelay dhcp-agent information option

Example
The following command disables the DHCP relay agent option (option 82):

unconfigure bootprelay dhcp-agent information option

History
This command was available in ExtremeWare 7.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
unconfigure bootprelay dhcp-agent information policy

Description
Disables the Dynamic Host Configuration Protocol (DHCP) relay agent reforwarding policy.

Syntax Description
This command has no arguments or variables.

Default
Replace. (Replaces the existing the relay agent information with its own information.)

Usage Guidelines
The following command configures the DHCP relay agent reforwarding policy:

```
configure bootprelay dhcp-agent information policy <policy>
```

To disable the DHCP relay agent reforwarding policy, use the following command:

```
unconfigure bootprelay dhcp-agent information policy
```

Example
The following command disables the DHCP relay agent reforwarding policy:

```
unconfigure bootprelay dhcp-agent information policy
```

History
This command was available in ExtremeWare 7.2.

This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
unconfigure icmp

Description
Resets all ICMP settings to the default values.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command resets all ICMP settings to the default values.
unconfigure icmp

History
This command was available in ExtremeWare 2.0.
This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure iparp

unconfigure iparp

Description
Resets IP ARP timeout, IP ARP max-entries, and IP ARP max-pending-entries to their default values.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command resets all IP ARP related settings to the default values:
unconfigure iparp

History
This command was first available in ExtremeWare 6.2.
This command was added to the “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
unconfigure irdp

Description
Resets all router advertisement settings to the default values.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
None

Example
The following command resets all router advertisement settings to the default values.
unconfigure irdp

History
This command was available in ExtremeWare 2.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure udp-profile

    unconfigure udp-profile vlan [<vlan name> | all]

Description
Removes the UDP-forwarding profile configuration for one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all UDP profiles.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command removes the UDP profile configuration from the VLAN accounting:

unconfigure udp-profile vlan accounting

History
This command was first available in ExtremeWare 4.0.
This command was added to the “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
This chapter documents commands used for the following interior gateway protocols:

- OSPF
- RIP
- Integrated IS-IS for “i” series platforms

OSPF is a link-state protocol that distributes routing information between routers belonging to a single IP domain, also known as an autonomous system (AS). In a link-state routing protocol, each router maintains a database describing the topology of the autonomous system. Each participating router has an identical database maintained from the perspective of that router.

From the link-state database (LSDB), each router constructs a tree of shortest paths, using itself as the root. The shortest path tree provides the route to each destination in the autonomous system. When several equal-cost routes to a destination exist, traffic can be distributed among them. The cost of a route is described by a single metric.

OSPF allows parts of a network to be grouped together into areas. The topology within an area is hidden from the rest of the autonomous system. Hiding this information enables a significant reduction in LSA traffic, and reduces the computations needed to maintain the LSDB. Routing within the area is determined only by the topology of the area.

The three types of routers defined by OSPF are as follows:

- **Internal Router (IR)—** An internal router has all of its interfaces within the same area.
- **Area Border Router (ABR)—** An ABR has interfaces belonging to two or more areas. It is responsible for exchanging summary advertisements with other ABRs.
- **Autonomous System Border Router (ASBR)—** An ASBR acts as a gateway between OSPF and other routing protocols, or other autonomous systems.

Each switch that is configured to run OSPF must have a unique router ID. It is recommended that you manually set the router ID of the switches participating in OSPF, instead of having the switch automatically choose its router ID based on the highest interface IP address. Not performing this configuration in larger, dynamic environments could result in an older LSDB remaining in use.

**NOTE**

Do not set the router ID to 0.0.0.0.
Routing Information Protocol (RIP) is an Interior Gateway Protocol (IGP) first used in computer routing in the Advanced Research Projects Agency Network (ARPAnet) as early as 1969. It is primarily intended for use in homogeneous networks of moderate size.

To determine the best path to a distant network, a router using RIP always selects the path that has the least number of hops. Each router that data must traverse is considered to be one hop.

The routing table in a router using RIP contains an entry for every known destination network. Each routing table entry contains the following information:

- IP address of the destination network
- Metric (hop count) to the destination network
- IP address of the next router
- Timer that tracks the amount of time since the entry was last updated

The router exchanges an update message with each neighbor every 30 seconds (default value), or if there is a change to the overall routed topology (also called triggered updates). If a router does not receive an update message from its neighbor within the route timeout period (180 seconds by default), the router assumes the connection between it and its neighbor is no longer available.

A new version of RIP, called RIP version 2 (RIPv2), expands the functionality of RIP version 1 to include:

- Variable-Length Subnet Masks (VLSMs)
- Next-hop addresses
- Support for next-hop addresses allows for optimization of routes in certain environments
- Multicasting

If you are using RIP with supernetting/Classless Inter-Domain Routing (CIDR), you must use RIPv2 only, and RIP route aggregation must be turned off.

**On the “i” series platforms.** The Intermediate System to Intermediate System (IS-IS) routing protocol is a link-state protocol that is very similar to OSPF. ExtremeWare Integrated IS-IS support allows switches to act as IP-only IS-IS routers.

The IS-IS routing protocol provides transport-independent routing. IS-IS partitions the network into “routing domains.” Routing domain boundaries are defined by interior and exterior links. Interior links are part of the IS-IS routing domain; exterior links are not. No IS-IS routing messages are sent on exterior links.
clear isis adjacency

clear isis adjacency {level-1 | level-2 | level-1-2 | point-to-point} {vlan <vlan name>}

Description
Clear the IS-IS adjacencies currently present.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1 adjacencies.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2 adjacencies.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2 adjacencies.</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Specifies IS-IS point-to-point adjacencies.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The command clears IS-IS adjacencies. If no parameters are specified, all adjacencies, for all VLANs, are cleared.

Example
The following command clears the level 1 adjacencies for VLAN v1:
clear isis adjacency level 1 vlan v1

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
clear isis lsdb

    clear isis lsdb {level-2 | area <isis area identifier>} {system-identifier <system identifier> | sysName <alphanumeric string>} {type [non-pseudonode | pseudonode {circuit-identifier <number(1-255)>}] {lsp-number <number(0-255)>}}

**Description**

Clears the IS-IS LSDB of the level 2 subdomain or a level 1 area.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies the level 2 subdomain.</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies a level 1 area identifier.</td>
</tr>
<tr>
<td>system identifier</td>
<td>Specifies a system identifier. The format is xxxx.xxxx.xxxx, where x is a hexadecimal digit.</td>
</tr>
<tr>
<td>alphanumeric string</td>
<td>Specifies the system name of the switch.</td>
</tr>
<tr>
<td>type</td>
<td>Specifies LSDB type, non-pseudonode or pseudonode.</td>
</tr>
<tr>
<td>number(1-255)</td>
<td>Specifies a circuit ID from 1 to 255.</td>
</tr>
<tr>
<td>number(0-255)</td>
<td>Specifies an LSP number from 0 to 255.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command clears the IS-IS LSDB for the level 2 subdomain or a level 1 area. If no parameters are specified, all entries are cleared.

**Example**

The following command clears all non-pseudonode LSDB:

    clear isis lsdb type non-pseudonode

**History**

This command was first available in ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms.
configure isis add area address

configure isis [level-2 | area <isis area identifier>] add <area address>

Description
Adds an IS-IS area address for a level 2 subdomain or a level 1 area.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies level 2.</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies an area identifier.</td>
</tr>
<tr>
<td>area address</td>
<td>Specifies an area address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
At least one area address must be configured per area or subdomain, up to a maximum of three. Configuring multiple area addresses can be temporarily useful when multiple areas are merged, or when one area is split into multiple areas. Multiple area addresses enable you to remember an area individually as needed.

If no area address is configured, the IS-IS process will not start.

Example
The following command adds an IS-IS area address for level 2 subdomains:

```bash
configure isis level-2 add 02
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis add vlan

configure isis add vlan [vlan name] | all] [level-1 | level-1-2] area
<isis area identifier> | level-2-only]

Description
Enables IS-IS routing on a routing interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>isis area iden</td>
<td>Specifies an area identifier.</td>
</tr>
</tbody>
</table>

Default
By default, IS-IS is not enabled on an interface.

Usage Guidelines
A VLAN must have an IP address configured on it for it to become a routing interface.

The interface type is specified with the level-1, level-1-2, and level-2-only options. The interface type determines the adjacencies that can be established on the interface. The types are:

- level-1: A level 1 adjacency can be established if there is at least one area address in common between this system and its neighbors. Level 2 adjacencies are never established over this interface. The area identifier of the level 1 area in which the interface is present is specified with this option.
- level-1-2: Both level 1 and level 2 adjacency is established if the neighbor’s interface is also configured as level-1-2 and there is at least one area in common. If there is no area in common, a level 2 adjacency is established. The area identifier of the level 1 area in which the interface is present is specified with this option.
- level-2-only: level 2 adjacency is established if the neighbors interface is configured for level 1-2 or level 2. Level 1 adjacencies will never be established over this interface.

Example
The following command adds vlan test as level 2 only interfaces to IS-IS:

```
configure isis add vlan test level-2-only
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis area add domain-summary

configure isis area <isis area identifier> add domain-summary
<ip address> /<netmask> [advertise {cost <cost(0-4261412864)>} | noadvert]

Description
Adds a summary address to be applied on the IP reachability information from this level 1 area, which
will be included in the level 2 LSP.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis area identifier</td>
<td>Specifies an area identifier.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies the cost for the route (0-4,261,412,864).</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that the summarized IP reachability information may be included in the level 2 LSP.</td>
</tr>
<tr>
<td>noadvert</td>
<td>Specifies that the summary IP reachability information must not be included in the level 2.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
When the advertise option is configured, the summarized IP reachability information should be included in the level 2 LSP. The noadvert option filters out the summary.

Example
The following command adds the domain summary address 10.0.0.0/8 to the level 1 area a1, advertises the address and sets the cost to 15:

```
configure isis area a1 add domain-summary 10.0.0.0/8 advertise cost 15
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis area delete domain-summary

configure isis area <isis area identifier> delete domain-summary
<ip address> /<netmask>

Description
Deletes a summary address to be applied on the IP reachability information from this level 1 area, which will be included in the level 2 LSP.

Syntax Description

<table>
<thead>
<tr>
<th>isis area identifier</th>
<th>Specifies an area identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies an IP mask</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
When the summary address is deleted, the summarized IP reachability information must not be included in the level 2 LSP.

Example
The following command deletes one summary address 10.0.0.0/8 from the level 1 area a1:
configure isis area a1 delete domain-summary 10.0.0.0/8

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis area domain-filter

configure isis area <isis area identifier> domain-filter [<access profile> | none]

Description
Configures an access profile to filter the IP reachability information from this level 1 area that will be included in the level 2 LSP:

Syntax Description

<table>
<thead>
<tr>
<th>isis area identifier</th>
<th>Specifies an area identifier.</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no access profile.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
When an access profile is not configured, none of the information is filtered. By default, no access profile is present on a level 1 area.

Example
The following command configures access profile ap1 as the domain filter for the area a1:

```
configure isis area a1 domain-filter ap1
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis authentication

configure isis {level-2 | area <isis area identifier>} authentication
[simple-password <isis simple password> {no-check} | hmac-md5 <hmac-md5> (no-check) | none]

Description
Configures authentication for a level 2 subdomain or a level 1 area.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies to configure authentication for a level 2 subdomain.</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies an area.</td>
</tr>
<tr>
<td>isis simple password</td>
<td>Specifies a text password in the transmitted packet.</td>
</tr>
<tr>
<td>no-check</td>
<td>Specifies not to drop received packets that cannot be authenticated.</td>
</tr>
<tr>
<td>hmac-md5</td>
<td>Specifies an MD5 authentication key.</td>
</tr>
</tbody>
</table>

Default
By default, authentication is not configured.

Usage Guidelines
Two types of authentication are supported: simple password and HMAC-MD5. Simple password authentication inserts a text password in the transmitted packet. HMAC-MD5 authentication inserts an authentication key that is generated using a cryptographic hash function, HMAC, on the data present in the packet. The no-check option prevents the system from dropping received packets that cannot be authenticated.

Example
The following command configures authentication using the simple password “extreme” with no checking for the level 2 subdomain:

configure isis level-2 authentication simple-password extreme no-check

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis delete area-address

configure isis [level-2 | area <isis area identifier>] delete <area address>

Description
Deletes an IS-IS area address for a level 2 subdomain or a level 1 area.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis area identifier</td>
<td>Specifies the area identifier.</td>
</tr>
<tr>
<td>area address</td>
<td>Specifies the area address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
At least one area address must be configured per area or subdomain, up to a maximum of three. Configuring multiple area addresses can be temporarily useful when multiple areas are merged, or when one area is split into multiple areas. Multiple area addresses enable you to remember an area individually as needed.

If no area address is configured, the IS-IS process will not start.

Example
The following command deletes an IS-IS area address 00.0001 for the level 2 subdomain:

```
configure isis level-2 delete 00.0001
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis delete vlan

configure isis delete vlan [<vlan name> | all]

Description
Disables IS-IS routing on a routing interface.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
By default, IS-IS is not enabled on an interface.

Usage Guidelines
None.

Example
The following command disables IS-IS on all VLANs.

configure isis delete vlan all

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis external-filter

configure isis [level-2 | area <isis area identifier>] external-filter [<access profile> | none]

Description
Configures an access profile to filter routes being redistributed into the level 1 area or level 2 subdomain.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis area identifier</td>
<td>Specifies an area identifier.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

Default
By default no access profile is present.

Usage Guidelines
The filter is applied on the routes from all the non-IS-IS origins. When an access profile is not configured, none of the routes are filtered.

Example
The following command configures an external filter for a level 1 area with the access profile ap:

```
configure isis area a1 external-filter ap
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis lsp holddown interval

    configure isis lsp-holddown-interval <seconds>

Description
Configures the LSP hold down interval.

Syntax Description

<table>
<thead>
<tr>
<th>seconds</th>
<th>Specifies the LSP hold down interval in seconds.</th>
</tr>
</thead>
</table>

Default
10 seconds.

Usage Guidelines
The LSP hold down interval range is from 3 to 120 seconds.

Example
The following command configures the LSP hold down interval:
configure isis lsp-holddown-interval 20

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis lsp lifetime

configure isis lsp-lifetime <seconds>

**Description**

Configures the LSP lifetime.

**Syntax Description**

| seconds | Specifies the LSP lifetime in seconds. |

**Default**

1200 seconds.

**Usage Guidelines**

You can only use this command when IS-IS is disabled.

The LSP lifetime range is from 400 to 65,535 seconds.

**Example**

The following command sets the LSP lifetime to 1000:

```
configure isis lsp-lifetime 1000
```

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms.
configure isis lsp refresh interval

    configure isis lsp-refresh-interval <seconds>

Description
Configures the LSP refresh interval.

Syntax Description

<table>
<thead>
<tr>
<th>seconds</th>
<th>Specifies the LSP refresh interval in seconds.</th>
</tr>
</thead>
</table>

Default
900 seconds.

Usage Guidelines
You can only use this command when IS-IS is disabled.
The LSP refresh interval range is from 100 to 65,235 seconds.

Example
The following command configures the LSP refresh interval:
configure isis lsp-refresh-interval 120

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis metric-size

configure isis [level-2 | area <isis area identifier>] metric-size [regular | wide | both]

Description
Configures the size of the metric originated in the LSP for the level 2 subdomain or level 1 area.

Syntax Description

| isis area identifier | Specifies an area identifier. |

Default
The default setting is regular.

Usage Guidelines
The regular option indicates that the metric can have a maximum value of 63 (as specified in the basic specifications). The wide option indicates that the metric can have a maximum value of 4,261,412,864 (as specified in the traffic engineering draft). The both option indicates that the metric should be described in both formats.

You can only use this command when IS-IS is disabled.

Example
The following command configures the metric size as both for the level 2 subdomain:

```
confi isis level-2 metric-size both
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis spf hold time

configure isis spf-hold-time <seconds>

**Description**

Configures the shortest-path-first hold time.

**Syntax Description**

| seconds | Specifies the SPF hold time in seconds. |

**Default**

3 seconds.

**Usage Guidelines**

The SPF hold time range is from 1 to 300 seconds.

**Example**

The following command configures the IS-IS shortest-path-first hold time:

```
configure isis spf-hold-time 7
```

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms.
configure isis system-identifier

    configure isis system-identifier <system identifier>

**Description**
Configures a 6 hex octet system identifier for IS-IS routing.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>system identifier</td>
<td>Specifies the 6 hex octet system identifier. The format is xxxx.xxxx.xxxx where x represents a hexadecimal digit.</td>
</tr>
</tbody>
</table>

**Default**
By default, the system identifier is set to the switch’s MAC address. This command overrides that default.

**Usage Guidelines**
The system identifier can only be configured when IS-IS processing is disabled.

**Example**
The following command sets the system identifier:

```
configure isis system-identifier 0000.0000.001a
```

**History**
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the “i” series platforms.
configure isis vlan

configure isis [vlan <vlan name> | all] [level-1 | level-2 | level-1-2] [passive | non-passive]

Description
Configures the different IS-IS levels on a routing interface as passive or non-passive.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2.</td>
</tr>
<tr>
<td>passive</td>
<td>Specifies passive.</td>
</tr>
<tr>
<td>non-passive</td>
<td>Specifies non-passive.</td>
</tr>
</tbody>
</table>

Default
By default, all the routing interfaces are non-passive.

Usage Guidelines
If all is specified, all routing interfaces in the system are configured as passive or non-passive.

When a level on an interface is configured as passive, the corresponding Hello packets are not sent or received on that interface. Any packet that is received is ignored. As a result of this no adjacency is established.

Example
The following command configures vlan v1 as a level 2 passive interface

```
configure isis vlan v1 level-2 passive
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis vlan authentication

configure isis vlan <vlan name> [level-1 | level-2 | level-1-2] authentication [simple-password <isis simple password> {no-check} | hmac-md5 <hmac-md5> {no-check} | none]

Description

Configures authentication on a VLAN for the IS-IS levels on a routing interface:

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2.</td>
</tr>
<tr>
<td>isis simple password</td>
<td>Specifies simple password authentication.</td>
</tr>
<tr>
<td>no-check</td>
<td>Specifies not to drop packets that cannot be authenticated.</td>
</tr>
<tr>
<td>md5 key</td>
<td>Specifies HMAC-MD5 authentication.</td>
</tr>
</tbody>
</table>

Default

An interface does not have any authentication configured on it by default.

Usage Guidelines

Two types of authentication are supported: simple password and HMAC-MD5. Simple password authentication inserts a text password in the transmitted packet. HMAC-MD5 authentication inserts an authentication key that is generated using the cryptographic hash function, HMAC, on the data present in the packet. The no-check option prevents the system from dropping received packets that cannot be authenticated.

The level-1, level-2, and level-1-2 options specify the levels on which the authentication is to be configured.

Example

The following command configures authentication for level 1 and level 2 to use the simple password “extreme” for vlan v1, and to drop non-authenticated packets:

configure isis vlan v1 level-1-2 authentication simple-password extreme

History

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the “i” series platforms.
configure isis vlan cost

configure isis [vlan <vlan name> | all] [level-1 | level-2 | level-1-2] cost <cost>

Description
Configures the IS-IS metric for the different IS-IS levels of a routing interface.

Syntax Description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies the cost value.</td>
</tr>
</tbody>
</table>

Default
The default cost value is 10.

Usage Guidelines
Extreme Networks recommends that you configure metrics on all interfaces. If you do not, the IS-IS metrics are similar to hop-count metrics.

If all is specified, the metric is applied to all the routing interfaces in the system.

The range of cost is 0 to 16,777,215, where 16,777,215 is the maximum value allowed with wide metrics. If cost is greater than 63, a value of 63 is advertised as the regular metric of the interface. The default is 10.

The level-1, level-2, and level-1-2 options specify the levels to which the metric is applied.

Example
The following command configures the level 1 vlan v1 cost as 25:

```
configure isis vlan v1 level-1 cost 25
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on all platforms.
configure isis vlan hello-multiplier

configure isis [vlan <vlan name> | all] [level-1 | level-2 | level-1-2] hello-multiplier <number(3-1000)>

Description
Configures the number of IS-IS Hello packets an IS-IS neighbor at a particular level on this routing interface must miss before the it declares that the adjacency with this system is down.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2.</td>
</tr>
<tr>
<td>hello-multiplier</td>
<td>Specifies the hello multiplier.</td>
</tr>
</tbody>
</table>

Default
The default hello multiplier number is 3.

Usage Guidelines
If all is specified, the hello multiplier is applied to all the routing interfaces in the system. The advertised hold time in the IS-IS hellos is the hello multiplier times the hello interval.

The hello multiplier range is 3 to 1000, and the default is 3.

The level-1, level-2, and level-1-2 options specify the levels to which the timers are applied.

Example
The following command configures the hello multiplier on level 1 of all VLANs to be 100.

configure isis vlan all level-1 hello-multiplier 100

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on all platforms.
configure isis vlan priority

configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2] priority <priority>

Description
Configures the IS-IS priority for the IS-IS levels of a routing interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies the priority to apply to IS-IS levels. Range is 0 to 127. Default is 64.</td>
</tr>
</tbody>
</table>

Default
The default priority is 64.

Usage Guidelines
If all is specified, the priority is applied to all the routing interfaces in the system. The priority in applicable only for broadcast routing interfaces. The priorities are advertised in the Hello packets. The router with the higher priority at a particular level becomes the designated IS for that level on that interface. The range of priority is 0 to 127, and the default is 64.

The level-1, level-2, and level-1-2 options specify the levels for which the priority is applied.

Example
The following command configures an IS-IS priority of 100 to level 1 of all VLANs.

configure isis vlan all level-1 priority 100

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
configure isis vlan timer

configure isis [vlan <vlan name> | all] [level-1| level-2 | level-1-2] timer [csnp <seconds>| hellotime <seconds>]

Description
Configures the IS-IS timer interval for the different levels of a routing interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of a VLAN.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>level-1</td>
<td>Specifies IS-IS level 1.</td>
</tr>
<tr>
<td>level-2</td>
<td>Specifies IS-IS level 2.</td>
</tr>
<tr>
<td>level-1-2</td>
<td>Specifies IS-IS level 1 and level 2.</td>
</tr>
<tr>
<td>csnp</td>
<td>Specifies the time in seconds between CSNP transmissions. Range is 1 to 3600. Default is 10.</td>
</tr>
<tr>
<td>hellotime</td>
<td>Specifies the time in seconds between Hello PDU transmissions. Range is 3 to 3600. Default is 10.</td>
</tr>
</tbody>
</table>

Default
The default for CSNP and Hello timer is 10 seconds.

Usage Guidelines
If all is specified, the timer intervals are applied to all the routing interfaces in the system. The command configures both the CSNP and Hello timer values.

The csnp interval is the time in seconds between transmission of CSNPs on multi access networks. This interval applies for the designated router. The range is 1 to 3600, and the default is 10.

The hellotime interval is the time in seconds between transmission of Hello PDUS on the interface. The range is 3 to 3600, and the default is 10.

The level-1, level-2, and level-1-2 options specify the levels to which the timers are applied.

Example
The following command configures the level 1 hellotime interval to 60 seconds for all VLANs

```
configure isis vlan all level-1 timer hellotime 60
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.
Platform Availability

This command is available on the “i” series platforms.
configure ospf add virtual-link

configure ospf add virtual-link <routerid> <area identifier>

Description
Adds a virtual link connected to another ABR.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routerid</td>
<td>Specifies an IP address that identifies the router.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
A virtual link provides a logical path between the ABR of the disconnected area and the ABR of the normal area that connects to the backbone. A virtual link must be established between two ABRs that have a common area, with one ABR connected to the backbone. Specify the following:

- routerid—Far-end router identifier number.
- area identifier—Transit area used for connecting the two end-points. The transit area cannot have the IP address 0.0.0.0. The transit area cannot be a stub area or an NSSA.

Example
The following command configures a virtual link between the two interfaces:

```
configure ospf add virtual-link 10.1.2.1 10.1.0.0
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf add vlan area

configure ospf add vlan [<vlan name> | all] area <area identifier> {passive}

Description
Enables OSPF on one or all VLANs (router interfaces).

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name to be associated with an OSPF area.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs to be associated with an OSPF area.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies the area to which the VLAN is assigned.</td>
</tr>
<tr>
<td>passive</td>
<td>Specifies to stop sending and receiving hello packets on this interface.</td>
</tr>
</tbody>
</table>

Default
Area 0.0.0.0

Usage Guidelines
Associates a VLAN (router interface) with an OSPF area. By default, all router interfaces are associated with area 0.0.0.0. Any OSPF network that contains more than one area is required to have an area configured as area 0, also called the backbone. All areas in an autonomous system must be connected to the backbone. When designing networks, you should start with area 0, and then expand into other areas.

The backbone allows summary information to be exchanged between ABRs. Every ABR hears the area summaries from all other ABRs. The ABR then forms a picture of the distance to all networks outside of its area by examining the collected advertisements, and adding in the backbone distance to each advertising router.

When a VLAN is configured to run OSPF, by default you must assign it to an area.

On the “e” series switches. The Summit “e” series of switches allow up to two non-passive interfaces. If a user attempts to configure more than two non-passive interfaces, the Summit switch displays the following warning message:

Cannot enable OSPF on vlan <name>. Non-passive interface limit reached.

Using OSPF and MPLS. The following detailed information pertains to using OSPF in conjunction with MPLS. When the peer LSR is also an Extreme switch, the following options are available for ensuring that an OSPF route is advertised for the tunnel endpoint IP address:

- A route is advertised when OSPF is enabled on the VLAN to which the IP address is assigned (using the configure ospf add vlan command on the peer switch).
- A route is advertised when the peer switch is configured to distribute direct routes into the OSPF domain (via the enable ospf export direct command). The export option should be used when the tunnel LSP needs to cross OSPF area boundaries or when the Extreme Standby Routing Protocol (ESRP) is enabled on the VLAN to which the IP address is assigned.
In either case, LDP must be configured to advertise label mappings for direct routing interfaces.

In some configurations, you may want to enable loopback mode on the VLAN to which the tunnel endpoint IP address is assigned. One situation where loopback mode may be useful is when multiple physical interfaces, associated with different VLANs, are connected to the MPLS backbone. In this case, use of loopback-mode can provide redundancy by enabling TLS traffic to continue even when the physical interfaces associated with the tunnel endpoint IP address VLAN fail.

**Example**

The following command enables OSPF on a VLAN named *accounting*:

```bash
configure ospf add vlan accounting area 0.0.0.1
```

**History**

This command was first available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in an ExtremeWare 7.2e to support the `all` keyword.

**Platform Availability**

This command is available on all platforms.
configure ospf add vlan area link-type

configure ospf add vlan [vlan name | all] area area identifier link-type [auto | broadcast | point-to-point] [passive]

Description
Configures the OSPF link type.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANS.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies the area to which the VLAN is assigned.</td>
</tr>
<tr>
<td>auto</td>
<td>Specifies to automatically determine the OSPF link type based on the interface type.</td>
</tr>
<tr>
<td>broadcast</td>
<td>Specifies a broadcast link, such as Ethernet. Routers must elect a DR and a BDR during synchronization.</td>
</tr>
<tr>
<td>point-to-point</td>
<td>Specifies a point-to-point link type, such as PPP.</td>
</tr>
<tr>
<td>passive</td>
<td>Specifies to stop sending and receiving packets on this interface.</td>
</tr>
</tbody>
</table>

Default
Auto.

Usage Guidelines
The passive parameter indicates that the router only synchronizes and listens, and does not originate or send any new information on the interface.

Example
The following command configures the OSPF link type as automatic on a VLAN named accounting:

configure ospf add vlan accounting area 0.0.0.1 link-type auto

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2e to support the all keyword.

Platform Availability
This command is available on all platforms.
configure ospf area add range

configure ospf area <area identifier> add range <ipaddress> <mask>
[advertise | noadvertise] {type-3 | type-7}

Description
Configures a range of IP addresses in an OSPF area to be aggregated.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies to advertise the aggregated range of IP addresses.</td>
</tr>
<tr>
<td>noadvertise</td>
<td>Specifies not to advertise the aggregated range of IP addresses.</td>
</tr>
<tr>
<td>type-3</td>
<td>Specifies type 3 LSA, summary LSA.</td>
</tr>
<tr>
<td>type-7</td>
<td>Specifies type 7 LSA, NSSA external LSA.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If advertised, the aggregated IP range is exported as a single LSA by the ABR.

Example
The following command is used to summarize a certain range of IP addresses within an area and export them out as a single address:

```
configure ospf area 1.2.3.4 add range 10.1.2.0/24 advertise type-3
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf area delete range

configure ospf area <area identifier> delete range <ipaddress> <mask>

Description
Deletes a range of aggregated IP addresses in an OSPF area.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command deletes an aggregated IP address range:

```
configure ospf area 1.2.3.4 delete range 10.1.2.0/24
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf area external-filter

configure ospf area <area identifier> external-filter [<access profile> |none]

Description
Configures an external filter policy.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies the OSPF target area.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies not to apply an external filter.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
For switches configured to support multiple OSPF areas (an ABR function), an access profile can be applied to an OSPF area that filters a set of OSPF external routes from being advertised into that area.

NOTE
If any of the external routes specified in the filter have already been advertised, those routes will remain until the associated LSAs in that area time-out.

Using the none mode specifies that no external filter is applied.

Example
The following command configures an external filter policy from the access profile nosales:

configure ospf area 1.2.3.4 external-filter nosales

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf area interarea-filter

    configure ospf area <area identifier> interarea-filter [<access profile> | none]

Description
Configures a global inter-area filter policy.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies the OSPF target area.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies not to apply an interarea filter.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
For switches configured to support multiple OSPF areas (an ABR function), an access profile can be applied to an OSPF area that filters a set of OSPF inter-area routes from being sourced from any other areas.

Example
The following command configures an inter-area filter policy from the access profile nosales:

```
configure ospf area 0.0.0.6 interarea-filter nosales
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf area normal

    configure ospf area <area identifier> normal

Description
Configures an OSPF area as a normal area.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

Default
Normal.

Usage Guidelines
A normal area is an area that is not any of the following:
- Stub area
- NSSA

Virtual links can be configured through normal areas. External routes can be distributed into normal areas.

Example
The following command configures an OSPF area as a normal area:

```
configure ospf area 10.1.0.0 normal
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf area nssa stub-default-cost

configure ospf area <area identifier> nssa [summary | nosummary] stub-default-cost <cost> {translate}

Description
Configures an OSPF area as an NSSA.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>summary</td>
<td>Specifies that type-3 can be propagated into the area.</td>
</tr>
<tr>
<td>nosummary</td>
<td>Specifies that type-3 cannot be propagated into the area.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>translate</td>
<td>Specifies whether type-7 LSAs are translated into type-5 LSAs.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
NSSAs are similar to the existing OSPF stub area configuration option, but have the following two additional capabilities:

- External routes originating from an ASBR connected to the NSSA can be advertised within the NSSA.
- External routes originating from the NSSA can be propagated to other areas, including the backbone area, if translated to type 5 LSAs.

When configuring an OSPF area as an NSSA, the translate option should only be used on NSSA border routers, where translation is to be enforced. If translate is not used on any NSSA border router in a NSSA, one of the ABRs for that NSSA is elected to perform translation (as indicated in the NSSA specification). The option should not be used on NSSA internal routers. Doing so inhibits correct operation of the election algorithm.

Example
The following command configures an OSPF area as an NSSA:

```
configure ospf area 10.1.1.0 nssa summary stub-default-cost 10 translate
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf area stub stub-default-cost

configure ospf area <area identifier> stub [summary | nosummary] stub-default-cost <cost>

Description
Configures an OSPF area as a stub area.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>summary</td>
<td>Specifies that type-3 can be propagated into the area.</td>
</tr>
<tr>
<td>nosummary</td>
<td>Specifies that type-3 cannot be propagated into the area.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a cost metric.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
A stub area is connected to only one other area. The area that connects to a stub area can be the backbone area. External route information is not distributed into stub areas. Stub areas are used to reduce memory and computation requirements on OSPF routers.

Example
The following command configures an OSPF area as a stub area:

```
configure ospf area 0.0.0.6 stub nosummary stub-default-cost 10
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf asbr-filter

configure ospf asbr-filter [<access profile> | none]

Description
Configures a route filter for all OSPF exported routes.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies not to apply an ASBR filter.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines

For “i” series switches. For switches configured to support RIP, BGP, VIP, IS-IS, and static route re-distribution into OSPF, an access profile can be used to limit the routes that are advertised into OSPF for the switch as a whole.

For “e” series switches. For switches configured to support RIP and static route re-distribution into OSPF, an access profile can be used to limit the routes that are advertised into OSPF for the switch as a whole.

Example
The following command configures a route filter for all routes OSPF exports from RIP or other sources:

```
configure ospf asbr-filter subnet25-filter
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf ase-limit

   configure ospf ase-limit <number> {timeout <seconds>}

Description
Configures the AS-external LSA limit and overflow duration associated with OSPF database overflow handling.

Syntax Description

<table>
<thead>
<tr>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
</tr>
<tr>
<td>seconds</td>
</tr>
</tbody>
</table>

Default
The default for timeout is 0, which indicates that once the router goes into overflow state, it stays there until OSPF is disabled and then re-enabled.

Usage Guidelines
None.

Example
The following command configures the AS-external LSA limit and overflow duration:

configure ospf ase-limit 50000 timeout 1800

History
This command was available in ExtremeWare 6.1.5.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf ase-summary add

```
configure ospf ase-summary add <ip address> <mask> cost <cost>
{tag <number>}
```

**Description**
Aggregates AS-external routes in a specified address range.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a metric that will be given to the summarized route.</td>
</tr>
<tr>
<td>tag</td>
<td>Specifies an OSPF external route tag.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
This command is only valid on an ASBR.

**Example**
The following command summarizes AS-external routes:

```
configure ospf ase-summary add 175.1.0.0/16 cost 10
```

**History**
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure ospf ase-summary delete

configure ospf ase-summary delete <ip address> <mask>

Description
Deletes an aggregated OSPF external route.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command is only valid on an ASBR.

Example
The following command deletes the aggregated AS-external route:

```
configure ospf ase-summary delete 175.1.0.0/16
```

History
This command was first available in ExtremeWare 6.1.5.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf cost

configure ospf [area <area identifier> | vlan [<vlan name> | all]] cost [automatic | <cost>]

Description
Configures the cost metric of one or all OSPF interface(s) for all the interfaces within the area.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>automatic</td>
<td>Determine the advertised cost from the OSPF metric table.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies the cost metric.</td>
</tr>
</tbody>
</table>

Default
The default cost is automatic.

Usage Guidelines
None.

Example
The following command configures the cost metric of the VLAN accounting:

```
configure ospf vlan accounting cost 10
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf delete virtual-link

configure ospf delete virtual-link <routerid> <area identifier>

Description
Removes a virtual link.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routerid</td>
<td>Specifies a router interface number.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command deletes a virtual link:

```
configure ospf delete virtual-link 10.1.2.1 10.1.0.0
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf delete vlan

configure ospf delete vlan [<vlan name> | all]

**Description**
Disables OSPF on one or all VLANs (router interfaces).

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command disables OSPF on VLAN `accounting`:

```
configure ospf delete vlan accounting
```

**History**
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure ospf direct-filter

configure ospf direct-filter [<access profile> | none]

Description
Configures a route filter for direct routes.

Syntax Description

<table>
<thead>
<tr>
<th>access profile</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies not to apply a direct filter.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If none is specified, all direct routes are exported if ospf export direct is enabled.

In versions of ExtremeWare before release 6.0, direct routes corresponding to the interfaces on which RIP was enabled were exported into OSPF as part of RIP routes, using the command enable ospf export rip. Using ExtremeWare 6.0 and above, you must configure ExtremeWare to export these direct routes to OSPF. You can use an access profile to filter unnecessary direct routes.

For switches configured to support direct route re-distribution into OSPF, an access profile can be used to limit the routes that are advertised into OSPF for the switch as a whole.

Example
The following command configures a route filter for direct routes based on the access profile nosales:

```
configure ospf direct-filter nosales
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf lsa-batch-interval

    configure ospf lsa-batch-interval <seconds>

Description
Configures the OSPF LSA batching interval.

Syntax Description

<table>
<thead>
<tr>
<th>seconds</th>
<th>Specifies a time in seconds.</th>
</tr>
</thead>
</table>

Default
The default setting is 30 seconds.

Usage Guidelines
The range is between 0 (disabled) and 600 seconds, using multiples of 5 seconds. The LSAs added to the LSDB during the interval are batched together for refresh or timeout.

Example
The following command configures the OSPF LSA batch interval to a value of 100 seconds:

configure ospf lsa-batch-interval 100

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure ospf metric-table

    configure ospf metric-table 10M <cost> 100M <cost> 1G <cost> {10G <cost>}

Description
Configures the automatic interface costs for 10 Mbps, 100 Mbps, 1 Gbps, and 10 Gbps interfaces.

Syntax Description

| cost | Specifies the interface cost for the indicated interfaces. |

Default
- 10 Mbps—The default cost is 10.
- 100 Mbps—The default cost is 5.
- 1 Gbps—The default cost is 4.
- 10 Gbps—The default cost is 2.

Usage Guidelines
None.

Example
The following command configures the automatic interface costs for 10 Mbps, 100 Mbps, and 1 Gbps interfaces:

```
configure ospf metric-table 10m 20 100m 10 1g 2
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf priority

configure ospf [area <area identifier> | vlan [<vlan name> | all]] priority <priority>

Description
Configures the priority used in the designated router-election algorithm for one or all OSPF interface(s) for all the interfaces within the area.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a priority range. The range is 0 through 255.</td>
</tr>
</tbody>
</table>

Default
The default setting is 1.

Usage Guidelines
The range is 0 through 255, and the default setting is 1. Setting the value to 0 ensures that the router is never selected as the designated router or backup designated router.

Example
The following command sets the switch to not be selected as the designated router:

```
configure ospf area 1.2.3.4 priority 0
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure ospf routerid

    configure ospf routerid [automatic | <routerid>]

Description
Configures the OSPF router ID. If automatic is specified, the switch uses the highest IP interface address as the OSPF router ID.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>automatic</td>
<td>Specifies to use automatic addressing.</td>
</tr>
<tr>
<td>routerid</td>
<td>Specifies a router address.</td>
</tr>
</tbody>
</table>

Default
Automatic.

Usage Guidelines
Each switch that is configured to run OSPF must have a unique router ID. It is recommended that you manually set the router ID of the switches participating in OSPF, instead of having the switch automatically choose its router ID based on the highest interface IP address. Not performing this configuration in larger, dynamic environments could result in an older link-state database remaining in use.

NOTE
Do not set the router ID to 0.0.0.0.

The implementation of the configure ospf routerid command has been augmented to support automatic advertisement of a label mapping for the OSPF router ID. A label is advertised for the OSPF router ID regardless of whether OSPF distributes a route for the router ID IP address in its router LSA.

To support the use of indirect LSPs, Extreme LSRs automatically advertise a label mapping for a /32 LSP to its OSPF router ID (configured using the configure ospf routerid command).

Example
The following command sets the router ID:

    configure ospf routerid 10.1.6.1

History
This command was available in ExtremeWare 2.0.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
configure ospf spf-hold-time

configure ospf spf-hold-time <seconds>

Description
Configures the minimum number of seconds between Shortest Path First (SPF) recalculations.

Syntax Description

| seconds | Specifies a time in seconds. |

Default
3 seconds.

Usage Guidelines
None.

Example
The following command configures the minimum number of seconds between Shortest Path First (SPF) recalculations:

```
configure ospf spf-hold-time 6
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf timer

configure ospf [vlan <vlan name> | area <area identifier> | virtual-link <routerid> <area identifier>] timer <retransmit interval> <transit delay> <hello interval> <dead interval> {<wait timer interval>}

Description
Configures the timers for one interface or all interfaces in the same OSPF area.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>routerid</td>
<td>Specifies a router number.</td>
</tr>
<tr>
<td>retransmit interval</td>
<td>Specifies the length of time that the router waits before retransmitting an LSA that is not acknowledged. The range is 0 - 3,600 seconds.</td>
</tr>
<tr>
<td>transit delay</td>
<td>Specifies the length of time it takes to transmit an LSA packet over the interface. The range is 0 - 3,600 seconds.</td>
</tr>
<tr>
<td>hello interval</td>
<td>Specifies the interval at which routers send hello packets. The range is 1 - 65,535 seconds.</td>
</tr>
<tr>
<td>dead interval</td>
<td>Specifies the interval after which a neighboring router is declared down due to the fact that hello packets are no longer received from the neighbor. The range is 1 - 2,147,483,647 seconds.</td>
</tr>
<tr>
<td>wait timer interval</td>
<td>Specifies the interval between the interface coming up and the election of the DR and BDR. Usually equal to the dead timer interval.</td>
</tr>
</tbody>
</table>

Default
- retransmit interval—Default: 5
- transit delay—Default: 1
- hello interval—Default: 10
- dead interval—Default: 40
- wait timer interval—Default: dead interval

Usage Guidelines
Configuring OSPF timers and authentication on a per-area basis is a shorthand for applying the timers and authentication to each VLAN in the area at the time of configuration. If you add more VLANs to the area, you must configure the timers and authentication for the new VLANs explicitly.

Example
The following command sets the timers on the virtual link in area 0.0.0.2:

```
configure ospf virtual-link 6.6.6.6 0.0.0.2 timer 10 1 20 200
```

History
This command was available in ExtremeWare 2.0.
The syntax was modified in ExtremeWare 6.2.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

The syntax was modified in ExtremeWare 7.2e to support the wait timer interval.

**Platform Availability**

This command is available on all platforms.
configure ospf virtual-link authentication password

configure ospf [vlan <vlan name> | area <area identifier> | virtual-link <routerid> <area identifier>] authentication [simple-password <password> | md5 <md5_key_id> <md5_key> | none | encrypted [simple-password <password> | md5 <md5_key_id> <md5_key>]

Description
Specifies the authentication password (up to eight characters) or Message Digest 5 (MD5) key for one or all interfaces in an area.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>routerid</td>
<td>Specifies a router identifier number.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies an authentication password (up to 8 ASCII characters).</td>
</tr>
<tr>
<td>md5-key_id</td>
<td>Specifies a Message Digest 5 key, from 0-255.</td>
</tr>
<tr>
<td>md5_key</td>
<td>Specifies a numeric value from 0-65,536. Can also be alphanumeric</td>
</tr>
<tr>
<td>none</td>
<td>Disables authentication.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The md5_key is a numeric value with the range 0 to 65,536 or alphanumeric. When the OSPF area is specified, authentication information is applied to all OSPF interfaces within the area.

Example
The following command configures MD5 authentication on the VLAN subnet_26:

```
configure ospf vlan subnet_26 authentication md5 32 test
```

History
This command was available in ExtremeWare 7.2e.

Platform Availability
This command is available on the “e” series platforms.
configure ospf vlan area

configure ospf [all | vlan <vlan name>] area <area identifier>

Description
Associates a VLAN (router interface) with an OSPF area. By default, all router interfaces are associated with area 0.0.0.0.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

Default
Area 0.0.0.0

Usage Guidelines
Any OSPF network that contains more than one area is required to have an area configured as area 0, also called the backbone. All areas in an autonomous system must be connected to the backbone. When designing networks, you should start with area 0, and then expand into other areas.

The backbone allows summary information to be exchanged between ABRs. Every ABR hears the area summaries from all other ABRs. The ABR then forms a picture of the distance to all networks outside of its area by examining the collected advertisements, and adding in the backbone distance to each advertising router.

When a VLAN is configured to run OSPF, by default you must assign it to an area.

Example
The following command associates the VLAN accounting with an OSPF area:

```
configure ospf vlan accounting area 0.0.0.6
```

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on the “i” series platforms.
**configure ospf vlan neighbor add**

configure ospf vlan <vlan name> neighbor add <ipaddress>

**Description**

Configures the IP address of a point-to-point neighbor.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

None.

**Example**

The following command configures the IP address of a point-to-point neighbor:

configure ospf vlan accounting neighbor add 10.0.0.1

**History**

This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
configure ospf vlan neighbor delete

configure ospf vlan <vlan name> neighbor delete <ipaddress>

Description
Deletes the IP address of a point-to-point neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command deletes the IP address of a point-to-point neighbor:

```
configure ospf vlan accounting neighbor delete 10.0.0.1
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure ospf vlan timer

configure ospf vlan <vlan name> timer <retransmit interval> <transit delay> <hello interval [1-655191]> <dead interval> {<wait timer interval>}

Description
Configures the OSPF timer intervals.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>retransmit interval</td>
<td>Specifies the length of time that the router waits before retransmitting an LSA that is not acknowledged.</td>
</tr>
<tr>
<td>transit delay</td>
<td>Specifies the length of time it takes to transmit an LSA packet over the interface.</td>
</tr>
<tr>
<td>hello interval</td>
<td>Specifies the interval at which routers send hello packets.</td>
</tr>
<tr>
<td>dead interval</td>
<td>Specifies the interval after which a neighboring router is declared down due to the fact that hello packets are no longer received from the neighbor.</td>
</tr>
<tr>
<td>wait timer interval</td>
<td>Specifies the interval between the interface coming up and the election of the DR and BDR.</td>
</tr>
</tbody>
</table>

Default
- retransmit interval—5 seconds.
- transit delay—1 second.
- hello interval—10 seconds.
- dead interval—40 seconds.
- wait timer interval—dead interval.

Usage Guidelines
Specify the following:
- retransmit interval—If you set an interval that is too short, unnecessary retransmissions will result.
- transit delay—The transit delay must be greater than 0.
- hello interval—Smaller times allow routers to discover each other more quickly, but also increase network traffic.
- dead interval—This interval should be a multiple of the hello interval.
- wait timer interval—This interval is required by the OSPF standard to be equal to the router dead interval. Under some circumstances, setting the wait interval to smaller values can help OSPF routers on a broadcast network to synchronize more quickly at the expense of possibly electing an incorrect DR or BDR. This value should not be set to less than the hello interval. The default value is equal to the router dead interval.

Example
The following command configures the OSPF wait interval on the VLAN accounting:

configure ospf vlan accounting timer 10 15 20 60 60
**History**
This command was first available in ExtremeWare 6.2.
This command was modified in ExtremeWare 6.22.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
This command was modified in ExtremeWare 7.2e.

**Platform Availability**
This command is available on all platforms.
configure rip add vlan

configure rip add vlan [<vlan name> | all]

**Description**
Configures RIP on an IP interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**
All. If no VLAN is specified, then all is assumed.

**Usage Guidelines**
When an IP interface is created, RIP configuration is disabled on the interface by default. When the RIP interface is disabled, the parameters are not reset to default automatically.

**Example**
The following command configures RIP on the VLAN `finance`:

```plaintext
configure rip add finance
```

**History**
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure rip delete vlan

configure rip delete vlan [<vlan name> | all]

**Description**
Disables RIP on an IP interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**
All. If no VLAN is specified, then all is assumed.

**Usage Guidelines**
When an IP interface is created, RIP configuration is disabled on the interface by default. When the RIP interface is disabled, the parameters are not reset to default automatically.

**Example**
The following command deletes RIP on a VLAN named *finance*:
```
configure rip delete finance
```

**History**
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
configure rip garbagetime

    configure rip garbagetime {<seconds>}

Description
Configures the RIP garbage time.

Syntax Description

<table>
<thead>
<tr>
<th>seconds</th>
<th>Specifies a time in seconds.</th>
</tr>
</thead>
</table>

Default
120 seconds.

Usage Guidelines
None.

Example
The following command configures the RIP garbage time to have a 60-second delay:
configure rip garbagetime 60

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e" series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure rip routetimeout

configure rip routetimeout {<seconds>}

Description
Configures the route timeout period.

Syntax Description

| seconds | Specifies a time in seconds. |

Default
180 seconds.

Usage Guidelines
If a router does not receive an update message from its neighbor within the route timeout period (180 seconds by default), the router assumes the connection between it and its neighbor is no longer available.

Example
The following example sets the route timeout period to 120 seconds:

```
configure rip routetimeout 120
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure rip rxmode

    configure rip rxmode [none | v1only | v2only | any] {vlan [<vlan name> | all]}

**Description**
Changes the RIP receive mode for one or more VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies to drop all received RIP packets.</td>
</tr>
<tr>
<td>v1only</td>
<td>Specifies to accept only RIP version 1 format packets.</td>
</tr>
<tr>
<td>v2only</td>
<td>Specifies to accept only RIP version 2 format packets.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies to accept RIP version 1 and RIP version 2 packets.</td>
</tr>
<tr>
<td>vlan &lt;name&gt;</td>
<td>Specifies to apply settings to specific VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**
Any.

**Usage Guidelines**
If no VLAN is specified, the setting is applied to all VLANs.

**Example**
The following command configures the receive mode for the VLAN finance to accept only RIP version 1 format packets:

```plaintext
configure rip rxmode v1only finance
```

**History**
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the all keyword.

**Platform Availability**
This command is available on all platforms.
configure rip txmode

configure rip txmode [none | v1only | v1comp | v2only] {vlan [<vlan name> | all]}

Description
Changes the RIP transmission mode for one or more VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies to not transmit any packets on this interface.</td>
</tr>
<tr>
<td>v1only</td>
<td>Specifies to transmit RIP version 1 format packets to the broadcast address.</td>
</tr>
<tr>
<td>v1comp</td>
<td>Specifies to transmit RIP version 2 format packets to the broadcast address.</td>
</tr>
<tr>
<td>v2only</td>
<td>Specifies to transmit RIP version 2 format packets to the RIP multicast address.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies to apply settings to a specific VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
v2only.

Usage Guidelines
If no VLAN is specified, the setting is applied to all VLANs.

Example
The following command configures the transmit mode for the VLAN finance to transmit version 2 format packets to the broadcast address:

```
configure rip txmode v1comp finance
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

This command was modified in ExtremeWare 7.2e to support the all keyword.

Platform Availability
This command is available on all platforms.
configure rip updatetime

configure rip updatetime {<seconds>}

Description
Specifies the time interval in seconds within which RIP sends update packets.

Syntax Description

| seconds | Specifies a time in seconds. |

Default
30 seconds.

Usage Guidelines
The router exchanges an update message with each neighbor every 30 seconds (default value), or if there is a change to the overall routed topology (also called triggered updates). The timer granularity is 10 seconds.

Example
The following command sets the update timer to 60 seconds:

configure rip updatetime 60

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure rip vlan cost

configure rip vlan [<vlan name> | all] cost <cost>

**Description**

Configures the cost (metric) of the interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a cost metric.</td>
</tr>
</tbody>
</table>

**Default**

The default setting is 1.

**Usage Guidelines**

None.

**Example**

The following command configures the cost for the VLAN finance to a metric of 3:

```
configure rip vlan finance cost 3
```

**History**

This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
configure rip vlan export-filter

configure rip vlan [<vlan name> | all] export-filter [<access profile> | none]

Description
Configures RIP to suppress certain routes when performing route advertisements.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access-profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to check the access profile for permit and deny attributes.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use an access profile to determine trusted RIP router neighbors for the VLAN on the switch running RIP.

Using the none mode, the access profile can contain a combination of permit and deny entries. Each entry must have a permit or deny attribute. The operation is compared with each entry in the list. When a match is found, the operation is either permitted or denied, depending on the configuration of the matched entry. If no match is found, the operation is implicitly denied.

Example
The following command uses the access profile nosales to determine which RIP routes are advertised into the VLAN backbone:

```
configure rip vlan backbone export-filter nosales
```

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure rip vlan import-filter

configure rip vlan [<vlan name> | all] import-filter [<access profile> | none]

Description
Configures RIP to ignore certain routes received from its neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access-profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to check the access profile for permit and deny attributes.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Configures an import filter policy, which uses an access profile to determine which RIP routes are accepted as valid routes. This policy can be combined with the trusted neighbor policy to accept selected routes only from a set of trusted neighbors.

Using the none mode, the access profile can contain a combination of permit and deny entries. Each entry must have a permit or deny attribute. The operation is compared with each entry in the list. When a match is found, the operation is either permitted or denied, depending on the configuration of the matched entry. If no match is found, the operation is implicitly denied.

Example
The following command configures the VLAN backbone to accept selected routes from the access profile nosales:

```
configure rip vlan backbone import-filter nosales
```

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure rip vlan trusted-gateway

configure rip vlan [<vlan name> | all] trusted-gateway [<access profile> | none]

Description
Configures a trusted neighbor policy, which uses an access profile to determine trusted RIP router neighbors for the VLAN on the switch running RIP.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access-profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to check the access profile for permit and deny attributes.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Using the none mode, the access profile can contain a combination of permit and deny entries. Each entry must have a permit or deny attribute. The operation is compared with each entry in the list. When a match is found, the operation is either permitted or denied, depending on the configuration of the matched entry. If no match is found, the operation is implicitly denied.

Example
The following command configures RIP to use the access profile nointernet to determine from which RIP neighbor to receive (or reject) the routes to the VLAN backbone:

```bash
configure rip vlan backbone trusted-gateway nointernet
```

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
create isis area

create isis area <name>

Description
Creates an IS-IS level 1 area.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies the area identifier.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
Currently, only one level 1 area can be created.

The maximum length for an area identifier is 32 characters. The identifier must begin with one alphabetic character followed by up to 31 alphabetic or numeric characters.

Example
The following command creates an IS-IS level 1 area:
create isis area a1000

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
create ospf area

create ospf area <area identifier>

Description
Creates an OSPF area.

Syntax Description

| area identifier | Specifies an OSPF area. |

Default
Area 0.0.0.0

Usage Guidelines
Area 0.0.0.0 does not need to be created. It exists by default.

Example
The following command creates an OSPF area:
create ospf area 1.2.3.4

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
**delete isis area**

```delete isis area [<isis area identifier> | all]```

**Description**

Deletes an IS-IS level 1 area.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>isis area identifier</td>
<td>Specifies the area identifier.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

Currently, only one level 1 area can be created.

The maximum length for an area identifier is 32 characters. The identifier must begin with one alphabetic character followed by up to 31 alphabetic or numeric characters.

The `all` option deletes all of the level 1 areas simultaneously.

The level 1 area can only be deleted when no interface attaches to it.

**Example**

The following command deletes an IS-IS level 1 area:

```delete isis area a1000```

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms.
delete ospf area

    delete ospf area [<area identifier> | all]

Description
Deletes an OSPF area.

Syntax Description

<table>
<thead>
<tr>
<th>area identifier</th>
<th>Specifies an OSPF area.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all areas.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
An OSPF area cannot be deleted if it has an associated interface.

Example
The following command deletes an OSPF area:

d delete ospf area 1.2.3.4

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable isis

disable isis

Description
Disables IS-IS routing.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
To enable IS-IS routing, use the following command:

enable isis

Example
The following command disables IS-IS routing:

disable isis

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
disable isis export

disable isis [level-2 | area <isis area identifier>] export [bgp | i-bgp | e-bgp | direct | rip | static | vip | ospf | ospf-intra | ospf-inter | ospf-extern1 | ospf-extern2]

Description
Disables the redistribution of non-IS-IS routes from the kernel routing table into a IS-IS level 2 subdomain or level 1 area:

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies a level 2 subdomain</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies an IS-IS level 1 area</td>
</tr>
<tr>
<td>bgp</td>
<td>Specifies BGP routes.</td>
</tr>
<tr>
<td>i-bgp</td>
<td>Specifies I-BGP routes.</td>
</tr>
<tr>
<td>e-bgp</td>
<td>Specifies E-BGP routes.</td>
</tr>
<tr>
<td>direct</td>
<td>Specifies direct routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies OSPF routes.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies Intra OSPF routes.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies Inter OSPF routes.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies Extern 1 OSPF routes.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies Extern 2 OSPF routes.</td>
</tr>
</tbody>
</table>

Default
The default setting is disabled.

Usage Guidelines
All the redistributed routes are associated with the same metric and metric type.

Example
The following command disables redistribution of OSPF routes for a level 2 subdomain:

disable isis level-2 export ospf

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.
Platform Availability

This command is available on the “i” series platforms.
disable isis ignore-attached-bit

disable isis ignore-attached-bit

Description
Disables ignoring the attached bit.

Syntax Description
This command has no arguments or variables.

Default
The default setting is disabled.

Usage Guidelines
This command can only be applied to a level 1 only switch. It specifies that the level 1 only switch will not ignore the attached bit (ATT bit) from level 1/2 switches.

This command has the effect of enabling the feature described in the ExtremeWare Software User Guide, Software Version 7.0.0, in the chapter, “Interior Gateway Protocols”, in the section, “Default Routes to Nearest Level 1/2 Switch for Level 1 Only Switches”. See the user guide for more information.

Example
The following command disables ignoring the attached bit:

disable isis ignore-attached-bit

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
disable isis originate-default

disable isis [level-2 | area <isis area identifier>] originate-default

Description
Disables the origination of an IS-IS default route from a system into the level 1 area or level 2 subdomain.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies the level 2 subdomain.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies a level 1 area identifier.</td>
</tr>
</tbody>
</table>

Default
The default setting is disabled.

Usage Guidelines
None.

Example
The following command disables the origination of an IS-IS default route for the level 2 subdomain:

disable isis level-2 originate-default

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
disable isis overload

disable isis [level-2 | area <isis area identifier>] overload {at-startup}

Description
Disables the setting of the overload bit in the LSP originated by the system in the level 2 subdomain or level 1 area.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies the level 2 subdomain.</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies a level 1 area.</td>
</tr>
<tr>
<td>at-startup</td>
<td>Specifies that setting the overload bit is disabled at startup.</td>
</tr>
</tbody>
</table>

Default
The default setting is disabled.

Usage Guidelines
The at-startup option disables setting the overload bit at system startup time.

Example
The following command disables setting the overload bit for the level 1 area a1:

disable isis area a1 overload

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
disable ospf

disable ospf

Description
Disables the OSPF process for the router.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command disables the OSPF process for the router:

disable ospf

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ospf capability opaque-lsa

   disable ospf capability opaque-lsa

Description
Disables opaque LSAs across the entire system.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Opaque LSAs are a generic OSPF mechanism used to carry auxiliary information in the OSPF database. Opaque LSAs are most commonly used to support OSPF traffic engineering.

Normally, support for opaque LSAs is auto-negotiated between OSPF neighbors. In the event that you experience interoperability problems, you can disable opaque LSAs.

If your network uses opaque LSAs, all routers on your OSPF network should support opaque LSAs. Routers that do not support opaque LSAs do not store or flood them. At minimum a well-interconnected subsection of your OSPF network needs to support opaque LSAs to maintain reliability of their transmission.

On an OSPF broadcast network, the designated router (DR) must support opaque LSAs or none of the other routers on that broadcast network will reliably receive them. You can use the OSPF priority feature to give preference to an opaque-capable router, so that it becomes the elected DR.

For transmission to continue reliably across the network, the backup designated router (BDR) must also support opaque LSAs.

Example
The following command disables opaque LSAs across the entire system:

disable ospf capability opaque-lsa

History
This command was available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ospf export

For “i” series switches:

```
disable ospf export [bgp | direct | e-bgp | i-bgp | isis | isis-level-1 |
isis-level-1-external | isis-level-2 | isis-level-2-external | rip | static |
vip]
```

For “e” series switches:

```
disable ospf export [direct | rip | static]
```

**Description**

Disables redistribution of routes to OSPF.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Specifies BGP routes.</td>
</tr>
<tr>
<td>direct</td>
<td>Specifies direct routes.</td>
</tr>
<tr>
<td>i-bgp</td>
<td>Specifies I-BGP routes.</td>
</tr>
<tr>
<td>e-bgp</td>
<td>Specifies E-BGP routes.</td>
</tr>
<tr>
<td>isis</td>
<td>Specifies IS-IS routes.</td>
</tr>
<tr>
<td>isis-level-1</td>
<td>Specifies IS-IS level 1 routes.</td>
</tr>
<tr>
<td>isis-level-1-external</td>
<td>Specifies IS-IS level 1 external routes</td>
</tr>
<tr>
<td>isis-level-2</td>
<td>Specifies IS-IS level 2 routes.</td>
</tr>
<tr>
<td>isis-level-2-external</td>
<td>Specifies IS-IS level 2 external routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routes.</td>
</tr>
</tbody>
</table>

**Default**

The default setting is disabled.

**Usage Guidelines**

Use this command to stop OSPF from exporting routes derived from other protocols.
Example
The following command disables OSPF to export BGP-related routes to other OSPF routers on “i” series switches:

disable ospf export bgp

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable ospf originate-router-id

Description
Disables distribution of a route for the OSPF router ID in the router LSA.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
When this function is enabled, OSPF includes a link with the router ID IP address and a mask of 255.255.255.255 in the router LSA. The link type is stub and the metric is 0.

When disabled, OSPF does not include a link with the router ID IP address in the router LSA.

Example
The following command disables the distribution of a route for the OSPF router ID in the router LSA:

disable ospf originate-router-id

History
This command was available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

Platform Availability
This command is available on the BlackDiamond switch only.
disable rip

disable rip

Description
Disables RIP for the whole router.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
RIP has a number of limitations that can cause problems in large networks, including:
- A limit of 15 hops between the source and destination networks
- A large amount of bandwidth taken up by periodic broadcasts of the entire routing table
- Slow convergence
- Routing decisions based on hop count; no concept of link costs or delay
- Flat networks; no concept of areas or boundaries

Example
The following command disables RIP for the whole router:
disable rip

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable rip aggregation

disable rip aggregation

Description
Disables the RIP aggregation of subnet information on a RIP version 2 (RIPv2) router.

Syntax Description
This command has no arguments or variables.

Default
RIP aggregation is disabled by default.

Usage Guidelines
The disable RIP aggregation command disables the RIP aggregation of subnet information on a switch configured to send RIPv2-compatible traffic. The switch summarizes subnet routes to the nearest class network route. The following rules apply when using RIP aggregation:

- Within a class boundary, no routes are aggregated.
- If aggregation is disabled, subnet routes are never aggregated, even when crossing a class boundary.

Example
The following command disables RIP aggregation on the interface:

disable rip aggregation

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable rip export

For “i” series switches:

    disable rip export [direct | isis | isis-level-1 | isis-level-1-external | isis-level-2 | isis-level-2-external | ospf | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | static | vip]

For “e” series switches:

    disable rip export [direct| ospf | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | static]

**Description**

Disables RIP from redistributing routes from other routing protocols.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>Specifies interface routes (only interfaces that have IP forwarding enabled are exported).</td>
</tr>
<tr>
<td>isis</td>
<td>Specifies IS-IS routes.</td>
</tr>
<tr>
<td>isis-level-1</td>
<td>Specifies IS-IS level 1 routes.</td>
</tr>
<tr>
<td>isis-level-1-external</td>
<td>Specifies IS-IS level 1 external routes.</td>
</tr>
<tr>
<td>isis-level-2</td>
<td>Specifies IS-IS level 2 routes.</td>
</tr>
<tr>
<td>isis-level-2-external</td>
<td>Specifies IS-IS level 2 external routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies all OSPF routes.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies OSPF external route type 1.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies OSPF external route type 2.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies OSPF-inter area routes.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies OSPF-intra area routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routes.</td>
</tr>
</tbody>
</table>

**Default**

Disabled.

**Usage Guidelines**

This command disables the exporting of static, direct and OSPF-learned routes into the RIP domain. On “i” series switches it also disables the export of IS-IS learned routes into the RIP domain.
**Example**
The following command disables RIP from redistributing any routes learned from OSPF:
```
disable rip export ospf
```

**History**
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
disable rip exportstatic

disable rip exportstatic

**Description**
Disables the redistribution of static routes.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled.

**Usage Guidelines**
Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure 64 static unicast routes. Static routes can also be used for security reasons, to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

**Example**
The following command disables the redistribution of static routes:

disable rip exportstatic

**History**
This command was removed in ExtremeWare 6.0 and ExtremeWare 7.2e.

**Platform Availability**
Although this command might show in the CLI, it is no longer supported.
disable rip originate-default

disable rip originate-default

Description
Disables the advertisement of a default route.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
None.

Example
The following command unconfigures a default route to be advertised by RIP if no other default route is advertised:

disable rip originate-default cost 0

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable rip poisonreverse

Description
Disables poison reverse algorithm for RIP.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Like split horizon, poison reverse is a scheme for eliminating the possibility of loops in the routed topology. In this case, a router advertises a route over the same interface that supplied the route, but the route uses a hop count of 16, defining it as unreachable.

Example
The following command disables the split horizon with poison reverse algorithm for RIP:

disable rip poisonreverse

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable rip splithorizon

Description
Disables the split horizon algorithm for RIP.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Split horizon is a scheme for avoiding problems caused by including routes in updates sent to the router from which the route was learned. Split horizon omits routes learned from a neighbor in updates sent to that neighbor.

Example
The following command disables the split horizon algorithm for RIP:

disable rip splithorizon

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable rip triggerupdate

disable rip triggerupdate

Description
Disables the trigger update mechanism. Triggered updates are a mechanism for immediately notifying a router’s neighbors when the router adds or deletes routes or changes their metric.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Triggered updates occur whenever a router changes the metric for a route and it is required to send an update message immediately, even if it is not yet time for a regular update message to be sent. This will generally result in faster convergence, but may also result in more RIP-related traffic.

Example
The following command disables the trigger update mechanism:

disable rip triggerupdate

History
This command was available in ExtremeWare 2.0

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable isis

enable isis

Description
Enables IS-IS routing.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
To enable IS-IS routing, use the following command:

```
enable isis
```

Example
The following command enables IS-IS routing:

```
enable isis
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms.
enable isis export

```
enable isis [level-2 | area <isis area identifier>] export [bgp | i-bgp | e-bgp | direct | rip | static | vip | ospf | ospf-intra | ospf-inter | ospf-extern1 | ospf-extern2] [cost <cost(0-4261412864)> type [internal | external] | <route map>]
```

**Description**

Enables the redistribution of non-IS-IS routes from the kernel routing table into a IS-IS level 2 subdomain or level 1 area:

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies a level 2 subdomain</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies an IS-IS level 1 area</td>
</tr>
<tr>
<td>bgp</td>
<td>Specifies BGP routes.</td>
</tr>
<tr>
<td>i-bgp</td>
<td>Specifies I-BGP routes.</td>
</tr>
<tr>
<td>e-bgp</td>
<td>Specifies E-BGP routes.</td>
</tr>
<tr>
<td>direct</td>
<td>Specifies direct routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies OSPF routes.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies Intra OSPF routes.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies Inter OSPF routes.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies Extern 1 OSPF routes.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies Extern 2 OSPF routes.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a cost from 0 to 4,261,412,864.</td>
</tr>
<tr>
<td>internal</td>
<td>Specifies an internal metric type.</td>
</tr>
<tr>
<td>external</td>
<td>Specifies an external metric type.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map name.</td>
</tr>
</tbody>
</table>

**Default**

The default setting is disabled.

**Usage Guidelines**

All the redistributed routes are associated with the same metric and metric type, if specified. If a route map is specified, routes can be assigned different metric and metric types. Routes maps can also filter out routes.
**Example**

The following command enables redistribution of direct routes to the level 1 area *a1* with the route map *rm*:

```
enable isis area a1 export direct rm
```

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms only.
enable isis ignore-attached-bit

enable isis ignore-attached-bit

Description
Enables ignoring the attached bit.

Syntax Description
This command has no arguments or variables.

Default
The default setting is disabled.

Usage Guidelines
This command can only be applied to a level 1 only switch. It specifies that the level 1 only switch will ignore the attached bit (ATT bit) from level 1/2 switches.

This command has the effect of disabling the feature described in the ExtremeWare User Guide, in the chapter, “Interior Gateway Protocols”, in the section, “Default Routes to Nearest Level 1/2 Switch for Level 1 Only Switches”. See the user guide for more information.

Example
The following command enables ignoring the attached bit:

```
enable isis ignore-attached-bit
```

History
This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the “i” series platforms only.
enable isis originate-default

enable isis [level-2 | area <isis area identifier>] originate-default (always) cost <cost(0-4261412864)> type [internal | external]

**Description**

Enables the origination of a default route from a system into the level 1 area or level 2 subdomain.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies the level 2 subdomain.</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies a level 1 area identifier</td>
</tr>
<tr>
<td>always</td>
<td>Specifies that the default route is always originated.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a cost from 0 to 4,261,412,864.</td>
</tr>
<tr>
<td>internal</td>
<td>Specifies an internal metric type.</td>
</tr>
<tr>
<td>external</td>
<td>Specifies an external metric type.</td>
</tr>
</tbody>
</table>

**Default**

The default setting is disabled.

**Usage Guidelines**

When the `always` option is specified, the default route is originated even if there is no default route in the kernel routing table. Otherwise the default route will be originated only if the default route is available in the kernel route table.

**Example**

The following command enables the origination of an IS-IS default route that uses the internal metric type and a cost of 15 for the level 2 subdomain:

```
enable isis level-2 originate-default cost 15 type internal
```

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms only.
enable isis overload

```
enable isis [level-2 | area <isis area identifier>] overload {at-startup}
{<seconds(1-86400)>}
```

**Description**

Enables the setting of the overload bit in the LSP originated by the system in the level 2 subdomain or level 1 area.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>level-2</td>
<td>Specifies the level 2 subdomain.</td>
</tr>
<tr>
<td>isis area identifier</td>
<td>Specifies a level 1 area.</td>
</tr>
<tr>
<td>at-startup</td>
<td>Specifies that setting the overload bit is enabled at startup.</td>
</tr>
<tr>
<td>seconds(1-86400)</td>
<td>Specifies the duration of the overload.</td>
</tr>
</tbody>
</table>

**Default**

The default setting is disabled.

**Usage Guidelines**

The `at-startup` option sets the overload bit at system startup time.

The `<seconds(1-186400)>` parameter sets the duration of the overload bit. If the duration is not specified, the bit is set until it is disabled. The range is 1 to 186,400 seconds.

**Example**

The following command enables IS-IS overload for the level 1 area `a1` with a duration of 100 seconds:

```
enable isis area a1 overload 100
```

**History**

This command was first available in ExtremeWare v6.1.8 IS-IS tech release and subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the “i” series platforms only.
enable ospf

Enable OSPF process for the router.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command enables the OSPF process for the router:

```
enable ospf
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ospf capability opaque-lsa

    enable ospf capability opaque-lsa

Description
Enables opaque LSAs across the entire system.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Opaque LSAs are a generic OSPF mechanism used to carry auxiliary information in the OSPF database. Opaque LSAs are most commonly used to support OSPF traffic engineering.

Normally, support for opaque LSAs is auto-negotiated between OSPF neighbors. In the event that you experience interoperability problems, you can disable opaque LSAs.

If your network uses opaque LSAs, all routers on your OSPF network should support opaque LSAs. Routers that do not support opaque LSAs do not store or flood them. At minimum a well-interconnected subsection of your OSPF network needs to support opaque LSAs to maintain reliability of their transmission.

On an OSPF broadcast network, the designated router (DR) must support opaque LSAs or none of the other routers on that broadcast network will reliably receive them. You can use the OSPF priority feature to give preference to an opaque-capable router, so that it becomes the elected DR.

For transmission to continue reliably across the network, the backup designated router (BDR) must also support opaque LSAs.

Example
The following command enables opaque LSAs across the entire system:

    enable ospf capability opaque-lsa

History
This command was available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ospf export

For “i” series switches:

```
enable ospf export [bgp | e-bgp | i-bgp | direct | rip | static | vip |
isis | isis-level-1 | isis-level-1-external | isis-level-2 |
isis-level-2-external] [cost <number> [ase-type-1 | ase-type-2]
{tag <number>} | <route map>]
```

For “e” series switches:

```
enable ospf export [direct | rip | static] [cost <number> [ase-type-1 |
ase-type-2] {tag <number>}
```

**Description**

Enables redistribution of routes to OSPF.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bgp</td>
<td>Specifies BGP routes. NOTE: This option is only available on “i” series switches.</td>
</tr>
<tr>
<td>e-bgp</td>
<td>Specifies E-BGP routes. NOTE: This option is only available on “i” series switches.</td>
</tr>
<tr>
<td>i-bgp</td>
<td>Specifies I-BGP routes. NOTE: This option is only available on “i” series switches.</td>
</tr>
<tr>
<td>direct</td>
<td>Specifies direct routes.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routes. NOTE: This option is only available on “i” series switches.</td>
</tr>
<tr>
<td>isis</td>
<td>Specifies IS-IS routes. NOTE: This option is only available on “i” series switches.</td>
</tr>
<tr>
<td>isis-level-1</td>
<td>Specifies IS-IS level 1 routes. NOTE: This option is only available on “i” series switches.</td>
</tr>
<tr>
<td>isis-level-1-external</td>
<td>Specifies IS-IS level 1 external routes.</td>
</tr>
<tr>
<td>isis-level-2</td>
<td>Specifies IS-IS level 2 routes.</td>
</tr>
<tr>
<td>isis-level-2-external</td>
<td>Specifies IS-IS level 2 external routes</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>ase-type-1</td>
<td>Specifies AS-external type 1 routes.</td>
</tr>
<tr>
<td>ase-type-2</td>
<td>Specifies AS-external type 2 routes.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a tag value.</td>
</tr>
</tbody>
</table>
Default
The default tag number is 0. The default setting is disabled.

Usage Guidelines
After it is enabled, the OSPF router is considered to be an ASBR. Interface routes that correspond to the interface that has OSPF enabled are ignored.

Exporting routes from OSPF to RIP, and from RIP to OSPF, are discrete configuration functions. To run OSPF and RIP simultaneously, you must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to RIP and the routes to export from RIP to OSPF.

The cost metric is inserted for all RIP-learned, static and direct routes injected into OSPF. For “i” series switches, the cost metric is also inserted for all BGP and VIP, injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

The same cost, type, and tag values can be inserted for all the export routes, or route maps can be used for selective insertion. When a route map is associated with the export command, the route map is applied on every exported route. The exported routes can also be filtered using route maps.

Example
The following command enables OSPF to export BGP-related routes using LSAs to other OSPF routers on an “i” series switch:

```
enable ospf export bgp cost 1 ase-type-1 tag 0
```

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ospf export direct

```
enable ospf export direct [cost <metric> [ase-type-1 | ase-type-2] [tag <number>] | <route map>]
```

**Description**
Enables the redistribution of local interface (direct) routes into the OSPF domain. This will not export the loopback address of 127.0.0.1.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>ase-type-1</td>
<td>Specifies AS-external type 1 routes.</td>
</tr>
<tr>
<td>ase-type-2</td>
<td>Specifies AS-external type 2 routes.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a tag value.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

**Default**
The default tag number is 0. The default setting is disabled.

**Usage Guidelines**
After it is enabled, the OSPF router is considered to be an ASBR. Interface routes that correspond to the interface that has OSPF enabled are ignored.

Exporting routes from OSPF to RIP, and from RIP to OSPF, are discreet configuration functions. To run OSPF and RIP simultaneously, you must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to RIP and the routes to export from RIP to OSPF.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

The same cost, type, and tag values can be inserted for all the export routes, or route maps can be used for selective insertion. When a route map is associated with the export command, the route map is applied on every exported route. The exported routes can also be filtered using route maps.

**Example**
The following command enables the distribution of local interface (direct) routes into the OSPF domain:
```
enable ospf export direct cost 1 ase-type-1 tag 0
```
History
This command was first available in ExtremeWare 6.1.

This command was modified in an ExtremeWare IP Technology Services Release based on ExtremeWare v6.1.8b12 to support MPLS modules.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ospf export rip

For “i” series switches:

   enable ospf export rip [cost <metric> [ase-type-1 | ase-type-2] {tag <number>} | <route map>]

For “e” series switches:

   enable ospf export rip [cost <metric> [ase-type-1 | ase-type-2] {tag <number>}]}

Description
Enables the redistribution of RIP to OSPF.

Syntax Description

<table>
<thead>
<tr>
<th>metric</th>
<th>Specifies a cost metric.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ase-type-1</td>
<td>Specifies AS-external type 1 routes.</td>
</tr>
<tr>
<td>ase-type-2</td>
<td>Specifies AS-external type 2 routes.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a tag value.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map name.</td>
</tr>
</tbody>
</table>

NOTE: This option is only available on “i” series switches.

Default
The default tag number is 0. The default setting is disabled.

Usage Guidelines
After it is enabled, the OSPF router is considered to be an ASBR.

This command enables the exporting of RIP by way of LSA to other OSPF routers as AS-external type 1 or type 2 routes.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

When re-distributing RIP routes, you should turn off RIP aggregation unless you are expertly familiar with the possible consequences and impact. By default, new configurations of RIP using ExtremeWare 4.0 and above disable RIP aggregation. In previous ExtremeWare versions, RIP aggregation is enabled by default. This configuration is preserved when upgrading to ExtremeWare 4.0. Verify the configuration using the command show rip.

Example
The following command enables the exporting of RIP to OSPF:

   enable ospf export rip cost 1 ase-type-1 tag 0
History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ospf export static

For “i” series switches:

    enable ospf export static [cost <metric> [ase-type-1 | ase-type-2] {tag <number>} | <route map>]

For “e” series switches:

    enable ospf export static [cost <metric> [ase-type-1 | ase-type-2] {tag <number>}]}

**Description**

Enables the redistribution of static routes to OSPF.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>ase-type-1</td>
<td>Specifies AS-external type 1 routes.</td>
</tr>
<tr>
<td>ase-type-2</td>
<td>Specifies AS-external type 2 routes.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a tag value.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map name.</td>
</tr>
</tbody>
</table>

**Default**

The default tag number is 0. The default setting is disabled.

**Usage Guidelines**

After it is enabled, the OSPF router is considered to be an ASBR.

This command enables the redistribution of static routes by way of LSA to other OSPF routers as AS-external type 1 or type 2 routes.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

**Example**

The following command enables the exporting of static routes to OSPF:

    enable ospf export static cost 0 ase-type-1 tag 0

**History**

This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.
Platform Availability

This command is available on all platforms.
enable ospf export vip

    enable ospf export vip [cost <metric> [ase-type-1 | ase-type-2] {tag <number>} | <route map>]

Description
Enables the redistribution of virtual IP addresses into the OSPF domain.

Syntax Description

<table>
<thead>
<tr>
<th>Metric</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>metric</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>ase-type-1</td>
<td>Specifies AS-external type 1 routes.</td>
</tr>
<tr>
<td>ase-type-2</td>
<td>Specifies AS-external type 2 routes.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a tag value.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

Default
The default tag number is 0. The default setting is disabled.

Usage Guidelines
After it is enabled, the OSPF router is considered to be an ASBR.

Exporting routes from OSPF to RIP, and from RIP to OSPF, are discreet configuration functions. To run OSPF and RIP simultaneously, you must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to RIP and the routes to export from RIP to OSPF.

These commands enable or disable the exporting of RIP, static, and direct routes by way of LSA to other OSPF routers as AS-external type 1 or type 2 routes. The default setting is disabled.

The cost metric is inserted for all BGP, VIP, RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag. The tag value in this instance has no relationship with 802.1Q VLAN tagging.

The same cost, cost-type, and tag values can be inserted for all the export routes, or route maps can be sued for selective insertion. When a route map is associated with the export command, the route map is applied on every exported route. The exported routes can also be filtered using route maps.

Example
The following command enables the redistribution of virtual IP addresses into the OSPF domain:

    enable ospf export vip cost 0 ase-type-1 tag 0

History
This command was first available in ExtremeWare 6.1.
Platform Availability

This command is available on the “i” series platforms only.
enable ospf originate-default

enable ospf originate-default {always} cost <metric> [ase-type-1 | ase-type-2] {tag <number>}

Description
Enables a default external LSA to be generated by OSPF, if no other default route is originated by OSPF by way of RIP and static route re-distribution.

Syntax Description

| always      | Specifies for OSPF to always advertise the default route. |
| meteric     | Specifies a cost metric.                                 |
| ase-type-1  | Specifies AS-external type 1 routes.                     |
| ase-type-2  | Specifies AS-external type 2 routes.                     |
| number      | Specifies a tag value.                                  |

Default
N/A.

Usage Guidelines
If always is specified, OSPF always advertises the default route. If always is not specified, OSPF adds the default LSA if a reachable default route is in the route table.

Example
The following command generates a default external type-1 LSA:

```
enable ospf originate-default cost 1 ase-type-1 tag 0
```

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ospf originate-router-id

enable ospf originate-router-id

Description
Enables distribution of a route for the OSPF router ID in the router LSA.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
When this function is enabled, OSPF includes a link with the router ID IP address and a mask of 255.255.255.255 in the router LSA. The link type is stub and the metric is 0.

When disabled, OSPF does not include a link with the router ID IP address in the router LSA.

Example
The following command enables the distribution of a route for the OSPF router ID in the router LSA:

```
enable ospf originate-router-id
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

Platform Availability
This command is available on the BlackDiamond switch only.
enable rip

enable rip

Description
Enables RIP for the whole router.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
RIP has a number of limitations that can cause problems in large networks, including:

- A limit of 15 hops between the source and destination networks
- A large amount of bandwidth taken up by periodic broadcasts of the entire routing table
- Slow convergence
- Routing decisions based on hop count; no concept of link costs or delay
- Flat networks; no concept of areas or boundaries

Example
The following command enables RIP for the whole router:

cenable rip

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable rip aggregation

enable rip aggregation

Description
Enables the RIP aggregation of subnet information on a RIP version 2 (RIPv2) interface.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
The enable (disable) rip aggregation command enables (disables) the RIP aggregation of subnet information on an interface configured to send RIPv1 or RIPv2-compatible traffic. The switch summarizes subnet routes to the nearest class network route. The following rules apply when using RIP aggregation:

- Subnet routes are aggregated to the nearest class network route when crossing a class boundary.
- Within a class boundary, no routes are aggregated.
- If aggregation is enabled, the behavior is the same as in RIPv1.
- If aggregation is disabled, subnet routes are never aggregated, even when crossing a class boundary.

Example
The following command enables RIP aggregation on the interface:

```
enable rip aggregation
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable rip export cost

For “i” series switches:

   enable rip export [direct | isis | isis-level-1 | isis-level-1-external | isis-level-2 | isis-level-2-external | ospf | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | static | vip] cost <number> {tag <number>}

For “e” series switches:

   enable rip export [direct | ospf | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | static] cost <number> {tag <number>}

Description

Enables RIP to redistribute routes from other routing functions.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>Specifies interface routes (only interfaces that have IP forwarding enabled are exported).</td>
</tr>
<tr>
<td>isis</td>
<td>Specifies IS-IS routes.</td>
</tr>
<tr>
<td>isis-level-1</td>
<td>Specifies IS-IS level 1 routes.</td>
</tr>
<tr>
<td>isis-level-1-external</td>
<td>Specifies IS-IS level 1 external routes.</td>
</tr>
<tr>
<td>isis-level-2</td>
<td>Specifies IS-IS level 2 routes.</td>
</tr>
<tr>
<td>isis-level-2-external</td>
<td>Specifies IS-IS level 2 external routes.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies all OSPF routes.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies OSPF external route type 1.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies OSPF external route type 2.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies OSPF-inter area routes.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies OSPF-intra area routes.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routes.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routes.</td>
</tr>
<tr>
<td>cost &lt;number&gt;</td>
<td>Specifies the cost metric, from 0-15. If set to 0, RIP uses the route metric obtained from the route origin.</td>
</tr>
<tr>
<td>tag &lt;number&gt;</td>
<td>Specifies a tag number.</td>
</tr>
</tbody>
</table>

Default

Disabled.
**Usage Guidelines**

This command enables the exporting of static, direct, IS-IS, and OSPF-learned routes into the RIP domain. You can choose which types of OSPF or IS-IS routes are injected, or you can simply choose ospf or isis, which will inject all learned OSPF or IS-IS routes regardless of type. (IS-IS is only supported on the “i” series of switches.)

The cost metric is inserted for all RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag.

**Example**

The following command enables RIP to redistribute routes from all OSPF routes:

```
enable rip export ospf cost 0
```

**History**

This command was first available in ExtremeWare 4.0.

The keyword metric was changed to the keyword cost.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable rip export static cost

   enable rip export static cost <number> {tag <number>}

**Description**
Enables the redistribution of static routes with cost preference.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>cost &lt;number&gt;</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>tag &lt;number&gt;</td>
<td>Specifies a tag number.</td>
</tr>
</tbody>
</table>

**Default**
Disabled.

**Usage Guidelines**
Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure 64 static unicast routes. Static routes can also be used for security reasons, enabling you to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

**Example**
The following command enables the redistribution of static routes with cost preference of 5:

```bash
enable rip export static cost 5
```

**History**
This command was first available in ExtremeWare 7.3.0.

**Platform Availability**
This command is available on all platforms.
enable rip exportstatic

enable rip exportstatic

Description
Enables the redistribution of static routes.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers. You can configure 64 static unicast routes. Static routes can also be used for security reasons, to control which routes you want advertised by the router. You can decide if you want all static routes to be advertised. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

Example
The following command enables the redistribution of static routes:

enable rip exportstatic

History
This command was removed in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable rip originate-default cost

enable rip originate-default {always} cost <number> {tag <number>}

Description
Configures a default route to be advertised by RIP if no other default route is advertised.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>always</td>
<td>Specifies to always advertise the default route.</td>
</tr>
<tr>
<td>cost &lt;number&gt;</td>
<td>Specifies a cost metric.</td>
</tr>
<tr>
<td>tag &lt;number&gt;</td>
<td>Specifies a tag number.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
If always is specified, RIP always advertises the default route to its neighbors. If always is not specified, RIP adds a default route if a reachable default route is not in the route table.

The cost metric is inserted for all RIP-learned, static, and direct routes injected into OSPF. If the cost metric is set to 0, the cost is inserted from the route. The tag value is used only by special routing applications. Use 0 if you do not have specific requirements for using a tag.

Example
The following command configures a default route to be advertised by RIP if no other default route is advertised:

```
enable rip originate-default cost 0
```

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable rip poisonreverse

**Description**
Enables poison reverse algorithm for RIP.

**Syntax Description**
This command has no arguments or variables.

**Default**
Enabled.

**Usage Guidelines**
Like split horizon, poison reverse is a scheme for eliminating the possibility of loops in the routed topology. In this case, a router advertises a route over the same interface that supplied the route, but the route uses a hop count of 16, defining it as unreachable.

**Example**
The following command enables the split horizon with poison reverse algorithm for RIP:

```
enable rip poisonreverse
```

**History**
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable rip splithorizon

Description
Enables the split horizon algorithm for RIP.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Split horizon is a scheme for avoiding problems caused by including routes in updates sent to the router from which the route was learned. Split horizon omits routes learned from a neighbor in updates sent to that neighbor.

Example
The following command enables the split horizon algorithm for RIP:

```
enable rip splithorizon
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable rip triggerupdate

Description
Enables the trigger update mechanism. Triggered updates are a mechanism for immediately notifying a router’s neighbors when the router adds or deletes routes or changes their metric.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
Triggered updates occur whenever a router changes the metric for a route and it is required to send an update message immediately, even if it is not yet time for a regular update message to be sent. This will generally result in faster convergence, but may also result in more RIP-related traffic.

Example
The following command enables the trigger update mechanism:

```
enable rip triggerupdate
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf

Description
Displays global OSPF information.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command displays global OSPF information:

```
show ospf
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf area

    show ospf area <area identifier>

Description
Displays information about a particular OSPF area.

Syntax Description

<table>
<thead>
<tr>
<th>area identifier</th>
<th>Specifies an OSPF area.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command displays information about OSPF area 1.2.3.4:
show ospf area 1.2.3.4

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf area detail

    show ospf area detail

Description
Displays information about all OSPF areas.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command displays information about all OSPF areas:
show ospf area detail

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf ase-summary

    show ospf ase-summary

Description
Displays the OSPF external route aggregation configuration.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command displays the OSPF external route aggregation configuration:

    show ospf ase-summary

History
This command was first available in ExtremeWare 6.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf interfaces

show ospf interfaces {vlan <vlan name> | area <area identifier>}

Description
Displays information about one or all OSPF interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

Default
If no argument is specified, all OSPF interfaces are displayed.

Usage Guidelines
None.

Example
The following command displays information about one or all OSPF interfaces on the VLAN accounting:

```
show ospf interfaces vlan accounting
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf interfaces detail

    show ospf interfaces detail

Description
Displays detailed information about all OSPF interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command displays information about all OSPF interfaces:

```
show ospf interfaces detail
```

History
This command was first available in ExtremeWare 6.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show ospf lsdb area lstype

show ospf lsdb area [all | <area identifier>[/<len>] | detail | interface | lsid <id>[/<len>] | lstype [all | as-external | external-type7 | network | opaque-area | opaque-global | opaque-local | router | summary-asb | summary-net | routerid <id>[/<len>] | stats | summary | vlan <vlan name>]

Description
Displays a table of the current LSDB.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all OSPF areas.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display all fields of matching LSAs in a multi-line format.</td>
</tr>
<tr>
<td>interface</td>
<td>Specifies to display interface types.</td>
</tr>
<tr>
<td>id</td>
<td>Specifies an LS ID.</td>
</tr>
<tr>
<td>id</td>
<td>Specifies a router ID.</td>
</tr>
<tr>
<td>stats</td>
<td>Specifies to display the number of matching LSAs, but not any of their contents.</td>
</tr>
<tr>
<td>summary</td>
<td>Specifies to display several important fields of matching LSAs, one line per LSA.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Display in summary format.

Usage Guidelines
ExtremeWare provides several filtering criteria for the show ospf lsdb command. You can specify multiple search criteria and only results matching all of the criteria are displayed. This allows you to control the displayed entries in large routing tables.

A common use of this command is to omit all optional parameters, resulting in the following shortened form:

```
show ospf lsdb
```

The shortened form displays all areas and all types in a summary format.

You can filter the display using either the area ID, the remote router ID, or the link-state ID. The default setting is `all` with no detail. If detail is specified, each entry includes complete LSA information.

Example
The following command displays all areas and all types in a summary format:

```
show ospf lsdb
```
IGP Commands

**History**
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show ospf virtual-link

    show ospf virtual-link {routerid <routerid> <area identifier>}

**Description**
Displays virtual link information about a particular router or all routers.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>routerid</td>
<td>Specifies a router interface number.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

*area identifier*—Transit area used for connecting the two end-points. The transit area cannot have the IP address 0.0.0.0.

**Example**
The following command displays virtual link information about a particular router:

```
show ospf virtual-link routerid 1.2.3.4 10.1.6.1
```

**History**
This command was available in ExtremeWare 2.0.

This command was added to the Summit "e" series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show rip

        show rip {detail}

Description
Displays RIP specific configuration and statistics for all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>detail</th>
<th>Specifies to display the information in detailed format.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command displays RIP specific configuration and statistics for all VLANs:

```
show rip
```

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show rip stats

show rip stats {detail}

**Description**
Displays RIP-specific statistics for all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**
All.

**Usage Guidelines**
Statistics include the following per interface:
- Packets transmitted
- Packets received
- Bad packets received
- Bad routes received
- Number of RIP peers
- Peer information

**Example**
The following command displays RIP-specific statistics for all VLANs:

```
show rip stat
```

**History**
This command was available in ExtremeWare 2.0
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show rip stats vlan

    show rip stats vlan <vlan name>

**Description**
Displays RIP specific statistics for a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command displays RIP specific statistics for the VLAN **accounting**:  
show rip stat accounting

**History**
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
show rip vlan

    show rip vlan <vlan name>

Description
Displays RIP configuration and statistics for a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>vlan name</th>
<th>Specifies a VLAN name.</th>
</tr>
</thead>
</table>

Default
All.

Usage Guidelines
None.

Example
The following command displays RIP configuration and statistics for the VLAN accounting:

    show rip vlan accounting

History
This command was first available in ExtremeWare 4.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure ospf

unconfigure ospf {vlan <vlan name> | area <area identifier>}

Description
Resets one or all OSPF interfaces to the default settings.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>area identifier</td>
<td>Specifies an OSPF area.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command resets the OSPF interface to the default settings on the VLAN accounting:

```
unconfigure ospf accounting
```

History
This command was first available in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure rip

    unconfigure rip {vlan <vlan name>}

**Description**
Resets all RIP parameters to the default VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
All.

**Usage Guidelines**
Does not change the enable/disable state of the RIP settings.

**Example**
The following command deletes RIP configuration from the VLAN *finance*:
```
unconfigure rip finance
```

**History**
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
Border Gateway Protocol (BGP) is an exterior routing protocol that was developed for use in TCP/IP networks. The primary function of BGP is to allow different autonomous systems (ASs) to exchange network reachability information.

An autonomous system is a set of routers that are under a single technical administration. This set of routers uses a different routing protocol (such as OSPF) for intra-AS routing. One or more routers in the AS are configured to be border routers, exchanging information with other border routers (in different autonomous systems) on behalf of all of the intra-AS routers.

BGP can be used as an exterior gateway protocol (E-BGP), or it can be used within an AS as an interior gateway protocol (I-BGP).

**BGP Attributes**

The following well-known BGP attributes are supported by the switch:

- **Origin** – Defines the origin of the route. Possible values are IGP, EGP, and incomplete.
- **AS_Path** – The list of ASs that are traversed for this route.
- **Next_hop** – The IP address of the next hop BGP router to reach the destination listed in the NLRI field.
- **Multi_Exit_Discriminator** – Used to select a particular border router in another AS when multiple border routers exist.
- **Local_Preference** – Used to advertise this router’s degree of preference to other routers within the AS.
- **Atomic_aggregate** – Indicates that the sending border router is used a route aggregate prefix in the route update.
- **Aggregator** – Identifies the BGP router AS number and IP address that performed route aggregation.
- **Community** – Identifies a group of destinations that share one or more common attributes.
- **Cluster_ID** – Specifies a 4 byte field used by a route reflector to recognize updates from other route reflectors in the same cluster.
BGP Communities

A BGP community is a group of BGP destinations that require common handling. ExtremeWare supports the following well-known BGP community attributes:

- no-export
- no-advertise
- no-export-subconfed

BGP Features

This section lists BGP features supported by ExtremeWare:

- Route Reflectors
- Route Confederations
- Route Aggregation
- IGP Synchronization
- Using the Loopback Interface
- BGP Peer Groups
- BGP Route Flap Dampening
- Route Redistribution
- Policy Filtering
- Maximum Prefix Limit
- MD5 TCP Authentication
clear bgp neighbor counters

clear bgp neighbor [<ip address> | all] counters

**Description**
Resets the BGP counters for one or all BGP neighbor sessions to zero.

**Syntax Description**

| ip address | Specifies the IP address of a specific BGP neighbor. |
| all        | Specifies that counters for all BGP neighbors should be reset. |

**Default**
N/A.

**Usage Guidelines**
This command resets the following counters:
- In-total-msgs
- Out-total-msgs
- In-updates
- Out-updates
- Last-error
- FsmTransitions

**Example**
The following command resets the counters for the BGP neighbor at 10.20.30.55:
clear bgp neighbor 10.20.30.55 counters

**History**
This command was first available in ExtremeWare 6.2.1

This command was modified in ExtremeWare 6.2.2 to add the FsmTransitions counter.

**Platform Availability**
This command is available on “i” series of switches.
clear bgp neighbor flap-statistics

clear bgp neighbor <ip address> flap-statistics
[community [access-profile <access profile> | no-advertise | no-export |
| no-export-subconfed | number <community number> |
| <autonomous system id (0 - 65535)>::<bgp community (0 - 65535)>]
| as-path [<path expression> | access-profile <access profile>]
| route-map <route map>
| network <ip address>/<mask> {exact}
| all]

Description
Clears flap statistics for routes to specified neighbors.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address that identifies a BGP neighbor.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile used as a community attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies the no-advertise community attribute.</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies the no-export community attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Specifies the no-export-subconfed community attribute.</td>
</tr>
<tr>
<td>community number</td>
<td>Specifies a community number.</td>
</tr>
<tr>
<td>autonomous system id</td>
<td>Specifies an autonomous system ID (0-65535).</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask (number of bits).</td>
</tr>
<tr>
<td>exact</td>
<td>Specifies an exact match with the IP address and subnet mask.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all routes.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to clear flap statistics for a specified BGP neighbor.

Example
The following command clears the flap statistics for a specified neighbor:
clear bgp neighbor 10.10.10.10 flap-statistics

History
This command was introduced in ExtremeWare 7.0.0.
Platform Availability

This command is available on “i” series of switches.
configure bgp add aggregate-address

configure bgp add aggregate-address <ip address>/<mask length> {as-set | as-match} {summary-only} {advertise-route-map <route-map>} {attribute-route-map <route-map>}

Description
Configures a BGP aggregate route.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask length</td>
<td>Specifies a netmask length.</td>
</tr>
<tr>
<td>as-set</td>
<td>Specifies to aggregate only the path attributes of the aggregate routes.</td>
</tr>
<tr>
<td>summary-only</td>
<td>Specifies to send only aggregated routes to the neighbors.</td>
</tr>
<tr>
<td>advertise-route-map</td>
<td>Specifies the route map used to select routes for this aggregated route.</td>
</tr>
<tr>
<td>attribute-route-map</td>
<td>Specifies the route map used to set the attributes of the aggregated route.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

To use BGP route aggregation, follow these steps:
1. Enable aggregation using the following command:
   ```plaintext
   enable bgp aggregation
   ```
2. Create an aggregate route using the following commands:
   ```plaintext
   configure bgp add aggregate-address <ip address>/<mask length> {as-set | as-match} {summary-only} {advertise-route-map <route-map>} {attribute-route-map <route-map>}
   ```

Example
The following command configures a BGP aggregate route:
```plaintext
configure bgp add aggregate-address 192.1.1.4/30
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp add confederation-peer sub-AS-number

configure bgp add confederation-peer sub-AS-number <number>

**Description**
Adds a sub-AS to a confederation.

**Syntax Description**

<table>
<thead>
<tr>
<th>number</th>
<th>Specifies a sub-AS number.</th>
</tr>
</thead>
</table>

**Default**
N/A.

**Usage Guidelines**
Invoke this command multiple times to add multiple sub-ASs.

IBGP requires networks to use a fully-meshed router configuration. This requirement does not scale well, especially when BGP is used as an interior gateway protocol. One way to reduce the size of a fully-meshed AS is to divide the AS into multiple sub-autonomous systems and group them into a routing confederation. Within the confederation, all BGP speakers in each sub-AS must be fully-meshed. The confederation is advertised to other networks as a single AS.

**Example**
The following command adds one sub-AS to a confederation:

```
configure bgp add confederation-peer sub-AS-number 65002
```

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on “i” series of switches.
configure bgp add network

configure bgp add network <ip address>/<mask length> {<route map>}

Description
Adds a network to be originated from this router.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask length</td>
<td>Specifies a netmask length.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The network must be present in the routing table.

Using the export command to redistribute routes complements the redistribution of routes using the configure bgp add network command. The configure bgp add network command adds the route to BGP only if the route is present in the routing table. The enable bgp export command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the network command take precedence over routes redistributed using the export command.

Example
The following command adds a network to be originated from this router:

```
configure bgp add network 192.1.1.16/12
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp AS-number

    configure bgp AS-number <number>

Description
Changes the local AS number used by BGP.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Specifies a local AS number.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
BGP must be disabled before the as number can be changed.

Example
The following command changes the local AS number used by BGP:

```
configure bgp AS-number 65001
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp cluster-id

    configure bgp cluster-id <bgp cluster id (0 - 4294967295)>

**Description**

Configures the local cluster ID.

**Syntax Description**

| bgp cluster id | Specifies a 4 byte field used by a route reflector to recognize updates from other route reflectors in the same cluster. |

**Default**

N/A.

**Usage Guidelines**

Used when multiple route reflectors are used within the same cluster of clients.

Extreme Networks recommends disabling BGP before configuring the cluster ID.

**Example**

The following command appends a BGP route reflector cluster ID to the cluster list of a route:

    configure bgp cluster-id 40000

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on “i” series of switches.
configure bgp confederation-id

    configure bgp confederation-id <number>

Description
Specifies a BGP routing confederation ID.

Syntax Description

| confederation-id | Specifies a routing confederation identifier. |

Default
N/A.

Usage Guidelines
IBGP requires networks to use a fully-meshed router configuration. This requirement does not scale well, especially when BGP is used as an interior gateway protocol. One way to reduce the size of a fully-meshed AS is to divide the AS into multiple sub-autonomous systems and group them into a routing confederation. Within the confederation, each sub-AS must be fully-meshed. The confederation is advertised to other networks as a single AS.

Use a confederation ID of 0 to indicate no confederation.

Example
The following command specifies the BGP routing confederation ID as 200:

    configure bgp confederation-id 200

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp delete aggregate-address

   configure bgp delete aggregate-address [<ip address/masklength> | all]

Description
Deletes one or all BGP aggregated route.

Syntax Description

| ip address/mask length      | Specifies an IP address and netmask length. |
| all                         | Specifies all aggregated routes.            |

Default
N/A.

Usage Guidelines
Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

Example
The following command deletes a BGP aggregate route:

   configure bgp delete aggregate-address 192.1.1.4/30

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp delete confederation-peer sub-AS-number

    configure bgp delete confederation-peer sub-AS-number <number>

Description
Specifies a sub-AS that should be deleted from a confederation.

Syntax Description

<table>
<thead>
<tr>
<th>number</th>
<th>Specifies a sub-AS-number.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
BGP requires networks to use a fully-meshed router configuration. This requirement does not scale well, especially when BGP is used as an interior gateway protocol. One way to reduce the size of a fully-meshed AS is to divide the AS into multiple sub-autonomous systems and group them into a routing confederation. Within the confederation, each sub-AS must be fully-meshed. The confederation is advertised to other networks as a single AS.

Example
The following command deletes a sub-AS from a confederation:

```
configure bgp delete confederation-peer sub-AS-number 65002
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp delete network

configure bgp delete network [all | <ip address>/<masklength>]

Description
Deletes a network to be originated from this router.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all networks.</td>
</tr>
<tr>
<td>ip address/mask length</td>
<td>Specifies an IP address and a netmask length.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command deletes a network to be originated from this router:
configure bgp delete network 192.1.1.12/30

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
configure bgp local-preference

configure bgp local-preference <number>

Description
Changes the default local preference attribute.

Syntax Description

| number | Specifies a value used to advertise this router’s degree of preference to other routers within the AS.

Default
100.

Usage Guidelines
The range is 0 to 2,147,483,647.

BGP selects routes based on the following precedence (from highest to lowest):
- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example
The following command changes the default local preference attribute to 500:

configure bgp local-preference 500

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp med

    configure bgp med [none | <number>]

Description
Configures the metric to be included in the Multi-Exit-Discriminator (MED) path attribute. The MED path attribute is included in route updates sent to external peers if a value is configured.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies not to use a multi-exist-discriminator number.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a multi-exist-discriminator number. The valid range is from 0 to 2,147,483,647.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example
The following command configures the metric to be included in the MED path attribute:

```
configure bgp med 3
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
**configure bgp neighbor as-path-filter**

configure bgp neighbor [<ip address> | all] as-path-filter [in|out] [none | <access profile>]

**Description**
Configures the AS path filter for a neighbor.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to install the filter on the input side.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to install the filter on the output side.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to remove the filter.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
The filter is defined using the access-profile mechanism and can be installed on the input side and/or the output side of the router.

**Example**
The following command configures the AS path filter for a neighbor based on the access profile nosales:

configure bgp neighbor 192.1.1.22 as-path-filter in nosales

**History**
This command was available in ExtremeWare 6.1.

**Platform Availability**
This command is available on “i” series of switches.
configure bgp neighbor dampening

configure bgp neighbor [<ip address> | all] dampening {{<half-life> {<reuse> <suppress> <max-suppress> }} | {route-map <route map>}}

Description
Configures route flap dampening over BGP peer sessions.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>half-life</td>
<td>Specifies the dampening half life.</td>
</tr>
<tr>
<td>reuse</td>
<td>Specifies the reuse limit.</td>
</tr>
<tr>
<td>suppress</td>
<td>Specifies the suppress limit.</td>
</tr>
<tr>
<td>max-suppress</td>
<td>Specifies the maximum hold down time.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map</td>
</tr>
</tbody>
</table>

Default
This feature is disabled by default.

Usage Guidelines
The half life is the period of time, in minutes, during which the accumulated penalty of a route is reduced by half. The range is 1 to 45 minutes, and the default is 15 minutes.

The reuse limit is the penalty value below which a route will be used again. The range is 1-20,000, and the default is 750.

The suppress limit is the penalty value above which a route will be suppressed. The range is 1-20,000, and the default is 2,000.

The maximum hold down time is the maximum time a route can be suppressed, no matter how unstable it has been, as long as it no longer flaps. The range is 1-255 minutes, and the default is 4 * the half life.

Use the following command to disable route flap dampening for BGP neighbors:

configure bgp neighbor [<ip address> | all] no-dampening

Example
The following command configures route flap dampening to the BGP neighbor at 192.168.1.22:

configure bgp neighbor 192.168.1.22 dampening

History
This command was first available in ExtremeWare 7.0.0.
Platform Availability

This command is available on “i” series of switches.
configure bgp neighbor maximum-prefix

configure bgp neighbor [<ip address> | all] maximum-prefix <number>
  {{threshold <percent>}} {teardown {holddown-interval <seconds>}}
  {send-traps}

Description
Configures the maximum number of IP prefixes accepted from a BGP neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the maximum number of prefixes accepted. The range is 0 to 4294967294. A value of 0 disables prefix limit feature.</td>
</tr>
<tr>
<td>percent</td>
<td>Specifies the percentage of the maximum prefix (threshold) at which a warning message is printed in the log (and console), and/or a trap will be sent to the SNMP manager.</td>
</tr>
<tr>
<td>teardown</td>
<td>Specifies that the peer session is torn down when the maximum is exceeded.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the length of time before the session is re-established. If the session is torn down due to maximum prefix exceeded, it is kept down until the peer is enabled. The range is 30 to 864000 seconds.</td>
</tr>
<tr>
<td>send-traps</td>
<td>Specifies sending “number of prefix reached threshold” and “number of prefix exceed the max-prefix limit” SNMP traps.</td>
</tr>
</tbody>
</table>

Default
This feature is disabled by default.

The default threshold is 75%.

By default, teardown is not specified.

By default, send-traps is not specified.

Usage Guidelines
Configure the peer group before configuring the neighbors. To configure the peer group, use the following command:

configure bgp peer-group maximum-prefix

Example
The following command configures the maximum number of IP prefixes accepted from all neighbors to 5000, sets the threshold for warning messages to 60%, and specifies SNMP traps:

configure bgp neighbor all maximum-prefix 5000 threshold 60 send-traps

History
This command was introduced in ExtremeWare 6.2.2.
Platform Availability

This command is available on “i” series of switches.
configure bgp neighbor next-hop-self

configure bgp neighbor [<ip address> | all] [next-hop-self | no-next-hop-self]

Description
Configures the next hop address used in the outgoing updates to be the address of the BGP connection originating the update.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>next-hop-self</td>
<td>Specifies that the next hop address used in the updates be the address of</td>
</tr>
<tr>
<td></td>
<td>the BGP connection originating the update.</td>
</tr>
<tr>
<td>no-next-hop-self</td>
<td>Specifies that the next hop address used in the updates not be the address</td>
</tr>
<tr>
<td></td>
<td>of the BGP connection originating it (lets BGP decide what would be the</td>
</tr>
<tr>
<td></td>
<td>next hop).</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
These settings apply to the peer group and all neighbors of the peer group.

Example
The following command configures the next hop address used in the updates to be the address of the BGP connection originating it:

configure bgp neighbor 172.16.5.25 next-hop-self

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor nlri-filter

configure bgp neighbor [<ip address> | all] nlri-filter [in | out] [none | <access profile>]

**Description**

Configures an NLRI filter for a neighbor.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies a BGP neighbor IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to install the filter on the input side.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to install the filter on the output side.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to remove the filter.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

The NLRI filter is defined using the access-profile mechanism and can be installed on the input side and/or the output side of the router.

**Example**

The following command configures the NLRI filter for a neighbor based on the access profile nosales:

```bash
configure bgp neighbor 192.1.1.22 nlri-filter in nosales
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on “i” series of switches.
configure bgp neighbor no-dampening

configure bgp neighbor [<ip address> | all] no-dampening

Description
Configures no route flap dampening over BGP peer sessions (disables route flap dampening).

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
</tbody>
</table>

Default
This feature is disabled by default.

Usage Guidelines
Use the following command to enable route flap dampening for BGP neighbors:

configure bgp neighbor [<ip address> | all] dampening {{<half-life> {<reuse>
<suppress> <max-suppress> }} | {route-map <route map>}}

Example
The following command disables route flap dampening to the BGP neighbor at 192.168.1.22:
configure bgp neighbor 192.168.1.22 no-dampening

The following command disables route flap dampening for all neighbors:
configure bgp neighbor all no-dampening

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor password

configure bgp neighbor [all | <ip address>] password [none | {encrypted} <password>]

Description
Configures a password for a neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies not to use a password</td>
</tr>
<tr>
<td>encrypted</td>
<td>This option is for use only by the switch when generating an ASCII configuration file. Specifies that the password should be encrypted when the configuration is uploaded to a file. Do not use this option.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password string.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
When a password is configured, TCP MD5 authentication is enabled on the TCP connection that is established with the neighbor.

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

To change any one of the following parameters you must disable and re-enable the peer session:
- timer
- source-interface
- soft-in-reset
- password

Changing a route reflector client will automatically disable and enable the peer session.

NOTE
Do not select the encrypted option in the CLI.

The encrypted option is used by the switch when generating an ASCII configuration file (using the upload configuration command), and parsing a switch-generated configuration file (using the download configuration command). Do not select the encrypted option in the CLI.

Example
The following command configures the password for a neighbor as *Extreme*:
configure bgp neighbor 192.168.1.5 password extreme

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on "i" series of switches.
configure bgp neighbor peer-group

configure bgp neighbor [all | <ip address>] peer-group [<peer group> | none] {acquire-all}

Description
Configures an existing neighbor as the member of a peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>peer group</td>
<td>Specifies a peer group name.</td>
</tr>
<tr>
<td>none</td>
<td>Removes the neighbor from the peer group.</td>
</tr>
<tr>
<td>acquire-all</td>
<td>Specifies that all parameters should be inherited by the neighbor from the peer group.</td>
</tr>
</tbody>
</table>

Default
By default, remote AS (if configured for the peer group), source-interface, out-NLRI-filter, out-ASPath-filter, out-route-map, send-community and next-hop-self settings are inherited.

Usage Guidelines
If acquire-all is not specified, only the default parameters are inherited by the peer group.

When you remove a neighbor from a peer group, it retains the parameter settings of the group. The parameter values are not reset to those the neighbor had before it inherited the peer group values.

To create a new neighbor and add it to a BGP peer group, use the following command:

create bgp neighbor <ip address> peer-group <peer group> {multi-hop}

The new neighbor is created as part of the peer group and inherits all of the existing parameters of the peer group. The peer group must have remote AS configured.

Example
The following command configures an existing neighbor as the member of the peer group outer:

configure bgp neighbor 192.1.1.22 peer-group outer

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor route-map-filter

configure bgp neighbor [<ip address> | all] route-map-filter [in | out] [none | <route map>]

Description
Configures a route map filter for a neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to install the filter on the input side.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to install the filter on the output side.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to remove the filter.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The route map filter can be installed on the input or output side of the router. The route map is used to modify or filter the NLRI information and the path attributes associated with it when exchanging updates with the neighbor.

Example
The following command configures the filter called route-map-filter for a neighbor based on the access profile nosales:

```
configure bgp neighbor 192.168.1.22 route-map-filter in nosales
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor route-reflector-client

configure bgp neighbor [<ip address> | all] [route-reflector-client | no-route-reflector-client]

Description
Configures a BGP neighbor to be a route reflector client.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>route-reflector-client</td>
<td>Specifies for the BGP neighbor to be a route reflector client.</td>
</tr>
<tr>
<td>no-route-reflector-client</td>
<td>Specifies for the BGP neighbor not to be a route reflector client.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Another way to overcome the difficulties of creating a fully-meshed AS is to use route reflectors. Route reflectors allow a single router to serve as a central routing point for the AS or sub-AS.

Use this command to implicitly define the router to be a route reflector. The neighbor must be in the same AS as the router.

When changing the route reflector status of a peer, the peer will automatically be disabled and re-enabled and a warning message will appear on the console and in the log.

A cluster is formed by the route reflector and its client routers. Peer routers that are not part of the cluster must be fully meshed according to the rules of BGP.

Example
The following command configures a BGP neighbor to be a route reflector client:

```
configure bgp neighbor 192.168.1.5 route-reflector-client
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor send-community

configure bgp neighbor [<ip address> | all] [send-community | dont-send-community]

Description

Configures whether the community path attribute associated with a BGP NLRI should be included in the route updates sent to the BGP neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>send-community</td>
<td>Specifies to include the community path attribute.</td>
</tr>
<tr>
<td>dont-send-community</td>
<td>Specifies not to include the community path attribute.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

A BGP community is a group of BGP destinations that require common handling. ExtremeWare supports the following well-known BGP community attributes:

- no-export
- no-advertise
- no-export-subconfed

Example

The following command includes the community path attribute associated with a BGP NLRI in the route updates sent to all BGP neighbors:

```
configure bgp neighbor all send-community
```

History

This command was first available in ExtremeWare 6.1.

Platform Availability

This command is available on “i” series of switches.
configure bgp neighbor soft-reset

configure bgp neighbor [<ip address> | all] soft-reset {in | out}

Description
Applies the current input or output routing policy to the routing information already exchanged with the neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to apply the input routing policy.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to apply the output routing policy.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The input/output policy is determined by the NLRI-filter, AS-path-filter, and the route map configured for the neighbor on the input and/or output side of the router. This command does not affect the switch configuration.

Example
The following command applies the current input routing policy to the routing information already exchanged with the neighbor:

```
configure bgp neighbor 192.168.1.5 soft-reset in
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor source-interface

configure bgp neighbor [<ip address> | all] source-interface [any | vlan <vlan name>]

Description
Changes the BGP source interface for TCP connections.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies any source interface.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name as a source interface for TCP.</td>
</tr>
</tbody>
</table>

Default
Any.

Usage Guidelines
None.

Example
The following command changes the BGP source interface on the VLAN accounting:
configure bgp neighbor 192.168.1.5 source-interface vlan accounting

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor timer

configure bgp neighbor [ip address | all] timer keep-alive <keepalive>
hold-time <holdtime>

Description
Configures the BGP neighbor timers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>keepalive</td>
<td>Specifies a BGP neighbor timer keepalive time in seconds. The range is 0 to 21,845 seconds.</td>
</tr>
<tr>
<td>holdtime</td>
<td>Specifies a BGP neighbor timer hold time in seconds. The range is 3 to 65,535 seconds.</td>
</tr>
</tbody>
</table>

Default
The default keepalive setting is 60 seconds. The default hold time is 180 seconds.

Usage Guidelines
None.

Example
The following command configures the BGP neighbor timers:

```
configure bgp neighbor 192.168.1.5 timer keep-alive 120 hold-time 360
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp neighbor weight

configure bgp neighbor [ip address | all] weight <weight>

Description
Assigns a locally-used weight to a neighbor connection for the route selection algorithm.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>weight</td>
<td>Specifies a BGP neighbor weight.</td>
</tr>
</tbody>
</table>

Default
0.

Usage Guidelines
All routes learned from this peer are assigned the same weight. The route with the highest weight is more preferable when multiple routes are available to the same network. The range is 0 to 4294967295.

BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example
The following command assigns a locally used weight of 10 to a neighbor connection:

```
configure bgp neighbor 192.168.1.5 weight 10
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group as-path-filter

configure bgp peer-group <peer group> as-path-filter [in | out] [none | <access profile>]

Description
Configures the AS-path filters for a peer group and all neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to install the filter on the input side.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to install the filter on the output side.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to remove the filter.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command configures the as-path filters for the peer group outer and its neighbors using the access profile nosales:

configure bgp peer-group outer as-path-filter in nosales

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
**configure bgp peer-group dampening**

```
configure bgp peer group <name> dampening {{<half-life> {<reuse> <suppress> {<max-suppress> }} | {route-map <route map>}}}
```

**Description**
Configures route flap dampening for a BGP peer group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies a peer group</td>
</tr>
<tr>
<td>half-life</td>
<td>Specifies the dampening half life.</td>
</tr>
<tr>
<td>reuse</td>
<td>Specifies the reuse limit.</td>
</tr>
<tr>
<td>suppress</td>
<td>Specifies the suppress limit.</td>
</tr>
<tr>
<td>max-suppress</td>
<td>Specifies the maximum hold down time.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map</td>
</tr>
</tbody>
</table>

**Default**
This feature is disabled by default.

**Usage Guidelines**
The half life is the period of time, in minutes, during which the accumulated penalty of a route is reduced by half. The range is 1 to 45 minutes, and the default is 15 minutes.

The reuse limit is the penalty value below which a route will be used again. The range is 1-20,000, and the default is 750.

The suppress limit is the penalty value above which a route will be suppressed. The range is 1-20,000, and the default is 2,000.

The maximum hold down time is the maximum time a route can be suppressed, no matter how unstable it has been, as long as it no longer flaps. The range is 1-255 minutes, and the default is 4 * the half life.

Use the following command to disable route flap dampening for a BGP peer-group:

```
configure bgp peer-group <name> no-dampening
```

**Example**
The following command configures route flap dampening for the BGP peer group outer:

```
configure bgp peer-group outer dampening
```

**History**
This command was first available in ExtremeWare 7.0.0.
Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group maximum-prefix

configure bgp peer-group <name> maximum-prefix <number> {{threshold <percent>}} {teardown {holddown-interval <seconds>}} {send-traps}

Description
Configures the maximum number of IP prefixes accepted for all neighbors in the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the maximum number of prefixes accepted. The range is 0 to 4294967294. A value of 0 disables prefix limit feature.</td>
</tr>
<tr>
<td>percent</td>
<td>Specifies the percentage of the maximum prefix (threshold) at which a warning message is printed in the log (and on the console). An SNMP trap can also be sent.</td>
</tr>
<tr>
<td>teardown</td>
<td>Specifies that the peer session is torn down when the maximum is exceeded.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the length of time before the session is re-established. If the session has been torn down due to exceeding the max limit, it is kept down until the peer is enabled. The range is 30 to 86400 seconds.</td>
</tr>
<tr>
<td>send-traps</td>
<td>Specifies sending “number of prefix reached threshold” and “number of prefix exceed the max-prefix limit” SNMP traps.</td>
</tr>
</tbody>
</table>

Default
This feature is disabled by default.

The default threshold is 75%.

By default, teardown is not specified.

By default, send-traps is not specified.

Usage Guidelines
Configure the peer group before configuring the neighbors. To configure the neighbors, use the following command:

```
configure bgp neighbor 192.168.1.1 maximum-prefix
```

Example
The following command configures the maximum number of IP prefixes accepted from the peer group outer to 5000, sets the threshold for warning messages to 60%, and specifies SNMP traps:

```
configure bgp peer-group outer maximum-prefix 5000 threshold 60 send-traps
```

History
This command was introduced in ExtremeWare 6.2.2.
Platform Availability

This command is available on “i” series of switches.
configure bgp peer-group next-hop-self

configure bgp peer-group <peer group> [next-hop-self | no-next-hop-self]

Description
Configures the next hop address used in the updates to be the address of the BGP connection originating the update.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>next-hop-self</td>
<td>Specifies that the next hop address used in the updates be the address of</td>
</tr>
<tr>
<td></td>
<td>the BGP connection originating it.</td>
</tr>
<tr>
<td>no-next-hop-self</td>
<td>Specifies that the next hop address used in the updates not be the address</td>
</tr>
<tr>
<td></td>
<td>of the BGP connection originating it.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
These settings apply to the peer group and all neighbors of the peer group.

Example
The following command configures the next hop address used in the updates to be the address of the BGP connection originating it:

```
configure bgp peer-group outer next-hop-self
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group nlri-filter

configure bgp peer-group <peer group> nlri-filter [in | out] [none | <access profile>]

**Description**

Configures the NLRI filter for a peer group and all the neighbors of the peer group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to install the filter on the input side.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to install the filter on the output side.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to remove the filter.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

None.

**Example**

The following command configures the NLRI filter for the peer group *outer* and its neighbors using the access profile *nosales*:

```bash
configure bgp peer-group outer nlri-filter in nosales
```

**History**

This command was available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on “i” series of switches.
configure bgp peer-group no-dampening

configure bgp peer-group <name> no-dampening

Description
Configures no route flap dampening for a BGP peer group (disables route flap dampening).

Syntax Description

| name | Specifies a BGP peer group. |

Default
This feature is disabled by default.

Usage Guidelines
Use the following command to enable route flap dampening for a BGP peer-group:

configure bgp peer-group <name> dampening {{<half-life> {<reuse> <suppress> <max-suppress> }} | {route-map <route map>}}

Example
The following command disables route flap dampening to the BGP peer group outer:

configure bgp peer-group no-dampening

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group route-reflector-client

configure bgp peer-group <peer group> [route-reflector-client | no-route-reflector-client]

Description
Configures all the peers in a peer group to be a route reflector client.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>route-reflector-client</td>
<td>Specifies that all the neighbors in the peer group be a route reflector client.</td>
</tr>
<tr>
<td>no-route-reflector-client</td>
<td>Specifies that all the neighbors in the peer group not be a route reflector client.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command implicitly defines this router to be a route reflector.

The peer group must be in the same AS of this router.

Example
The following command configures the peer group outer as a route reflector client:

```
configure bgp peer-group outer route-reflector-client
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group send-community

    configure bgp peer-group <peer group> [send-community |
        dont-send-community]

Description
Configures whether communities should be sent to neighbors as part of route updates.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>send-community</td>
<td>Specifies that communities are sent to neighbors as part of route updates.</td>
</tr>
<tr>
<td>dont-send-community</td>
<td>Specifies that communities are not sent to neighbors as part of route updates.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
These settings apply to the peer group and all neighbors of the peer group.

Example
The following command configures communities to be sent to neighbors as part of route updates:
configure bgp peer-group outer send-community

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group password

configure bgp peer-group <peer group> password {encrypted} [none | <password>]

Description
Configures the password for a peer group and all neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>encrypted</td>
<td>Specifies an encrypted password.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no password.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies a password.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:
- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example
The following command configures the password as *Extreme* for the peer group *outer* and its neighbors:

```
configure bgp peer-group outer password extreme
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
**configure bgp peer-group remote-AS-number**

`configure bgp peer-group <peer group> remote-AS-number <number>`

**Description**
Configures the remote AS number for a peer group and all the neighbors of the peer group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a remote AS number.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:
- remote-as
- timer
- source-interface
- soft-in-reset
- password

**Example**
The following command configures the remote AS number for the peer group `outer` and its neighbors:
`configure bgp peer-group outer remote-AS-number 65001`

**History**
This command was available in ExtremeWare 6.1.5.

**Platform Availability**
This command is available on “i” series of switches.
configure bgp peer-group route-map-filter

configure bgp peer-group <peer group> route-map-filter [in | out] [none | <routemap>]

Description
Configures the route maps for a peer group and all the neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to install the filter on the input side.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to install the filter on the output side.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to remove the filter.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command configures the route map filter for the peer group outer and its neighbors using the access profile nosales:

```
configure bgp peer-group outer route-map-filter in nosales
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group soft-reset

configure bgp peer-group <peer group> soft-reset {[in | out]}

Description
Applies the current input/output routing policy to the neighbors in the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>in</td>
<td>Specifies to apply the input routing policy.</td>
</tr>
<tr>
<td>out</td>
<td>Specifies to apply the output routing policy.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The input/output routing policy is determined by the NLRI-filter, AS-path-filter, and the route-map configured for the neighbors in the peer group on the input/output side of the router. This command does not affect configuration of the switch.

Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:
- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example
The following command applies the current input routing policy to the neighbors in the peer group outer:

```
configure bgp peer-group outer soft-reset in
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group source-interface

configure bgp peer-group <peer group> source-interface [any | vlan <vlan name>]

Description
Configures the source interface for a peer group and all the neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>any</td>
<td>Specifies any source interface.</td>
</tr>
<tr>
<td>name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:
- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example
The following command configures the source interface for the peer group outer and its neighbors on the VLAN accounting:

```bash
configure bgp peer-group outer source-interface accounting
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group timer

configure bgp peer-group <peer group> timer keep-alive <seconds> hold-time <seconds>

Description
Configures the keepalive timer and hold timer values for a peer group and all the neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>keep-alive &lt;seconds&gt;</td>
<td>Specifies a keepalive time in seconds.</td>
</tr>
<tr>
<td>hold-time &lt;seconds&gt;</td>
<td>Specifies a hold-time in seconds.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Changes made to the parameters of a peer group are applied to all neighbors in the peer group.

Modifying the following parameters automatically disables and enables the neighbors before changes take effect:

- remote-as
- timer
- source-interface
- soft-in-reset
- password

Example
The following command configures the keepalive timer and hold timer values for the peer group outer and its neighbors:

configure bgp peer-group outer timer keep-alive 30 hold-time 90

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
configure bgp peer-group weight

configure bgp peer-group <peer group> weight <number>

Description
Configures the weight for the peer group and all the neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a BGP peer group weight.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
BGP selects routes based on the following precedence (from highest to lowest):

- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest routerID

Example
The following command configures the weight for the peer group outer and its neighbors:

```
configure bgp peer-group outer weight 5
```

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
**configure bgp routerid**

`configure bgp routerid <router identifier>`

**Description**
Changes the router identifier.

**Syntax Description**

| router identifier | Specifies a router identifier. |

**Default**
N/A.

**Usage Guidelines**
BGP must be disabled before changing the router ID.

BGP selects routes based on the following precedence (from highest to lowest):
- higher weight
- higher local preference
- shortest length (shortest AS path)
- lowest origin code
- lowest MED
- route from external peer
- lowest cost to Next Hop
- lowest router ID

**Example**
The following command changes the router ID:
`configure bgp router-id 192.1.1.13`

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on “i” series of switches.
configure bgp soft-reconfiguration

Description
Immediately applies the route map associated with the network command, aggregation, and redistribution.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
This command does not affect the switch configuration.

Example
The following command applies the route map associated with the network command, aggregation and redistribution:
configure bgp soft-reconfiguration

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
create bgp neighbor peer-group

create bgp neighbor <ip address> peer-group <peer group> {multi-hop}

**Description**
Creates a new neighbor and makes it part of the peer group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>multi-hop</td>
<td>Specifies to allow connections to EBGP peers that are not directly connected.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
All the parameters of the neighbor are inherited from the peer group. The peer group should have the remote AS configured.

To add an existing neighbor to a peer group, use the following command:

```
configure bgp neighbor [<ip address> | all] peer-group <peer group> {acquire-all}
```

If you do not specify acquire-all, only the mandatory parameters are inherited from the peer group. If you specify acquire-all, all of the parameters of the peer group are inherited. This command disables the neighbor before adding it to the peer group.

**Example**
The following command creates a new neighbor and makes it part of the peer group `outer`:

```
create bgp neighbor 192.1.1.22 peer-group outer
```

**History**
This command was available in ExtremeWare 6.1.5.

**Platform Availability**
This command is available on “i” series of switches.
create bgp neighbor remote-AS-number

    create bgp neighbor <ip address> remote-AS-number <number> {multi-hop}

**Description**

Creates a new BGP peer.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a remote AS number.</td>
</tr>
<tr>
<td>multi-hop</td>
<td>Specifies to allow connections to EBGP peers that are not directly connected.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

If the AS number is the same as the AS number provided in the `configure bgp as` command, then the peer is considered an IBGP peer, otherwise the neighbor is an EBGP peer. The BGP session to a newly created peer is not started until the `enable bgp neighbor` command is issued.

**Example**

The following command creates a new BGP peer:

`create bgp neighbor 192.168.1.17 remote-AS-number 65001`

**History**

This command was available in ExtremeWare 6.2.

**Platform Availability**

This command is available on “i” series of switches.
create bgp peer-group

create bgp peer-group <name>

Description
Creates a new peer group.

Syntax Description

<table>
<thead>
<tr>
<th>name</th>
<th>Specifies a peer group.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
You can use BGP peer groups to group together up to 200 BGP neighbors. All neighbors within the peer group inherit the parameters of the BGP peer group. The following mandatory parameters are shared by all neighbors in a peer group:

- remote AS
- source-interface
- out-nlri-filter
- out-aspath-filter
- out-route-map
- send-community
- next-hop-self

Each BGP peer group is assigned a unique name when the peer group is created.

Example
The following command creates a new peer group named external:
create bgp peer-group outer

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
delete bgp neighbor

delete bgp neighbor [<ip address> | all]

Description
Deletes one or all BGP neighbors.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip address&gt;</td>
<td>Specifies the IP address of the BGP neighbor to be deleted.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to delete one or all BGP neighbors.

Example
The following command deletes the specified BGP neighbor:

delte bgp neighbor 192.168.1.17

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
delete bgp peer-group

    delete bgp peer-group <peer group>

**Description**

Deletes a peer group.

**Syntax Description**

| peer group | Specifies a peer group. |

**Default**

N/A.

**Usage Guidelines**

Use this command to delete a specific BGP peer group.

**Example**

The following command deletes the peer group named `external`:

display bgp peer-group outer

**History**

This command was available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on “i” series of switches.
disable bgp

Description
Disables BGP.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Use this command to disable BGP on the router.

Example
The following command disables BGP:

disable bgp

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on "i" series of switches.
disable bgp aggregation

disable bgp aggregation

Description
Disables BGP route aggregation.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

Use this command to disable BGP route aggregation.

Example
The following command disables BGP route aggregation:

disable bgp aggregation

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
disable bgp always-compare-med

disable bgp always-compare-med

Description
Disables Multi Exit Discriminator (MED) from being used in the route selection algorithm.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
MED is only used when comparing paths from the same AS. Use this command to disable the MED from being used when selecting a route.

Example
The following command disables MED from being used in the route selection algorithm:

disable bgp always-compare-med

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
disable bgp community format

disable bgp community format AS-number : number

**Description**
Disables the AS-number: number format of display for communities in the output of show and upload commands.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled.

**Usage Guidelines**
Using this command, communities are displayed as a single decimal value.

**Example**
The following command disables the AS-number: number format of display for communities:
disable bgp community format AS-number : number

**History**
This command was first available in ExtremeWare 6.2.

**Platform Availability**
This command is available on “i” series of switches.
disable bgp export

disable bgp export [direct | ospf | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | isis | isis-level-1 | isis-level-1-external | isis-level-2 | isis-level-2-external | rip | static | vip]

Description
Disables BGP from exporting routes from other protocols to BGP peers.

Syntax Description

<table>
<thead>
<tr>
<th>Direct / Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>Specifies direct routing.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies OSPF routing.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies OSPF-extern1 routing.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies OSPF-extern2 routing.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies OSPF-inter routing.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies OSPF-intra routing.</td>
</tr>
<tr>
<td>isis</td>
<td>Specifies IS-IS routing.</td>
</tr>
<tr>
<td>isis-level-1</td>
<td>Specifies IS-IS level 1 routing</td>
</tr>
<tr>
<td>isis-level-1-external</td>
<td>Specifies IS-IS level 1 external routing.</td>
</tr>
<tr>
<td>isis-level-2</td>
<td>Specifies IS-IS level 2 routing</td>
</tr>
<tr>
<td>isis-level-2-external</td>
<td>Specifies IS-IS level 2 external routing.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routing.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routing.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routing.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
The exporting of routes between any two routing protocols is a discreet configuration function. For example, you must configure the switch to export routes from OSPF to BGP and, if desired, you must configure the switch to export routes from BGP to OSPF. You must first configure both protocols and then verify the independent operation of each. Then you can configure the routes to export from OSPF to BGP, and the routes to export from BGP to OSPF. Similarly for BGP and ISIS, or BGP and RIP.

You can use route maps to associate BGP attributes including Community, NextHop, MED, Origin, and Local Preference with the routes. Route maps can also be used to filter out exported routes.

Using the export command to redistribute routes complements the redistribution of routes using the configure bgp add network command. The configure bgp add network command adds the route to BGP only if the route is present in the routing table. The enable bgp export command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the network command take precedence over routes redistributed using the export command.
Example
The following command disables BGP from exporting routes from the OSPF protocol to BGP peers:

disable bgp export ospf

History
This command was first available in ExtremeWare 6.1.
The IS-IS options were added in ExtremeWare 7.0.0

Platform Availability
This command is available on “i” series of switches.
disable bgp neighbor

disable bgp neighbor [<ip address> | all]

Description
Disables the BGP session.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
After the session has been disabled, all the information in the route information base (RIB) for the neighbor is flushed.

Example
The following command disables the BGP session:

disable bgp neighbor 192.1.1.17

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
disable bgp neighbor remove-private-AS-numbers

disable bgp neighbor [<ip address> | all] remove-private-AS-numbers

Description
Disables the removal of private AS numbers from the AS path in route updates sent to EBGP peers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
Private AS numbers are AS numbers in the range 64512 through 65534. You can remove private AS numbers from the AS path attribute in updates that are sent to external BGP (EBGP) neighbors. Possible reasons for using private AS numbers include:
- The remote AS does not have officially allocated AS numbers.
- You want to conserve AS numbers if you are multi-homed to the local AS.

Private AS numbers should not be advertised on the Internet. Private AS numbers can only be used locally within an administrative domain. Therefore, when routes are advertised out to the Internet, the private AS number can be stripped out from the AS paths of the advertised routes using this feature.

Example
The following command disables the removal of private AS numbers from the AS path in route updates sent to the EBGP peers:

disable bgp neighbor 192.168.1.17 remove-private-AS-numbers

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
disable bgp neighbor soft-in-reset

disable bgp neighbor [all | <ip address>] soft-in-reset

Description
Disables the soft input reset feature.

Syntax Description

<table>
<thead>
<tr>
<th>all</th>
<th>Specifies all neighbors.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
Disabling the soft input reset feature can potentially limit the amount of system memory consumed by the RIB-in.

Example
The following command disables the soft input reset feature:

disable bgp neighbor 192.168.1.17 soft-in-reset

History
This command was available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
disable bgp peer-group

disable bgp peer-group <peer group> {soft-in-reset} {remove-private-AS-numbers}

Description
Disables a BGP peer group and all the neighbors of the peer group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>soft-in-reset</td>
<td>Specifies the soft input reset feature.</td>
</tr>
<tr>
<td>remove-private-AS-numbers</td>
<td>Specifies to remove private AS numbers.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
You can use BGP peer groups to group together up to 200 BGP neighbors. All neighbors within the peer group inherit the parameters of the BGP peer group. The following mandatory parameters are shared by all neighbors in a peer group:

- remote AS
- source-interface
- out-nlri-filter
- out-aspath-filter
- out-route-map
- send-community
- next-hop-self

Example
The following command disables the BGP peer group outer and all of its neighbors:

disable bgp peer-group outer

History
This command was available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
disable bgp synchronization

disable bgp synchronization

Description
Disables the synchronization between BGP and IGP.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
When enabled, BGP waits for IGP to provide the exact same IP route before installing the route into the local forwarding database and advertising the route to an external neighbor.

Example
The following command disables the synchronization between BGP and IGP:

disable bgp synchronization

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
enable bgp

enable bgp

Description
Enables BGP.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
This command enables the Border Gateway Protocol (BGP) on the router. Before invoking this command, the local AS number and BGP router ID must be configured.

Example
The following command enables BGP:

```
enable bgp
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
enable bgp aggregation

enable bgp aggregation

Description
Enables BGP route aggregation.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Route aggregation is the process of combining the characteristics of several routes so that they are advertised as a single route. Aggregation reduces the amount of information that a BGP speaker must store and exchange with other BGP speakers. Reducing the information that is stored and exchanged also reduces the size of the routing table.

To use BGP route aggregation, follow these steps:
1. Enable aggregation using the following command:
   
   enable bgp aggregation

2. Create an aggregate route using the following command:
   
   configure bgp add aggregate-address <ip address>/ <mask length> {as-set | as-match} {summary-only} {advertise-route-map <route-map>} {attribute-route-map <route-map>}

Example
The following command enables BGP route aggregation:

   enable bgp aggregation

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
enable bgp always-compare-med

Description
Enables BGP to use the Multi Exit Discriminator (MED) from neighbors in different autonomous systems (ASs) in the route selection algorithm.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
MED is only used when comparing paths from the same AS. A MED value of zero is treated as the lowest MED and therefore the most preferred route.

Example
The following command enables BGP to use the Multi Exit Discriminator (MED) from neighbors in different autonomous systems in the route selection algorithm:

```
enable bgp always-compare-med
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
enable bgp community format

    enable bgp community format AS-number : number

Description
Enables the as-number:number format of display for the communities in the output of show and upload commands.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
If not enabled, the communities are displayed as a single decimal value.

Example
The following command enables the AS-number:number format of display for communities:

    enable bgp community format AS-number : number

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
enable bgp export

`enable bgp export [direct | ospf | ospf-extern1 | ospf-extern2 | ospf-inter | ospf-intra | isis | isis-level-1 | isis-level-1-external | isis-level-2 | isis-level-2-external | rip | static | vip] {<route map>}

Description

Enables BGP to export routes from other protocols to BGP peers.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>Specifies direct routing.</td>
</tr>
<tr>
<td>ospf</td>
<td>Specifies OSPF routing.</td>
</tr>
<tr>
<td>ospf-extern1</td>
<td>Specifies OSPF-extern1 routing.</td>
</tr>
<tr>
<td>ospf-extern2</td>
<td>Specifies OSPF-extern2 routing.</td>
</tr>
<tr>
<td>ospf-inter</td>
<td>Specifies OSPF-inter routing.</td>
</tr>
<tr>
<td>ospf-intra</td>
<td>Specifies OSPF-intra routing.</td>
</tr>
<tr>
<td>isis</td>
<td>Specifies IS-IS routing.</td>
</tr>
<tr>
<td>isis-level-1</td>
<td>Specifies IS-IS level 1 routing</td>
</tr>
<tr>
<td>isis-level-1-external</td>
<td>Specifies IS-IS level 1 external routing.</td>
</tr>
<tr>
<td>isis-level-2</td>
<td>Specifies IS-IS level 2 routing</td>
</tr>
<tr>
<td>isis-level-2-external</td>
<td>Specifies IS-IS level 2 external routing.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies RIP routing.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies static routing.</td>
</tr>
<tr>
<td>vip</td>
<td>Specifies VIP routing.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

Default

Disabled.

Usage Guidelines

The exporting of routes between any two routing protocols is a discreet configuration function. For example, you must configure the switch to export routes from OSPF to BGP and, if desired, you must configure the switch to export routes from BGP to OSPF. You must first configure both protocols and then verify the independent operation of each. Then, you can configure the routes to export from OSPF to BGP, and the routes to export from BGP to OSPF. Similarly for BGP and ISIS, or BGP and RIP.

You can use route maps to associate BGP attributes including Community, NextHop, MED, Origin, and Local Preference with the routes. Route maps can also be used to filter out exported routes.

Using the `export` command to redistribute routes complements the redistribution of routes using the `configure bgp add network` command. The `configure bgp add network` command adds the route to BGP only if the route is present in the routing table. The `enable bgp export` command redistributes an individual route from the routing table to BGP. If you use both commands to redistribute routes, the routes redistributed using the `network` command take precedence over routes redistributed using the `export` command.
Example
The following command enables BGP to export routes from the OSPF protocol to BGP peers:
```
enable bgp export ospf
```

History
This command was first available in ExtremeWare 6.1.
The IS-IS options were added in ExtremeWare 7.0.0

Platform Availability
This command is available on “i” series of switches.
enable bgp neighbor

   enable bgp neighbor [<ip address> | all]

Description
Enables the BGP session. The neighbor must be created before the BGP neighbor session can be enabled.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
To create a new neighbor and add it to a BGP peer group, use the following command:

create bgp neighbor <ip address> peer-group <peer group> {multi-hop}

Example
The following command enables the BGP neighbor session:

enable bgp neighbor 192.168.1.17

History
This command was available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
enable bgp neighbor remove-private-AS-numbers

    enable bgp neighbor [<ip address> | all] remove-private-AS-numbers

Description
Enables the removal of private AS numbers from the AS path in route updates sent to EBGP peers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
Private AS numbers are AS numbers in the range 64512 through 65534. You can remove private AS numbers from the AS path attribute in updates that are sent to external BGP (EBGP) neighbors. Possible reasons for using private AS numbers include:

- The remote AS does not have officially allocated AS numbers.
- You want to conserve AS numbers if you are multi-homed to the local AS.

Private AS numbers should not be advertised on the Internet. Private AS numbers can only be used locally within an administrative domain. Therefore, when routes are advertised out to the Internet, the routes can be stripped out from the AS paths of the advertised routes using this feature.

Example
The following command enables the removal of private AS numbers from the AS path in route updates sent to the EBGP peers:

    enable bgp neighbor 192.168.1.17 remove-private-AS-numbers

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
enable bgp neighbor soft-in-reset

    enable bgp neighbor [all | <ip address>] soft-in-reset

Description
Enables the soft input reset feature.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all neighbors.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
Disabling the soft input reset feature can potentially limit the amount of system memory consumed by the RIB-in.

Example
The following command enables the soft recognition feature:

```
enable bgp neighbor 192.168.1.17 soft-in-reset
```

History
This command was available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
enable bgp peer-group

enable bgp peer-group <peer group> {soft-in-reset} {remove-private-AS-numbers}

**Description**

Enables a peer group and all the neighbors of a peer group.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>soft-in-reset</td>
<td>Specifies the soft recognition feature.</td>
</tr>
<tr>
<td>remove-private-AS-numbers</td>
<td>Specifies to remove private AS numbers.</td>
</tr>
</tbody>
</table>

**Default**

Disabled.

**Usage Guidelines**

You can use BGP peer groups to group together up to 200 BGP neighbors. All neighbors within the peer group inherit the parameters of the BGP peer group. The following mandatory parameters are shared by all neighbors in a peer group:

- remote AS
- source-interface
- out-nlri-filter
- out-aspath-filter
- out-route-map
- send-community
- next-hop-self

**Example**

The following command enables the BGP peer group *outer* and all its neighbors:

```plaintext
enable bgp peer-group outer
```

**History**

This command was available in ExtremeWare 6.1.5.

**Platform Availability**

This command is available on “i” series of switches.
enable bgp synchronization

    enable bgp synchronization

Description
Enables synchronization between BGP and IGP.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
When enabled, BGP waits for IGP to provide the exact same route before advertising the BGP route to an external neighbor.

Example
The following command enables synchronization between BGP and IGP:

    enable bgp synchronization

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on “i” series of switches.
show bgp

Description
Displays BGP configuration information.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Displays information such as AS number, router ID, local preference, sync flag, route reflection, cluster ID, confederation ID, and AS redistributed networks.

Example
The following command displays BGP configuration information:

```
show bgp
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series of switches.
show bgp neighbor

show bgp neighbor <ip address> {[accepted-routes | flap-statistics | received-routes | rejected-routes | suppressed-routes | transmitted-routes] (detail) [community [access-profile <access profile> | no-advertise | no-export | no-export-subconfed | number <community number> | <autonomous system id>:<bgp community>] | as-path [<as-path-expression> | access-profile <access profile>] | route-map <route map> | network <ip address>/<mask> (exact) | all]}

Description
Displays information about a specified neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address that identifies a BGP neighbor.</td>
</tr>
<tr>
<td>accepted-routes</td>
<td>Specifies that only accepted routes should be displayed.</td>
</tr>
<tr>
<td>flap-statistics</td>
<td>Specifies that only flap-statistics should be displayed (for route flap dampening enabled routes).</td>
</tr>
<tr>
<td>received-routes</td>
<td>Specifies that only received routes should be displayed.</td>
</tr>
<tr>
<td>rejected-routes</td>
<td>Specifies that only rejected routes should be displayed.</td>
</tr>
<tr>
<td>suppressed-routes</td>
<td>Specifies that only suppressed routes should be displayed (for route flap dampening enabled routes).</td>
</tr>
<tr>
<td>transmitted-routes</td>
<td>Specifies that only transmitted routes should be displayed.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile used as a community attribute.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies the no-advertise community attribute.</td>
</tr>
<tr>
<td>no-export</td>
<td>Specifies the no-export community attribute.</td>
</tr>
<tr>
<td>no-export-subconfed</td>
<td>Specifies the no-export-subconfed community attribute.</td>
</tr>
<tr>
<td>community number</td>
<td>Specifies a community number.</td>
</tr>
<tr>
<td>autonomous system id</td>
<td>Specifies an autonomous system ID (0-65535).</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask (number of bits).</td>
</tr>
<tr>
<td>exact</td>
<td>Specifies an exact match with the IP address and subnet mask.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all routes.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Use this command to display information about a specific BGP neighbor. If you do not specify a neighbor, information about all neighbors is displayed.
Example
The following command displays information about a specified neighbor:

```
show bgp neighbor 10.10.10.10
```

Following is the output from this command:

```
IBGP Peer: 10.10.10.10  As: 14490  Enabled: Yes  Router: Enabled  Weight: 1
ConnectRetry: 120   HoldTimeCfg: 180   KeepaliveCfg: 60   MinAsOrig:15
Source Interface: Not configured  RRClient: No  EBGP-Multihop: No
NextHopSelf: Enabled  Send Communities: No  Soft Input Reconfiguration: Disabled
Max-Prefix: 100000  Threshold: 75  Teardown: Yes(HoldInt: 300)  SendTraps: No
Remove Private AS : No
IN NLRI Filter    : None
OUT NLRI Filter   : None
IN AS-Path Filter : None
OUT AS-Path Filter: None
IN ROUTE-MAP      : None
OUT ROUTE-MAP     : None
State: IDLE(Reached maximum prefix limit)
RemoteAddr: 10.10.10.10:179  LocalAddr: 10.10.10.51:1024  PeerRtrId: 0.0.0.0
InUpdates: 26549  OutUpdates(InQ): 0(0)  InTotalMsgs: 26559  OutTotalMsgs: 9
InUpdateElapsedTime: 0:0:0:20  InMsgElapsedTime: 0:0:0:20  InPrefix: 0
HoldTime: 180  KeepAlive: 60  FsmTransitions: 1  RestartAfter: 0:04:43
FSM Down since: Mon Apr 1 15:59:42 2002 (Duration: 0:0:0:17)
LastErr: 0/0
```

History
This command was available in ExtremeWare 6.1.

This command was modified in ExtremeWare 6.2.2 to include information about maximum prefix settings.

This command was modified in ExtremeWare 7.0.0 to show flap statistics and suppressed routes for BGP route flap dampening.

Platform Availability
This command is available on “i” series of switches.
show bgp peer-group

    show bgp peer-group {detail | <peer group> {detail}}

Description
Displays the peer groups configured in the system.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
<tr>
<td>peer group</td>
<td>Specifies a peer group.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If the `detail` keyword is specified then the parameters of the neighbors in the peer group, which are different from the ones that are configured in the peer group, will be displayed.

If no peer group name is specified, all the peer group information will be displayed.

Example
The following command displays the peer groups configured in the system:

```
show bgp peer-group detail
```

History
This command was first available in ExtremeWare 6.1.5.

Platform Availability
This command is available on “i” series of switches.
show bgp routes

show bgp routes [all | as-path <as-path-expression> | community <number> | detail | network <ip address>/<mask> {exact} | route-map <route map> ]

**Description**
Displays the BGP route information base (RIB).

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all routes.</td>
</tr>
<tr>
<td>as-path-expression</td>
<td>Specifies an AS path.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies a community number.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies a subnet mask (number of bits).</td>
</tr>
<tr>
<td>exact</td>
<td>Specifies an exact match with the IP address and subnet mask.</td>
</tr>
<tr>
<td>route map</td>
<td>Specifies a route map.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
None.

**Example**
The following command displays the BGP route information base (RIB): show bgp routes all

**History**
This command was available in ExtremeWare 6.1.

**Platform Availability**
This command is available on “i” series of switches.
BGP Commands—"i" Series Switches Only
IP multicast routing is a function that allows a single IP host to send a packet to a group of IP hosts. This group of hosts can include devices that reside on the local network, within a private network, or outside of the local network.

IP multicast routing consists of the following functions:

- A router that can forward IP multicast packets
- A router-to-router multicast protocol (for example, Distance Vector Multicast Routing Protocol (DVMRP) or Protocol Independent Multicast (PIM))
- A method for the IP host to communicate its multicast group membership to a router (for example, Internet Group Management Protocol (IGMP))

**NOTE**

You must configure IP unicast routing before you configure IP multicast routing.

IGMP is a protocol used by an IP host to register its IP multicast group membership with a router. Periodically, the router queries the multicast group to see if the group is still in use. If the group is still active, a single IP host responds to the query, and group registration is maintained.

IGMP is enabled by default on the switch. However, the switch can be configured to disable the generation of period IGMP query packets. IGMP query should be enabled when the switch is configured to perform IP unicast or IP multicast routing.

### DVMRP—“i” Series of Switches Only

Distance Vector Multicast Routing Protocol (DVMRP) is a distance-vector protocol that is used to exchange routing and multicast information between routers. Like RIP, DVMRP periodically sends the entire routing table to its neighbors.

DVMRP has a mechanism (flood and prune) that allows it to prune and graft multicast trees to reduce the bandwidth consumed by IP multicast traffic.

Protocol Independent Multicast (PIM) is a multicast routing protocol with no inherent route exchange mechanism. The “i” series of switches support both dense mode and sparse mode operation; the “e” series of switches support spare mode operation. On the “i” series of switches, you can configure dense
mode or sparse mode on a per-interface basis. After they are enabled, some interfaces can run dense mode, while others run sparse mode.

PIM Dense Mode—“i” Series of Switches Only

Protocol Independent Multicast-Dense Mode (PIM-DM) is a multicast routing protocol that is similar to DVMRP. PIM-DM routers perform reverse path multicasting (RPM). However, instead of exchanging its own unicast route tables for the RPM algorithm, PIM-DM uses the existing unicast route table for the reverse path. As a result, PIM-DM requires less system memory.

PIM-DM is a broadcast and prune protocol. Using PIM-DM, multicast routes are pruned and grafted in a similar way as DVMRP.

PIM Sparse Mode (PIM-SM)

Unlike PIM-DM, PIM-SM is an explicit join and prune protocol, and it supports shared trees as well as shortest path trees (SPTs). The routers must explicitly join the group(s) in which they are interested in becoming a member, which is beneficial for large networks that have group members who are sparsely distributed.

Using PIM-SM, the router sends a join message to the rendezvous point (RP). The RP is a central multicast router that is responsible for receiving and distributing multicast packets. By default, the RP is selected dynamically (but not automatically). You can also define a static RP in your network, using the following command:

```
configure pim crp static <rp address> [none | <access profile>] {<priority [0-254]>}
```

When a router has a multicast packet to distribute, it encapsulates the packet in a unicast message and sends it to the RP. The RP decapsulates the multicast packet and distributes it among all member routers.

When a router determines that the multicast rate from of a particular group has exceeded a configured threshold, that router can send an explicit join to the originating router. When this occurs, the receiving router gets the multicast directly from the sending router, and bypasses the RP.

On the “e” series of switches, the switch cannot act as a candidate RP or as a candidate bootstrap router (BSR).

NOTE

You can run either PIM-DM or PIM-SM per VLAN.

PIM Mode Interoperation—“i” Series of Switches Only

An Extreme Networks switch can function as a PIM multicast border router (PMBR). A PMBR integrates PIM-SM and PIM-DM traffic.

When forwarding PIM-DM traffic into a PIM-SM network, the PMBR notifies the RP that the PIM-DM network exists. The PMBR forwards PIM-DM multicast packets to the RP, which in turn forwards the packets to those routers that have joined the multicast group.
The PMBR also forwards PIM-SM traffic to a PIM-DM network. The PMBR sends a join message to the RP and the PMBR floods traffic from the RP into the PIM-DM network.

No commands are needed to enable PIM mode interoperation. PIM mode translation is automatically enabled when a dense mode interface and a sparse mode interface are enabled on the same switch.
clear igmp group

clear igmp group {vlan <vlan name>}

Description
Removes one or all IGMP groups.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command can be used by network operations to manually remove IGMP group entries instantly. It deletes the layer 3 IGMP group entries while leaving IGMP entries at layer 2 unaffected: that is, IGMP snooping entries will still be present in the switch.

Example
The following command clears IGMP groups from VLAN accounting:

```plaintext
clear igmp group accounting
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
clear igmp snooping

    clear igmp snooping {vlan <vlan name>}

Description
Removes one or all IGMP snooping entries.

Syntax Description

<table>
<thead>
<tr>
<th><em>vlan name</em></th>
<th>Specifies a VLAN name.</th>
</tr>
</thead>
</table>

Default
N/A.

Usage Guidelines
This command can be used by network operations to manually remove IGMP snooping entries instantly. However, removing an IGMP snooping entry can disrupt the normal forwarding of multicast traffic.

The static IGMP snooping entries will not be removed. The dynamic IGMP snooping entries will be removed, then re-created upon the next general queries.

Example
The following command clears IGMP snooping from VLAN accounting:

clear igmp snooping accounting

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
clear ipmc cache

    clear ipmc cache {<IP multicast group> {<source IP address>/<netmask>}}

Description
Resets the IP multicast cache table.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP multicast group</td>
<td>Specifies a group address.</td>
</tr>
<tr>
<td>source IP address</td>
<td>Specifies a source IP address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
If no options are specified, all IP multicast cache entries are flushed.

Usage Guidelines
This command can be used by network operators to manually remove IP multicast software and hardware forwarding cache entries instantly. If the source is available, caches will be re-created, otherwise caches are removed permanently. This command can disrupt the normal forwarding of multicast traffic.

Example
The following command resets the IP multicast table for group 224.1.2.3:

```
clear ipmc cache 224.1.2.3
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
clear ipmc fdb

clear ipmc fdb {group <ip address> {sender <ip address> / <netmask>}}

Description
Resets the IP multicast forwarding database entry.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a netmask.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If no options are specified, all IP multicast forwarding database entries are cleared. This command has an effect similar to the command `clear ipmc cache`, except that the targets are the forwarding database entries.

Example
The following command resets the IP multicast forwarding database entry:

```
clear ipmc fdb group 224.1.2.3 sender 10.0.0.2/24
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure dvmrp add vlan

configure dvmrp add vlan [<vlan name> | all]

Description
Enables DVMRP on one or all IP interfaces.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
If all is specified, DVMRP is enabled on all IP interfaces. When an IP interface is created, DVMRP is disabled by default.

Example
The following command enables DVMRP on the VLAN accounting:

```
class dvmrp add vlan accounting
```

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on the “i” series of switches only.
configure dvmrp delete vlan

configure dvmrp delete vlan [<vlan name> | all]

Description
Disables DVMRP on one or all IP interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
If all is specified, DVMRP is disabled on all IP interfaces.

Example
The following command disables DVMRP on the VLAN accounting:
configure dvmrp delete vlan accounting

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on the “i” series of switches only.
configure dvmrp timer

configure dvmrp timer <route-report-interval> <route-replacement-time>

Description

Configures the global DVMRP timers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-report-interval</td>
<td>Specifies the time in seconds between transmission of periodic report packets.</td>
</tr>
<tr>
<td>route-replacement-time</td>
<td>Specifies a time in seconds before a route becomes unreachable.</td>
</tr>
</tbody>
</table>

Default

- route-report-interval default—60 seconds.
- route-replacement-time default—140 seconds.

Usage Guidelines

Specify the following:

- route-report-interval—The amount of time the system waits between transmitting periodic route report packets. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 60 seconds. Because triggered update is always enabled, the route report will always be transmitted prior to the expiration of the route report interval.

- route-replacement-time—The route expiration time, commonly called route timeout. Initially it is 2 × route-report-interval +20 (2 × 60 + 20 = 140). It is the time for a particular DVMRP route to expire, while the route hold-down time is initially 2 × route-report-interval (2 × 60 = 120) which is the time before a route gets removed from advertisement after it has been expired. The range is 1 to 2,147,483,647 seconds (68 years).

Example

The following command configures the DVMRP timers:

```
cfg dvmrp timer 300 620
```

History

This command was available in ExtremeWare 2.0.

Platform Availability

This command is available on the “i” series of switches only.
configure dvmrp vlan cost

    configure dvmrp vlan [<vlan name> | all] cost <cost>

**Description**
Configures the cost (metric) of the interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>cost</td>
<td>Specifies a cost metric.</td>
</tr>
</tbody>
</table>

**Default**
The default setting is 1.

**Usage Guidelines**
The cost range is 1 - 32.

**Example**
The following command configures the cost (metric) of the interface on the VLAN accounting:

```
configure dvmrp vlan accounting cost 5
```

**History**
This command was available in ExtremeWare 4.0.

**Platform Availability**
This command is available on the “i” series of switches only.
configure dvmrp vlan export-filter

configure dvmrp vlan [<vlan name> | all] export-filter [<access profile> | none]

Description
Configures DVMRP to filter out certain routes when performing the route advertisement.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Deletes any associated filter.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to filter out certain routes when performing the route advertisement. The filtered routes are specified in an access profile.

Example
The following command configures DVMRP to filter out routes according to the nosales access profile:

```
configure dvmrp vlan accounting export-filter nosales
```

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on the “i” series of switches only.
configure dvmrp vlan import-filter

configure dvmrp vlan [<vlan name> | all] import-filter [<access profile> | none]

**Description**

Configures DVMRP to filter certain routes received from its neighbor, and uses an access profile to determine which DVMRP routes are accepted as valid routes.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Deletes any associated filter.</td>
</tr>
</tbody>
</table>

**Default**

None.

**Usage Guidelines**

Use this command to filter out certain routes when accepting routes from its neighbors. The filtered routes are specified in an access profile.

**Example**

The following command configures DVMRP to use the `nosales` access profile to determine which DVMRP routes are to accept:

```bash
configure dvmrp vlan accounting import-filter nosales
```

**History**

This command was first available in ExtremeWare 4.0.

**Platform Availability**

This command is available on the “i” series of switches only.
configure dvmrp vlan timer

configure dvmrp vlan <vlan name> timer <probe interval> <neighbor timeout>

Description
Configures DVMRP interface timers.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>probe interval</td>
<td>Specifies the time in seconds between probe messages.</td>
</tr>
<tr>
<td>neighbor timeout</td>
<td>Specifies the time in seconds before a neighbor router is declared to be down.</td>
</tr>
</tbody>
</table>

Default
The probe interval default setting is 10 seconds. The neighbor timeout default setting is 35 seconds.

Usage Guidelines
Specify the following:

- probe interval—The amount of time that the system waits between transmitting DVMRP probe messages. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 10 seconds.

- neighbor timeout—The amount of time before a DVMRP neighbor router is declared to be down. The range is 1 to 2,147,483,647 seconds (68 years). The default setting is 35 seconds (3.5 * probe interval).

Example
The following command configures the DVMRP timers:

```
configure dvmrp vlan accounting timer 3000 9000
```

History
This command was first available in ExtremeWare 6.2.

Platform Availability
This command is available on the “i” series of switches only.
configure dvmrp vlan trusted-gateway

configure dvmrp vlan [<vlan name> | all] trusted-gateway [<access profile> | none]

Description
Configures DVMRP to use the access policy to determine which DVMRP neighbor is trusted and to receive routes from.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that all neighbors are trusted (no neighbors are compared to an access profile).</td>
</tr>
</tbody>
</table>

Default
None (all neighbors are trusted).

Usage Guidelines
Use this command to specify trusted versus non-trusted neighbors.

Example
The following command configures DVMRP to use the nosales access profile to determine which DVMRP neighbor is trusted and to receive routes from:

```
configure dvmrp vlan accounting trusted-gateway nosales
```

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on the “i” series of switches only.
configure ext-mcast loopback-port

    configure ext-mcast loopback-port <portid> [vlan <vlanid>]

Description
Creates an internal VLAN and associates the port ID to the loopback port.

Syntax Description

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portid</td>
<td>Specifies a port using the display string configured for the port.</td>
</tr>
<tr>
<td>vlanid</td>
<td>Specifies a unique loopback VLAN tag.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to extend the layer 3 multicast capability to create more than 512 copies (up to a maximum of 1023 copies) for a multicast stream. When this feature is not enabled, only 512 copies are possible for any multicast stream.

Example
The following command configures an internal VLAN on port 4:
configure ext-mcast loopback-port 4 vlan 1

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” series of switches only.
configure igmp

configure igmp <query interval> <query response interval> <last member query interval>

Description
Configures the Internet Group Management Protocol (IGMP) timers.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>query interval</td>
<td>Specifies the interval (in seconds) between general queries.</td>
</tr>
<tr>
<td>query response interval</td>
<td>Specifies the maximum query response time (in seconds).</td>
</tr>
<tr>
<td>last member query interval</td>
<td>Specifies the maximum group-specific query response time (in seconds).</td>
</tr>
</tbody>
</table>

Default
- query interval—125 seconds
- query response interval—10 seconds
- last member query interval—1 second

Usage Guidelines
Timers are based on RFC2236. Specify the following:
- query interval—The amount of time, in seconds, the system waits between sending out general queries. The range is 1 to 429,496,729 seconds.
- query response interval—The maximum response time inserted into the periodic general queries. The range is 1 to 25 seconds.
- last member query interval—The maximum response time inserted into a group-specific query sent in response to a leave group message. The range is 1 to 25 seconds.

Example
The following command configures the IGMP timers:
configure igmp 100 5 1

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure igmp snooping add static group

configure igmp snooping vlan <vlan name> ports <portlist> add static group <ip address>

Description
Configures VLAN ports to receive the traffic from a multicast group, even if no IGMP joins have been received on the port.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the multicast group IP address.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines

Use this command to forward a particular multicast group to VLAN ports. In effect, this command emulates a host on the port that has joined the multicast group. As long as the port is configured with the static entry, multicast traffic for that multicast group will be forwarded to that port.

The switch sends proxy IGMP messages in place of those generated by a real host. The proxy messages use the VLAN IP address for source address of the messages. If the VLAN has no IP address assigned, the proxy IGMP message will use 0.0.0.0 as the source IP address.

The multicast group should be in the class-D multicast address space, but should not be in the multicast control subnet range (224.0.0.x/24).

If the ports also have an IGMP filter configured, the filter entries take precedence. IGMP filters are configured using the command:

configure igmp snooping vlan <vlan name> ports <portlist> filter <access profile>

Example

The following command configures a static IGMP entry so the multicast group 224.34.15.37 will be forwarded to VLAN marketing on ports 2:1-2:4:

configure igmp snooping vlan marketing ports 2:1-2:4 add static group 224.34.15.37

History

This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

**Platform Availability**

This command is available on all platforms.
configure igmp snooping add static router

configure igmp snooping {vlan <vlan name>} {ports <portlist>} add static router

Description
Configures VLAN ports to forward the traffic from all multicast groups, even if no IGMP joins have been received on the port.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to forward all multicast groups to the specified VLAN ports. In effect, this command emulates a multicast router attached to those ports. As long as the ports are configured with the static entry, all available multicast traffic will be forwarded to those ports.

Example
The following command configures a static IGMP entry so all multicast groups will be forwarded to VLAN marketing on ports 2:1-2:4:

```
configure igmp snooping vlan marketing ports 2:1-2:4 add static router
```

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure igmp snooping delete static group

configure igmp snooping vlan <vlan name> ports <portlist> delete static group [<ip address> | all]

Description
Removes the port configuration that causes multicast group traffic to be forwarded, even if no IGMP leaves have been received on the port.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the multicast group IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Delete all the static groups.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to remove an entry created by the following command:

configure igmp snooping vlan <vlan name> ports <portlist> add static group <group address>

Example
The following command removes a static IGMP entry that forwards the multicast group 224.34.15.37 to the VLAN marketing on ports 2:1-2:4:

configure igmp snooping vlan marketing ports 2:1-2:4 delete static group 224.34.15.37

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure igmp snooping delete static router

configure igmp snooping vlan <vlan name> ports <portlist> delete static router

Description
Removes the configuration that causes VLAN ports to forward the traffic from all multicast groups, even if no IGMP joins have been received on the port.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to remove the static IGMP entry created with the following command:

```
configure igmp snooping vlan <vlan name> ports <portlist> add static router
```

Example
The following command removes the static IGMP entry that caused all multicast groups to be forwarded to VLAN `marketing` on ports 2:1-2:4:

```
configure igmp snooping vlan marketing ports 2:1-2:4 delete static router
```

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure igmp snooping filter

configure igmp snooping vlan <vlan name> ports <portlist> filter [<access profile> | none]

Description
Configures an IGMP snooping access profile filter on VLAN ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile for the ports.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies not to use an access profile for the ports.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to filter multicast groups to the specified VLAN ports.

The access profile specified in this command must only include IP address type entries, and the IP addresses included in the entries must be in the class-D multicast address space, but should not be in the multicast control subnet range (224.0.0.x/24).

To remove IGMP snooping filtering from a port, use the none keyword version of the command.

Example
The following command configures the access profile ap_multicast to filter multicast packets forwarded to VLAN marketing on ports 2:1-2:4:
```
configure igmp snooping vlan marketing ports 2:1-2:4 filter ap_multicast
```

History
This command was first available in ExtremeWare 7.1.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure igmp snooping flood-list

configure igmp snooping flood-list [access profile | none]

Description
Configures certain multicast addresses to be slow path flooded within the VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>access profile</th>
<th>Specifies an access profile with a list of multicast addresses to be handled. The access profile must be type IP address.</th>
</tr>
</thead>
<tbody>
<tr>
<td>none</td>
<td>Specifies no access profile is to be used.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
With this command, a user can configure certain multicast addresses to be slow path flooded within the VLAN, which otherwise will be fast path forwarded according to IGMP and/or layer 3 multicast protocol.

The specified access profile `<access_profile>` should contain a list of addresses which will determine if certain multicast streams are to be treated specially. Typically, if the switch receives a stream with destination address which is in the `<access_profile>` in 'permit' mode, that stream will be software flooded and no hardware entry would be installed.

The specified access profile must be type IP address.

When adding an IP address into the access-profile, a 32-bit host address is recommended.

This feature is meant to solve the multicast connectivity problem for unknown destination addresses within system reserved ranges. Specifically this feature was introduced to solve the problem of recognizing certain stream as control packets.

NOTE
The switch will not validate any IP address in the access profile used in this command. Therefore, slow-path flooding should be used only for streams which are very infrequent, such as control packets. It should not be used for multicast data packets. This option overrides any default mechanism of hardware forwarding (with respect to IGMP, PIM, or DVMRP) so it should be used with caution.

Slow path flooding will be done within the L2 VLAN only.

Use the `none` option to effectively disable slow path flooding.

You can use the `show ipconfig` command to see the configuration of slow path flooding. It will be listed in the IGMP snooping section of the display.
Example
Given access profile *access1* created as follows:

```plaintext
create access-profile access1 type ipaddress
configure access-profile access1 add ipaddress 224.1.0.1/32
```

The following command configures the multicast data stream specified in *access1* for slow path flooding:

```plaintext
configure igmp snooping flood-list access1
```

The following command specifies that no access profile is to be used, this effectively disabling slow path flooding:

```plaintext
configure igmp snooping flood-list none
```

History
This command was first available in ExtremeWare 6.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure igmp snooping leave-timeout

    configure igmp snooping leave-timeout <leave_time ms>

Description
Configures the IGMP snooping leave timeout.

Syntax Description

| leave_time ms | Specifies an IGMP leave timeout value in milliseconds. |

Default
1000 ms.

Usage Guidelines
The range is 0 - 10000 ms (10 seconds). For timeout values of one second or less, you must set the leave-timeout to a multiple of 100 ms. For values of more than one second, you must set the leave-timeout to a multiple of 1000 ms (one second).

The specified time is the maximum leave timeout value. The switch could leave sooner if an IGMP leave message is received before the timeout occurs.

Example
The following command configures the IGMP snooping leave timeout:

    configure igmp snooping leave-timeout 10000

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure igmp snooping timer

configure igmp snooping timer <router timeout> <host timeout>

Description
Configures the IGMP snooping timers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>router timeout</td>
<td>Specifies the time in seconds between router discovery. Default is 260</td>
</tr>
<tr>
<td>host timeout</td>
<td>seconds.</td>
</tr>
</tbody>
</table>

Default

- router timeout default—260 seconds
- host timeout default—260 seconds

Usage Guidelines

Timers should be set to approximately 2.5 times the router query interval in use on the network. Specify the following:

- router timeout—The interval, in seconds, between the last time the router was discovered and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds.
- host timeout—The interval, in seconds, between the last IGMP group report message from the host and the current time. The range is 10 to 2,147,483,647 seconds (68 years). The default setting is 260 seconds.

IGMP snooping is a layer 2 function of the switch. It does not require multicast routing to be enabled. The feature reduces the flooding of IP multicast traffic. IGMP snooping optimizes the usage of network bandwidth and prevents multicast traffic from being flooded to parts of the network that do not need it. The switch does not reduce any IP multicast traffic in the local multicast domain (224.0.0.x).

IGMP snooping is enabled by default on the switch. If you are using multicast routing, IGMP snooping can be enabled or disabled (in versions of ExtremeWare previous to 7.0.0, IGMP snooping must have been enabled for multicast routing). If IGMP snooping is disabled, all IGMP and IP multicast traffic floods within a given VLAN. IGMP snooping expects at least one device on every VLAN to periodically generate IGMP query messages. Without an IGMP querier, the switch eventually stops forwarding IP multicast packets to any port, because the IGMP snooping entries will time out, based on the value specified in host timeout. An optional optimization for IGMP snooping is the strict recognition of routers only if the remote devices are running a multicast protocol.

Example
The following command configures the IGMP snooping timers:

configure igmp snooping timer 600 600
History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure mcast-queue-mgmt

    configure mcast-queue-mgmt start-queue <0-7> end-queue <0-7>

Description
This command configures a range of queues per port for multicast queue management.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0-7</td>
<td>Specifies the number of queues per port that are used in a round-robin based system of load balancing multicast queues.</td>
</tr>
</tbody>
</table>

Default
All queues (0-7)

Usage Guidelines
Use this command to configure more than a single queue for multicast stream forwarding. This feature is useful in high bandwidth multicast stream video deployments, where multiple streams are converging on a single egress port. By using multiple queues per port, the queues are load balanced.

Example
The following command configures eight queues per port for multicast queue management:

    configure mcast-queue-mgmt start-queue 0 end-queue 7

History
This command was available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” series of switches only.
configure mroute add

configure mroute add <source>/<mask> {<protocol>} <rpf-address> {<distance>}

Description
Adds a static multicast route to the static multicast routing table.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Specifies the IP address of the multicast source or RP.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies the mask of the IP address of the multicast source or RP.</td>
</tr>
<tr>
<td>protocol</td>
<td>(Optional) Specifies the unicast routing protocol that will be used. The source address will be compared with only those routes that have been learned from the specified unicast routing protocol.</td>
</tr>
<tr>
<td>rpf-address</td>
<td>Specifies the next hop (address) through which the source can be reached.</td>
</tr>
<tr>
<td>distance</td>
<td>(Optional) Specifies the distance metric that will be used to compare with the route that would be obtained from the unicast routing table. The route preference is greater for the route with the lower distance value. If this static multicast route has the same distance as that of the route obtained from the unicast route table, the static multicast route will be preferred. If the value for this argument is not specified, the default value of 0 (highest preference) is assumed.</td>
</tr>
</tbody>
</table>

Default
The default distance value is 0 (zero).

Usage Guidelines
None.

Example
The following command adds a static multicast route, specifying that the OSPF routing protocol will be used:

```
configure mroute add 100.10.0.0/16 ospf 20.10.0.1 2
```

History
This command was first available in ExtremeWare 7.3.0

Platform Availability
This command is available on all platforms.
configure mroute delete

configure mroute delete <source>/<mask> {<protocol>} <rpf-address> {<distance>}

Description
Deletes a static multicast route from the static multicast routing table.

Syntax Description

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>source</td>
<td>Specifies the IP address of the multicast source or RP.</td>
</tr>
<tr>
<td>mask</td>
<td>Specifies the mask of the IP address of the multicast source or RP.</td>
</tr>
<tr>
<td>protocol</td>
<td>(Optional) Specifies the unicast routing protocol that will be used. The source address will be compared with only those routes that have been learned from the specified unicast routing protocol.</td>
</tr>
<tr>
<td>rpf-address</td>
<td>Specifies the next hop (address) through which the source can be reached.</td>
</tr>
<tr>
<td>distance</td>
<td>(Optional) Specifies the distance metric that will be used to compare with the route that would be obtained from the unicast routing table. The route preference is greater for the route with the lower distance value. If this static multicast route has the same distance as that of the route obtained from the unicast route table, the static multicast route will be preferred. If the value for this argument is not specified, the default value of 0 (highest preference) is assumed.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None.

Example
The following command deletes a static multicast route from the static multicast routing table:

```
configure mroute delete 100.10.0.0/16
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on all platforms.
**configure pim add vlan**

For the “i” series of switches:

```
configure pim add vlan [<vlan name> | all] {dense | sparse}
```

For the “e” series of switches:

```
configure pim add {vlan} [<vlan name>] {passive}
```

**Description**

Enables PIM on one or more IP interfaces.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>dense</td>
<td>Specifies PIM dense mode (PIM-DM).</td>
</tr>
<tr>
<td>passive</td>
<td>Specifies the IP interface as passive.</td>
</tr>
<tr>
<td>sparse</td>
<td>Specifies PIM sparse mode (PIM-SM).</td>
</tr>
</tbody>
</table>

**Default**

Dense.

**Usage Guidelines**

When an IP interface is created, per-interface PIM configuration is disabled by default.

**On the “i” Series of Switches.** The switch supports both dense mode and sparse mode operation. You can configure dense mode or sparse mode on a per-interface basis. After they are enabled, some interfaces can run dense mode, while others run sparse mode.

**On the “e” Series of Switches.** The switch supports edge mode operation. You can configure sparse-mode on a per-interface basis. If you specify passive, the interface does not act as a neighbor with another PIM router or switch. Typically all non-passive interfaces align with USPF non-passive interfaces. A maximum of 2 non-passive PIM interfaces is allowed on the “e” series.

**Example**

The following command enables PIM-DM multicast routing on VLAN *accounting*:

```
configure pim add vlan accounting dense
```
History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure pim cbsr

configure pim cbsr [vlan <vlan name> {<priority [0-254]> | none}]

Description
Configures a candidate bootstrap router (BSR) for PIM sparse-mode operation.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a priority setting. The range is 0 - 254.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies to delete a CBSR.</td>
</tr>
</tbody>
</table>

Default
The default setting for priority is 0, and indicates the lowest priority.

Usage Guidelines
The VLAN specified for the candidate BSR must have IPMC forwarding enabled for PIM sparse mode. On the “e” series of switches, an error message is displayed if you attempt to configure a VLAN as a candidate BSR.

Example
The following command configures a candidate bootstrap router on the VLAN accounting:

```
configure pim cbsr vlan accounting 30
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on all platforms.
configure pim crp static

configure pim crp static <rp address> [none | <access profile>] {<priority [0-254]>}

Description
Configures a candidate rendezvous point (RP) and its associated groups statically, for PIM sparse mode operation.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>rp address</td>
<td>Specifies a rendezvous point address.</td>
</tr>
<tr>
<td>none</td>
<td>Deletes the static rendezvous point.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a priority setting. The range is 0 - 254, with 0 indicating the highest priority and 254 indicating the lowest priority.</td>
</tr>
</tbody>
</table>

Default
The default setting for priority is 0, which indicates highest priority. (A priority setting of 254 indicates the lowest priority.)

Usage Guidelines
Using PIM-SM, the router sends a join message to the rendezvous point (RP). The RP is a central multicast router that is responsible for receiving and distributing multicast packets. If you use a static RP, all switches in your network must be configured with the same RP address for the same group (range).

The access profile contains a list of multicast group accesses served by this RP.

On the “e” Series of Switches. The RP address cannot be any locally configured IP interface. The series “e” switches are not eligible to be RPs.

Example
The following command statically configures an RP and its associated groups defined in access profile rp-list:

classic pim crp static 10.0.3.1 rp-list

History
This command was first available in ExtremeWare 6.1.5.
This command was added to the Summit “e” series of switches in ExtremeWare 71e.

Platform Availability
This command is available on all platforms.
configure pim crp timer

    configure pim crp timer <crp advertisement interval>

**Description**

Configures the candidate rendezvous point advertising interval for PIM sparse mode operation.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>crp advertisement interval</td>
<td>Specifies a candidate rendezvous point advertising interval in seconds. The valid range is 1 to 1717986918.</td>
</tr>
</tbody>
</table>

**Default**

The default is 60 seconds.

**Usage Guidelines**

None.

**Example**

The following command configures the candidate rendezvous point advertising interval to 120 seconds:

```
configure pim crp timer 120
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on all platforms.
configure pim crp vlan access profile

    configure pim crp vlan <vlan name> [none | <access profile>] {<priority>}

**Description**
Configures the dynamic candidate rendezvous point for PIM sparse-mode operation.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no access profile.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies a priority setting. The range is 0 - 254.</td>
</tr>
</tbody>
</table>

**Default**
The default setting is for priority is 0 and indicates the highest priority.

**Usage Guidelines**
The access profile contains the list of multicast group accesses serviced by this RP. To delete a CRP, use the keyword none as the access policy.

The VLAN specified for CRP must have IPMC forwarding enabled for PIM sparse mode.

**Example**
The following command configures the candidate rendezvous point for PIM sparse-mode operation on the VLAN *HQ_10_0_3* with the access profile *rp-list* and priority set to 30:

configure pim crp HQ_10_0_3 rp-list 30

**History**
This command was available in ExtremeWare 6.2.

**Platform Availability**
This command is available on all platforms.
configure pim delete vlan

configure pim delete vlan [<vlan name> | all]

Description
Disables PIM on one or more interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command would disable PIM-SM on an “e” series switch (or PIM-DM or PIM-SM for an “i” series switch) for the VLAN accounting:

configure pim delete vlan accounting

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure pim register-checksum-to

    configure pim register-checksum-to [include-data | exclude-data]

Description
Configures the checksum computation to either include data (for compatibility with Cisco Systems products) or to exclude data (for RFC-compliant operation), in the register message.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>include-data</td>
<td>Specifies to include data.</td>
</tr>
<tr>
<td>exclude-data</td>
<td>Specifies to exclude data.</td>
</tr>
</tbody>
</table>

Default
Include data

Usage Guidelines
None.

Example
The following command configures the checksum mode to include data for compatibility with Cisco Systems products:

```sh
configure pim register-checksum-to include-data
```

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure pim register-rate-limit-interval

    configure pim register-rate-limit-interval <time>

Description
Configures the initial PIM-SM periodic register rate.

Syntax Description

<table>
<thead>
<tr>
<th>time</th>
<th>Specifies an interval time in seconds. Range is 0 - 60. Default is 0.</th>
</tr>
</thead>
</table>

Default
Default is 0.

Usage Guidelines
Configuring a non-zero interval time can reduce the CPU load on the first hop in case register stop messages are not received normally.

If a non-zero value is configured, the first hop switch would send register messages only at time second intervals. The default value is zero, which sends continuous register messages. This command takes effect only until the register stop message is not received, in other words, when the register suppression timer is not running.

Example
The following command configures the initial PIM register rate limit interval:

    configure pim register-rate-limit-interval 2

History
This command was first available in ExtremeWare 6.2.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure pim register-suppress-interval
register-probe-interval

configure pim register-suppress-interval <time> register-probe-interval <time>

Description
Configures an interval for periodically sending null-registers.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>register-suppress-interval &lt;time&gt;</td>
<td>Specifies an interval time in seconds. Range is 30 - 200 seconds. Default is 60.</td>
</tr>
<tr>
<td>register-probe-interval &lt;time&gt;</td>
<td>Specifies an interval time in seconds. Default is 5.</td>
</tr>
</tbody>
</table>

Default
- register-suppress-interval—60
- register-probe-interval—5

Usage Guidelines
The register-probe-interval time should be set less than the register-suppress-interval time. By default, a null register is sent every 55 seconds \( (\text{register-suppress-interval} - \text{register-probe-interval}) \). A response to the null register is expected within register probe interval. By specifying a larger interval, a CPU peak load can be avoided because the null-registers are generated less frequently. The register probe time should be less than half of the register suppress time, for best results.

Example
The following command configures the register suppress interval and register probe time:
configure pim register-suppress-interval 90 register-probe time 10

History
This command was first available in ExtremeWare 6.2.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
configure pim spt-threshold

    configure pim spt-threshold <last hop router threshold> {<rp threshold>}

Description
Configures the threshold, in kbps, for switching to SPT. On leaf routers, this setting is based on data packets. On the RP, this setting is based on register packets.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>last hop router threshold</td>
<td>Specifies a last hop router threshold.</td>
</tr>
<tr>
<td>rp threshold</td>
<td>Specifies an RP threshold.</td>
</tr>
</tbody>
</table>

Default
The default setting is 0.

Usage Guidelines
For the best performance leveraged by hardware forwarding, use default value “0,0”, or small values below 16. From release 6.2.2 onwards, since the RP learns the source address from the register message, the RP threshold has no effect.

Example
The following command sets the threshold for switching to SPT:

configure pim spt-threshold 4 16

History
This command was first available in ExtremeWare 6.1.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure pim timer vlan

configure pim timer <hello interval> <join prune interval> vlan [<vlan name>]

Description
Configures the timers on one or more VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello interval</td>
<td>Specifies the amount of time before a hello message is sent out by the PIM router. The range is 1 to 65,519 seconds.</td>
</tr>
<tr>
<td>join prune interval</td>
<td>Specifies the join/prune interval. The range is 1 to 65,519 seconds.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
- hello interval—30 seconds.
- join prune interval—60 seconds.

Usage Guidelines
Use this command to configure one or more timers that are associated to each VLAN where PIM is enabled. If the VLAN name is not specified, the configuration is applied to all the VLANs on which PIM is enabled.

Example
The following command configures the global PIM timers on the VLAN accounting:

```bash
configure pim timer 150 300 vlan accounting
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
configure pim vlan trusted-gateway

configure pim vlan [<vlan name> | all] trusted-gateway [<access profile> | none]

Description
Configures a trusted neighbor policy.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>access profile</td>
<td>Specifies an access profile name.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no access profile, so all gateways are trusted.</td>
</tr>
</tbody>
</table>

Default
No access profile, so all gateways are trusted.

Usage Guidelines
Because PIM leverages the unicast routing capability that is already present in the switch, the access policy capabilities are, by nature, different. When the PIM protocol is used for routing IP multicast traffic, the switch can be configured to use an access profile to determine trusted PIM router neighbors for the VLAN on the switch running PIM.

You can use this feature to select or exclude routers as peers. PIM control packets from non-trusted sources are not processed.

Example
The following command configures a trusted neighbor policy on the VLAN backbone:

```
configure pim vlan backbone trusted-gateway nointernet
```

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable dvmrp

disable dvmrp
disable dvmrp
disable dvmrp

Description
Disables DVMRP on the system.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
None.

Example
The following command disables DVMRP on the system:

disable dvmrp

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on “i” series platforms only.
disable dvmrp rxmode vlan

    disable dvmrp rxmode vlan [<vlan name> | all]

Description
Disables the receive capability of DVMRP packets on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
None.

Example
The following command disables the receive capability of DVMRP packets on the VLAN accounting:

disable dvmrp rxmode vlan accounting

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on "i" series platforms only.
disable dvmrp txmode vlan

disable dvmrp txmode vlan [vlan <vlan name> | all]

**Description**
Disables the transmit capability of DVMRP packets on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**
Enabled

**Usage Guidelines**
None.

**Example**
The following command disables the transmit capability of DVMRP packets on the VLAN `accounting`:

disable dvmrp txmode vlan accounting

**History**
This command was first available in ExtremeWare 6.1.

**Platform Availability**
This command is available on “i” series platforms only.
disable ext-mcast

disable ext-mcast

Description
Disables the multicast copy count extension feature.

Syntax Description
This command has no options or parameters.

Default
Disabled

Usage Guidelines
Use this command to disable the multicast copy count extension feature. When this feature is disabled, the switch can generate a maximum of 512 copies for a multicast stream.

Example
The following example resets multicast copy count extension to a single FDB entry:

disable ext-mcast

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” series of switches only.
disable igmp

disable igmp {vlan <vlan name>}

Description
Disables IGMP on a router interface. If no VLAN is specified, IGMP is disabled on all router interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled.

Usage Guidelines
IGMP is a protocol used by an IP host to register its IP multicast group membership with a router. Periodically, the router queries the multicast group to see if the group is still in use. If the group is still active, hosts respond to the query, and group registration is maintained.

IGMP is enabled by default on the switch. However, the switch can be configured to disable the generation and processing of IGMP packets. IGMP should be enabled when the switch is configured to perform IP unicast or IP multicast routing. IGMP must be enabled if the switch is configured for DVMRP.

Example
The following command disables IGMP on VLAN accounting:

disable igmp vlan accounting

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable igmp snooping

disable igmp snooping {forward-mcrouter-only | hardware-flooding | vlan <vlan name>}

**Description**
Disables IGMP snooping.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-mcrouter-only</td>
<td>Specifies that the switch forwards all multicast traffic to the multicast router only.</td>
</tr>
<tr>
<td>hardware-flooding</td>
<td>Disables IGMP snooping in the hardware and allows multicast IP traffic to be flooded in hardware.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN.</td>
</tr>
</tbody>
</table>

**Default**
Enabled.

**Usage Guidelines**

If a VLAN is specified, IGMP snooping is disabled only on that VLAN, otherwise IGMP snooping is disabled on all VLANs.

If the switch is in the forward-mcrouter-only mode, then the command disable igmp snooping forward-mcrouter-only changes the mode so that all multicast traffic is forwarded to any IP router. If not in the forward-mcrouter-mode, the command disable igmp snooping forward-mcrouter-only has no effect.

Without the hardware-flooding keyword, this command disables IGMP snooping only in software. Multicast packets with unicast IP addresses are sent using slow path forwarding and are flooded using slow path forwarding. This can load the CPU with heavy multicast traffic. To operate the switch in Layer 2 mode and disable IGMP snooping, it is best to flood multicast IP traffic in hardware, using the hardware-flooding keyword.

When IGMP snooping is disabled with hardware-flooding, if you enable IGMP snooping for one or more VLANs, the hardware-flooding option is automatically turned off, and IGMP snooping is re-enabled.

To change the snooping mode you must disable IP multicast forwarding. Use the command:

disable ipmcforwarding

**Example**
The following command disables IGMP snooping on the VLAN accounting:

disable igmp snooping accounting

**History**
This command was first available in ExtremeWare 7.0.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
disable igmp snooping with-proxy

disable igmp snooping with-proxy

Description
Disables the IGMP snooping proxy. The feature is enabled by default.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
This command can be used for troubleshooting purpose. It should be enabled for normal network operation.

Enabling the proxy allows the switch to suppress the duplicate join requests on a group to forward to the connected layer 3 switch. The proxy also suppresses unnecessary IGMP leave messages so that they are forwarded only when the last member leaves the group.

Example
The following command disables the IGMP snooping proxy:

disable igmp snooping with-proxy

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit "e" series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
disable ipmcfowarding

disable ipmcfowarding {vlan <vlan name>}

Description
Disables IP multicast forwarding on an IP interface.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Disabled.

Usage Guidelines
If no options are specified, all configured IP interfaces are affected. When new IP interfaces are added, IP multicast forwarding is disabled by default.

IP forwarding must be enabled before enabling IP multicast forwarding, and IP multicast forwarding must be disabled before disabling IP forwarding.

Disabling IP multicast forwarding disables any layer 3 forwarding for the streams coming to the interface.

Example
The following command disables IP multicast forwarding on the VLAN accounting:

disable ipmcfowarding vlan accounting

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable mcast-queue-mgmt

disable mcast-queue-mgmt

Description
Disables multicast queue management for multicast stream forwarding.

Syntax Description
This command has no options or parameters.

Default
Disabled

Usage Guidelines
Use this command to disable the queues configured for multicast forwarding using the configure mcast-queue-mgmt command. This command causes the switch to use a single queue per port for multicast forwarding. However, this change does not take effect while multicast forwarding entries exist for the stream.

Example
The following example disables multiple queues for multicast stream forwarding:

disable mcast-queue-mgmt

History
This command was available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” series of switches only.
disable pim

disable pim

Description
Disables PIM on the system.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
None.

Example
The following command disables PIM on the system:

disable pim

History
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
disable pim snooping

disable pim snooping {vlan <vlan name>}

Description
Disables PIM snooping on the selected VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of the VLAN on which to disable PIM snooping. If no VLAN name is specified, PIM snooping is disabled on all VLANs.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Use this command to disable PIM snooping for a selected VLAN. To disable PIM snooping on a single VLAN, specify the VLAN name. If no VLAN name is specified, PIM snooping is disabled on all VLANs.

Example
The following command disables PIM snooping on the VLAN demo-pim:

disable pim snooping vlan demo-pim

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms only.
enable dvmrp

enable dvmrp

Description
Enables DVMRP on the system.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
None

Example
The following command enables DVMRP on the system:
   enable dvmrp

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on “i” series platforms only.
enable dvmrp rxmode vlan

   enable dvmrp rxmode vlan [<vlan name> | all]

**Description**

Enables the receive capability of DVMRP packets on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

**Default**

Enabled

**Usage Guidelines**

None.

**Example**

The following command enables the receive capability of DVMRP packets on the VLAN `accounting`:

```
enable dvmrp rxmode vlan accounting
```

**History**

This command was first available in ExtremeWare 6.1.

**Platform Availability**

This command is available on "i" series platforms only.
enable dvmrp txmode vlan

enable dvmrp txmode vlan [vlan <vlan name> | all]

Description
Enables the transmit capability of DVMRP packets on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
None.

Example
The following command enables the transmit capability of DVMRP packets on the VLAN accounting:

```
enable dvmrp txmode vlan accounting
```

History
This command was first available in ExtremeWare 6.1.

Platform Availability
This command is available on “i” series platforms only.
enable ext-mcast

enable ext-mcast

Description
Enables the multicast copy count extension feature.

Syntax Description
This command has no options or parameters.

Default
Disabled

Usage Guidelines
Use this command to enable the multicast copy count extension feature. This feature extends the layer 3 multicast function to allow more than 512 copies, and up to 1023 copies, for a multicast stream. When this feature is not enabled, only 512 copies are possible for every multicast stream. Before enabling, the user must configure this feature using the configure ext-mcast loopback-port command.

Example
The following example enables the multicast copy count extension feature:

enable ext-mcast

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” series of switches only.
enable igmp

    enable igmp (vlan <vlan name>)

**Description**

Enables IGMP on a router interface. If no VLAN is specified, IGMP is enabled on all router interfaces.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

Enabled.

**Usage Guidelines**

IGMP is a protocol used by an IP host to register its IP multicast group membership with a router. Periodically, the router queries the multicast group to see if the group is still in use. If the group is still active, IP hosts respond to the query, and group registration is maintained.

IGMP is enabled by default on the switch. However, the switch can be configured to disable the generation and processing of IGMP packets. IGMP should be enabled when the switch is configured to perform IP unicast or IP multicast routing.

**Example**

The following command enables IGMP on the VLAN accounting:

```
enable igmp vlan accounting
```

**History**

This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**

This command is available on all platforms.
enable igmp snooping

    enable igmp snooping {forward-mcrouter-only | vlan <vlan name>}

Description
Enables IGMP snooping on the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>forward-mcrouter-only</td>
<td>Specifies that the switch forwards all multicast traffic to the multicast router only.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN.</td>
</tr>
</tbody>
</table>

Default
Enabled.

Usage Guidelines
If a VLAN is specified, IGMP snooping is enabled only on that VLAN, otherwise IGMP snooping is enabled on all VLANs.

Two IGMP snooping modes are supported:

- The `forward-mcrouter-only` mode forwards all multicast traffic to the multicast router (that is, the router running PIM or DVMRP).
- When not in the `forward-mcrouter-only` mode, the switch forwards all multicast traffic to any IP router (multicast or not).

To change the snooping mode you must disable IP multicast forwarding. To disable IP multicast forwarding, use the command:

```
disable ipmcforwarding
```

To change the IGMP snooping mode from the `forward-mcrouter-only` mode to the `non-forward-mcrouter-only` mode, use the command:

```
disable igmp snooping forward-mcrouter-only
```

The snooping mode is not changed from the `non-forward-mcrouter-only` mode to the `forward-mcrouter-only` mode solely by enabling that mode. You must disable IGMP snooping, then enable IGMP snooping for multicast only. Disable IP multicast forwarding, then use the following commands:

```
disable igmp snooping
enable igmp snooping forward-mcrouter-only
```

Example
The following command enables IGMP snooping on the switch:

```
enable igmp snooping
```
History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable igmp snooping with-proxy

Description
Enables the IGMP snooping proxy. The default setting is enabled.

Syntax Description
This command has no arguments or variables.

Default
Enabled.

Usage Guidelines
This command should be enabled for normal network operation. The command does not alter the snooping setting. IP multicast forwarding should be disabled globally for this command.

Enabling the proxy allows the switch to suppress the duplicate join requests on a group to forward to the connected layer 3 switch. The proxy also suppresses unnecessary IGMP leave messages so that they are forwarded only when the last member leaves the group.

Example
The following command enables the IGMP snooping proxy:

```
enable igmp snooping with-proxy
```

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
enable ipmcforwarding

    enable ipmcforwarding {vlan <vlan name>}

**Description**
Enables IP multicast forwarding on an IP interface.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
Disabled.

**Usage Guidelines**
If no options are specified, all configured IP interfaces are affected. When new IP interfaces are added, IPMC forwarding is disabled by default.

IP forwarding must be enabled before enabling IPMC forwarding, and IPMC forwarding must be disabled before disabling IP forwarding.

**Example**
The following command enables IPMC forwarding on the VLAN `accounting`:

```
enable ipmcforwarding vlan accounting
```

**History**
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable mcast-queue-mgmt

enable mcast-queue-mgmt

**Description**
Enables multicast queue management for multicast stream forwarding.

**Syntax Description**
This command has no options or parameters.

**Default**
Disabled

**Usage Guidelines**
Use this command to enable multiple queues for multicast stream forwarding. This command enables the queues configured using the `configure mcast-queue-mgmt` command.

**Example**
The following example enables multiple queues for multicast stream forwarding:

```plaintext
enable mcast-queue-mgmt
```

**History**
This command was available in ExtremeWare 7.4.

**Platform Availability**
This command is available on the “i” platforms only.
enable pim

enable pim

**Description**
Enables PIM on the system.

**Syntax Description**
This command has no arguments or variables.

**Default**
Disabled.

**Usage Guidelines**
None.

**Example**
The following command enables PIM on the system:
```
enable pim
```

**History**
This command was first available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

**Platform Availability**
This command is available on all platforms.
enable pim snooping

    enable pim snooping {vlan <vlan name>}

Description
Enables PIM snooping for a selected VLAN.

Syntax Description

| vlan name | \(\text{Specifies the name of the VLAN on which to enable PIM snooping. If no VLAN name is specified, PIM snooping is enabled on all VLANs.}\) |

Default
Disabled.

Usage Guidelines
Use this command to enable PIM snooping for a selected VLAN. To enable PIM snooping on a single VLAN, specify the VLAN name. If no VLAN name is specified, PIM snooping is enabled on all VLANs.

Example
The following command enables PIM snooping on the VLAN demo-pim:

```
enable pim snooping vlan demo-pim
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms only.
mrinfo

mrinfo <ip address> {from <ip address>} {timeout <seconds>}

Description
Initiates a request to get multicast information from a router.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip address&gt;</td>
<td>Specifies an IP address. The first &lt;ip address&gt; parameter specifies the unicast IP address of the router to query.</td>
</tr>
<tr>
<td>from</td>
<td>Specifies the unicast address of an interface in the system to use as the source address in the request.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the time to wait before indicating a failure.</td>
</tr>
</tbody>
</table>

Defaults
- from—outgoing interface
- timeout—three seconds

Usage Guidelines
This command queries a multicast router for information useful for tracing and troubleshooting. The command returns the following information:

- code version
- system multicast information
- interface information
  - interface IP address
  - interface multicast capabilities
  - metric configured on the interface
  - threshold configured on the interface
  - count and IP address of the neighbors discovered on the interface

Example
The following command queries the router at 10.10.34.14:

mrinfo 10.10.34.14

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.
Platform Availability

This command is available on all platforms.
mtrace

mtrace source <ip address> {destination <ip address>} {group <ip address>} {from <ip address>} {gateway <ip address>} {timeout <seconds>} {maximum-hops <number>}

Description

Initiates a request to trace the path of multicast traffic from the source to the destination of a multicast group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;ip address&gt;</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>source</td>
<td>Specifies the unicast address of the multicast source.</td>
</tr>
<tr>
<td>destination</td>
<td>Specifies the unicast address of the destination to which the path of the multicast traffic will be traced.</td>
</tr>
<tr>
<td>group</td>
<td>Specifies the multicast IP address of the group for which the traffic will be traced.</td>
</tr>
<tr>
<td>from</td>
<td>Specifies the unicast address of an interface in the system to use as the response address in the request.</td>
</tr>
<tr>
<td>gateway</td>
<td>Specifies the unicast address of a first hop router to which the query will be directed.</td>
</tr>
<tr>
<td>timeout</td>
<td>Specifies the time to wait before indicating a failure.</td>
</tr>
<tr>
<td>maximum-hops</td>
<td>Specifies the maximum number of hops the mtrace request can traverse.</td>
</tr>
</tbody>
</table>

Defaults

- destination—current system
- group—0.0.0.0
- from—outgoing interface to reach the source or destination
- gateway—destination 224.0.0.2
- timeout—three seconds
- maximum-hops—255

Usage Guidelines

This command relies on a feature of multicast routers that is accessed using the IGMP protocol. Since multicast uses reverse path forwarding, a multicast trace is run from the destination to the source. A query packet is sent to the last-hop multicast router. This router builds a trace response packet, fills in a report for its hop, and forwards the packet to the next upstream router. As the request is forwarded, each router in turn adds its own report to the trace response. When the request reaches the first-hop router, the filled in request is sent back to the system requesting the trace. The request will also be returned if the maximum hop limit is reached.

If a router does not support the mtrace functionality, it will silently drop the request packet and no information will be returned. For this situation, you would send the trace with a small number of maximum hops allowed, increasing the number of hops as the stream is traced.
The group IP address must be in the class-D multicast address space, but should not be in the multicast control subnet range (224.0.0.x/24).

ExtremeWare based systems do not maintain packet forwarded statistics for each source/group combination (S,G) and cannot return that information.

Example
The following command traces the multicast group 227.160.14.23 originating at 10.10.32.14 that is coming through the gateway at 172.16.255.1:

mtrace source 10.10.34.14 group 227.160.14.23 gateway 172.16.255.1 mtrace source 3.3.3.200 group 225.1.1.1 gateway 22.22.22.9

Output from the command is similar to:

Mtrace from 10.10.34.14 to 172.16.255.2 via group 227.160.14.23
mtrace_proc_resp: Src: 10.10.34.14, Dst: 172.16.255.2
  0   (172.16.255.2)
-1   (172.16.255.1)  PIM thresh^ 1      [10.10.34.14/32]
-2   (172.17.255.1)  PIM thresh^ 1      [10.10.34.14/32]
-3   (172.18.255.1)  PIM thresh^ 1      [10.10.34.14/32]
Round trip time 10 ms; total ttl of 4 required.

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
run ipmcfdb-check

run ipmcfdb-check [index <bucket> <entry> | <IP multicast group> <source IP address> vlan <vlan name>] {extended} {detail}

Description
Checks IP multicast FDB entries for consistency.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bucket</td>
<td>Specifies the bucket portion of the FDB hash index.</td>
</tr>
<tr>
<td>entry</td>
<td>Specifies the entry portion of the FDB hash index.</td>
</tr>
<tr>
<td>IP multicast group</td>
<td>Specifies a multicast group. FDB entries with this group will be checked.</td>
</tr>
<tr>
<td>source IP address</td>
<td>Specifies an IP source address.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name. FDB entries for this VLAN with the specified multicast group number will be checked.</td>
</tr>
<tr>
<td>extended</td>
<td>Enables OTP index checking in the MAC entry and VPST of the egress port.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies that more detailed debug information should be logged.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The FDB error checking function logs the error count into the system log. Use the detail option to log more detailed debug information.

Example
The following command runs a consistency check on the FDB entries for the IP multicast group 168.192.2.4:
run ipmcfdb-check 168.192.2.4 195.1.1.100 vlan lab1 extended detail

History
This command was first available in ExtremeWare 6.1.9.

Platform Availability
This command is available on “i” series platforms only.
show dvmrp

    show dvmrp {vlan <vlan name> | route {detail}}

Description
Displays the DVMRP configuration and statistics, or the unicast route table.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>route</td>
<td>Specifies a route.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
All.

Usage Guidelines
None.

Example
The following command displays the DVMRP configuration and statistics for the VLAN accounting:

    show dvmrp vlan accounting

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on “i” series platforms only.
show igmp group

    show igmp group {<ip address> {sender <ip address>}} {vlan <vlan name>}

Description
Lists the IGMP group membership for the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group &lt;ip address&gt;</td>
<td>Specifies a group IP address.</td>
</tr>
<tr>
<td>sender &lt;ip address&gt;</td>
<td>Specifies a sender's IP address.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If no VLAN is specified all VLANs are displayed. You can also filter the display by group address and by multicast stream sender address.

Example
The following command lists the IGMP group membership for the VLAN accounting:

```
show igmp group 10.0.0.1 sender 10.0.0.2 accounting
```

History
This command was first available in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show igmp snooping

    show igmp snooping {vlan <vlan name> | detail}

Description
Displays IGMP snooping registration information and a summary of all IGMP timers and states.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The two types of IGMP snooping entry are sender entry and subscribed entry.

The following information is displayed in a per-interface format:
- Group membership information
- Router entry
- Timeout information

Example
The following command displays IGMP snooping registration information on the VLAN accounting:

```
show igmp snooping vlan accounting
```

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show igmp snooping filter

  show igmp snooping {vlan <vlan name>} filter

Description
Displays IGMP snooping filters.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to display IGMP snooping filters configured on the specified VLAN. When no VLAN is specified, all the filters will be displayed.

Example
To display the IGMP snooping filter configured on VLAN vlan101, use the following command:

show igmp snooping vlan101 filter

The output of the command will be similar to the following:

VLAN vlan101 (4094)
Filter      Port
ap5              31    (-)
Total number of configured static filters = 1

Flags: (a) Active

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show igmp snooping static group

    show igmp snooping {vlan <vlan name>} static group

Description
Displays static IGMP snooping entries.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
None.

Usage Guidelines
Use this command to display IGMP snooping filters configured on the specified VLAN. When no VLAN is specified, all the filters will be displayed.

Example
To display the IGMP snooping static groups configured on VLAN `vlan101`, use the following command:

```
show igmp snooping vlan101 static group
```

The output of the command will be similar to the following:

```
VLAN vlan101 (4094)
  Group  Port  Flags
  239.1.1.2  29     s-
  239.1.1.2  30     s-
  239.1.1.2  31     sa
  239.1.1.2  32     s-
  239.1.1.2  34     s-
```

Total number of configured static IGMP groups = 5
Flags: (s) Static, (a) Active

History
This command was first available in ExtremeWare 7.1.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show ipmc cache

    show ipmc cache {detail} | {<IP multicast group> {<source IP address> <netmask>}}

Description
Displays the IP multicast forwarding cache.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
<tr>
<td>IP multicast group</td>
<td>Specifies an IP group address.</td>
</tr>
<tr>
<td>source IP address</td>
<td>Specifies an IP source address.</td>
</tr>
<tr>
<td>netmask</td>
<td>Specifies a subnet mask.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Displays the following information:
- IP group address
- IP source address / source mask
- Upstream neighbor (RPF neighbor)
- Interface (VLAN-port) to upstream neighbor
- Cache expiry time
- Routing protocol

When the detail option is specified, the switch displays the egress VLAN list and the pruned VLAN list.

Example
The following command displays the IP multicast table for group 224.1.2.3:
show ipmc cache 224.1.2.3

History
This command was available in ExtremeWare 2.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show ipmc fdb

   show ipmc fdb {<ip address>}

Description
Displays the IP multicast forwarding database in hardware.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ip address</td>
<td>Specifies an IP group address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
If the group address is specified, only the IP multicast FDB entries corresponding to the group address are displayed.

Example
The following command displays the IP multicast forwarding database:

show ipmc fdb

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show l2stats

    show l2stats {vlan <vlan name>}

Description
Displays the counters for the number of packets bridged, switched, and snooped.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
None.

Example
The following command displays the counters for the number of packets bridged, switched, and snooped for the VLAN accounting:
show l2stats accounting

History
This command was first available in ExtremeWare 6.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
show mcast-queue-mgmt

Description
Displays the current queue configuration for multicast data forwarding.

Syntax Description
This command has no options or parameters.

Default
N/A

Usage Guidelines
Use this command to display the current configuration being used for multicast data load balancing. This feature is configured using the `configure mcast-queue-mgmt` command.

Example
The following command displays the current configuration for the multicast queue management:

```
show mcast-queue-mgmt
```

Output from this command is similar to:

```
show mcast-queue-mgmt
Multicast Queue management : Enabled
Start Queue               : 0
End Queue                 : 7
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” platforms only.
show mroute

Description
Displays static multicast route configuration information.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
This command displays the static multicast table entries in the order defined with the configure mroute add command. The following fields are displayed in the command output:

SrcAddr : Specifies the IP Address of the multicast source or RP.
SrcMask : Specifies the mask of the IP Address of the multicast source or RP.
rpfNbr : Specifies the next-hop address (multicast neighbor address) through which the source could be reached.

The following flags are also displayed in the output:

U - Indicates that the interface through which the RPF neighbor could be reached is active.
m - Indicates that multicast is enabled on the interface through which the RPF neighbor could be reached.
G - Indicates that the RPF neighbor is the gateway for this route.

Metric : Metric for the route. If the metric was not specified during configuration of this route (using the configure mroute add command), the default value 0 would be displayed.

Proto : The protocol with which the route was configured using the configure mroute add command. If the protocol was not specified during the configuration of this route, ANY is displayed.

The asterisk "*" displayed along with each of the route indicates that the route is active. Otherwise, the route is considered inactive and is not used.

Example
The following command displays static multicast route configuration information:

show mroute

---------------------------------------------------------------------
<table>
<thead>
<tr>
<th>SrcAddr</th>
<th>SrcMask</th>
<th>rpfNbr</th>
<th>flags</th>
<th>metric</th>
<th>Proto</th>
</tr>
</thead>
</table>
---------------------------------------------------------------------
Given the following configuration:

```
configure mroute add 90.90.90.0/24 ospf 2.2.2.2
```

The following command displays mroute information for this configuration:

```
show mroute
```

Output for the command is similar to:

```
---------------------------------------------------
SrcAddr     SrcMask     rpfNbr  flags  metric  Proto
---------------------------------------------------
*90.90.90.0  255.255.255.0  2.2.2.2  UmG    0      OSPF
---------------------------------------------------
```

Flags: (U) Up, (m) Multicast, (G) Gateway, (*) Active routes

**History**

This command was first available in ExtremeWare 7.3.0.

**Platform Availability**

This command is available on “i” series platforms only.
show pim

show pim {detail | rp-set {<IP multicast group>}| vlan <vlan name>}

Description
Displays the PIM configuration and statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Specifies to display the detailed format.</td>
</tr>
<tr>
<td>IP multicast group</td>
<td>Specifies an IP multicast group.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
If no VLAN is specified, the configuration is displayed for all PIM interfaces.

If no multicast group is specified for the rp-set option (Rendezvous Point set), all groups are displayed.

Usage Guidelines
The detail version of this command displays the global statistics for PIM register and register-stop packets.

Example
The following command displays the PIM configuration and statistics for the VLAN accounting:
show pim accounting

History
This command was first available in ExtremeWare 4.0.

The rp-set option was added in ExtremeWare 6.1.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
show pim snooping

    show pim snooping {vlan <vlan name>}

Description
Displays PIM snooping information for a selected VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the name of the VLAN for which PIM snooping information will be displayed. If no VLAN name is specified, PIM snooping information will be displayed for all VLANs.</td>
</tr>
</tbody>
</table>

Default
If no VLAN name is specified, PIM snooping information is displayed for all VLANs.

Usage Guidelines
Use this command to display PIM snooping information for a selected VLAN. To display PIM snooping for a single VLAN, specify the VLAN name. If no VLAN name is specified, PIM snooping information is displayed for all VLANs.

Example
The following command displays PIM snooping on the VLAN demo-pim:
show pim snooping vlan demo-pim

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “i” series platforms only.
unconfigure dvmrp

    unconfigure dvmrp {vlan <vlan name>}

Description
Resets the DVMRP timers to their default settings.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
If no VLAN is specified, all interfaces are reset.

Usage Guidelines
None.

Example
The following command resets all DVMRP timers on VLAN accounting:
unconfigure dvmrp vlan accounting

History
This command was available in ExtremeWare 2.0.

Platform Availability
This command is available on “i” series platforms only.
unconfigure ext-mcast

unconfigure ext-mcast

Description
This command disables the multicast copy count extension feature.

Syntax Description
This command has no options or parameters.

Default
N/A

Usage Guidelines
Use this command to disable the multicast copy count extension feature and to destroy the internal VLAN and all the FDBs that are associated with this internal VLAN. It also disassociates the port ID from the loopback port.

Example
In this example, the feature is disabled and the configuration is removed.

unconfigure ext-mcast

History
This command was available in ExtremeWare 7.4.

Platform Availability
This command is available on "e" series platforms only.
unconfigure igmp

unconfigure igmp

Description
Resets all IGMP settings to their default values and clears the IGMP group table.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command resets all IGMP settings to their default values and clears the IGMP group table:

`unconfigure igmp`

History
This command was available in ExtremeWare 2.0.

This command was added to the Summit “e” series of switches in ExtremeWare 7.1e.

Platform Availability
This command is available on all platforms.
unconfigure mcast-queue-mgmt

Description
This command resets the configured queues for the multicast data forwarding.

Syntax Description
This command has no options or parameters.

Default
N/A

Usage Guidelines
Use this command to return to using a single queue for multicast stream forwarding. It does not disable the multicast queue management feature that was configured using the configure mcast-queue-mgmt command.

Example
The following example removes multiple queue configuration for multicast stream forwarding:

unconfigure mcast-queue-mgmt

History
This command was available in ExtremeWare 7.4.

Platform Availability
This command is available on the “i” platforms only.
unconfigure pim

    unconfigure pim {vlan <vlan name>}

Description
Resets all PIM settings on one or all VLANs to their default values.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
If no VLAN is specified, the configuration is reset for all PIM interfaces.

Usage Guidelines
None.

Example
The following command resets all PIM settings on the VLAN accounting:
unconfigure pim vlan accounting

History
This command was available in ExtremeWare 4.0.
This command was added to the Summit “e” series of switches in ExtremeWare 7.2e.

Platform Availability
This command is available on all platforms.
Basic IPX Command Overview

The “i” series switches provide support for the IPX, IPX/RIP, and IPX/SAP protocols. The switch dynamically builds and maintains an IPX routing table and an IPX service table.

The routing software and hardware routes IPX traffic between IPX router interfaces. A router interface is simply a VLAN that has an IPX network identifier (NetID) and IPX encapsulation type assigned to it.

As you create VLANs with different IPX NetIDs the switch automatically routes between them. Both the VLAN switching and the IPX routing function occur within the switch.

**NOTE**

A VLAN can be configured with either an IPX NetID or an IP address. A VLAN cannot be configured for both IPX and IP routing simultaneously.

This chapter describes the IPX commands.
configure ipxmaxhops

configure ipxmaxhops <number>

Description
Configures the IPX maximum hop count when forwarding IPX packets.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>number</td>
<td>Specifies a hop count number.</td>
</tr>
</tbody>
</table>

Default
The default setting is 16.

Usage Guidelines
Change the default number only if NetWare Link Services Protocol (NLSP) is running in the IPX network.

Example
The following command configures a maximum IPX hop count of 24:

```
configure ipxmaxhops 24
```

History
This command was first available in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxrip add vlan

configure ipxrip add vlan [<vlan name> | all]

Description
Configures one or all IPX VLANs to run IPX/RIP.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
IPX/RIP is enabled by default when you configure the IPX VLAN.

Usage Guidelines
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example
The following command configures the IPX VLAN named backbone to run IPX/RP:

```
configure ipxrip add vlan backbone
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxrip delete vlan

configure ipxrip delete vlan [<vlan name> | all]

Description
Disables IPX/RIP on one or all interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example
The following command disables IPX/RIP on the VLAN named backbone:
configure ipxrip delete vlan backbone

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series systems.
configure ipxrip vlan delay

configure ipxrip vlan [<vlan name> | all] delay <msec>

Description
Configures the time between each IPX/RIP packet within an update interval.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>msec</td>
<td>Specifies the delay time in milliseconds.</td>
</tr>
</tbody>
</table>

Default
The default setting is 55 milliseconds.

Usage Guidelines
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example
The following command configures a delay of 80 milliseconds:
configure ipxrip vlan accounting delay 80

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxrip vlan export-filter

configure ipxrip vlan [<vlan name>  | all] export-filter [none  |<access_profile>]

Description
Assigns an export route filter to an ingress VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no export filters.</td>
</tr>
<tr>
<td>access_profile</td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Only the network ID matching the export filter will be added to the IPX route table.

Example
The following command assigns an export route filter to the ingress VLAN named accounting:

```
configure ipxrip vlan accounting export-filter my-profile
```

History
This command was introduced in ExtremeWare 4.0; access-profiles modified in version 6.1.5b20.

Platform Availability
This command is available on all “i” series platforms.
configure ipxrip vlan import-filter

configure ipxrip vlan [<vlan name> | all] import-filter [none | <access_profile>]

**Description**
Assigns an import route filter to an ingress VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no import filters.</td>
</tr>
<tr>
<td>access_profile</td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Only the network ID matching the import filter will be added to the IPX route table.

**Example**
The following command assigns an import route filter to the ingress VLAN named accounting:

```
configure ipxrip vlan accounting import-filter my-profile
```

**History**
This command was introduced in ExtremeWare 4.0; access-profiles modified in version 6.1.5b20.

**Platform Availability**
This command is available on all “i” series platforms.
configure ipxrip vlan max-packet-size

    configure ipxrip vlan [vlan name] | all] max-packet-size <size>

Description
Configures the maximum transmission unit (MTU) size of the IPX/RIP packet.

Syntax Description

<table>
<thead>
<tr>
<th>Denis</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>size</td>
<td>Specifies the maximum packet size in bytes.</td>
</tr>
</tbody>
</table>

Default
The default setting is 432 bytes.

Usage Guidelines
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example
The following command configures an MTU size of 128 for the IPX/RIP packet:
configure ipxrip vlan accounting max-packet-size 128

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxrip vlan trusted-gateway

configure ipxrip vlan [<vlan name> | all] trusted-gateway [none | <access_profile>]

Description
Assigns an export route filter to the egress VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no export filters.</td>
</tr>
<tr>
<td>access_profile</td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Only services matching the trusted gateway are advertised on the egress VLAN.

Example
The following command assigns export route filter named smith to the VLAN named accounting:

```
configure ipxrip vlan accounting trusted-gateway access_profile
```

History
This command was introduced in ExtremeWare 4.0; access-profiles modified in version 6.1.5b20.

Platform Availability
This command is available on all “i” series platforms.
configure ipxrip vlan update-interval

configure ipxrip vlan [<vlan name> | all] update-interval <time>
{hold-multiplier <number>}

**Description**
Configures the update interval and hold multiplier for IPX/RIP updates.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>update-interval</td>
<td>Specifies the update interval time.</td>
</tr>
<tr>
<td>hold-multiplier</td>
<td>Specifies the hold multiplier for IPX/RIP updates.</td>
</tr>
</tbody>
</table>

**Default**
The default update interval is 60 seconds. The default multiplier is 3.

**Usage Guidelines**
This setting affects both the periodic update interval of IPX/RIP and the aging interval of learned routes. The aging period is calculated using the formula (update-interval * multiplier).

**Example**
The following command configures the IPX/RIP updates for an update interval of 30 seconds and a hold multiplier of 2 for the VLAN named accounting:

```
configure ipxrip vlan accounting update-interval 30 hold-multiplier 30
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all "i" series platforms.
configure ipxroute add

configure ipxroute add [dest_netid] | default] <next_hop_id> <next_hop_node_addr> <hops> <tics>

Description
Adds a static IPX route entry in the IPX route table.

Syntax Description

<table>
<thead>
<tr>
<th>dest_netid</th>
<th>Specifies the destination NetID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>next_hop_id</td>
<td>Specifies the NetID of the neighbor IPX network.</td>
</tr>
<tr>
<td>next_hop_node_addr</td>
<td>Specifies the node address of the next IPX router.</td>
</tr>
<tr>
<td>hops</td>
<td>Specifies the maximum hop count.</td>
</tr>
<tr>
<td>tics</td>
<td>Specifies the timer delay value.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Static routes are used to reach networks not advertised by routers. You can configure up to 64 static IPX routes on the switch. Static routes are never aged out of the routing table. Static routes are advertised to the network using IPX/RIP.

Example
The following command adds a static IPX route entry to the IPX route table:

```
configure ipxroute add default 0011 00:eb:2a:0b:1e:0a
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxroute delete

configure ipxroute delete [<dest_netid> | default] <next_hop_netid> <next_hop_node_addr>

Description
Removes a static IPX route entry from the route table.

Syntax Description

<table>
<thead>
<tr>
<th>dest_netid</th>
<th>Specifies the destination NetID.</th>
</tr>
</thead>
<tbody>
<tr>
<td>next_hop_id</td>
<td>Specifies the NetID of the neighbor IPX network.</td>
</tr>
<tr>
<td>next_hop_node_addr</td>
<td>Specifies the node address of the next IPX router.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you have defined default or static routes, those routes will remain in the configuration independent of whether the VLAN or VLAN IP address that used them remains. You should manually delete these routes if no VLAN IP address is capable of using them.

Example
The following command deletes a static IPX route entry to the IPX route table:

```
configure ipxroute delete default 0011 00:eb:2a:0b:1e:0a
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxsap add vlan

configure ipxsap add vlan [<vlan name> | all]

Description
Configures an IPX VLAN to run IPX/SAP routing.

Syntax Description
- **vlan name**: Specifies a VLAN name.
- **all**: Specifies all VLANs.

Default
N/A

Usage Guidelines
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example
The following command configures the IPX VLAN named accounting to run IPX/SAP routing:

```bash
configure ipxsap add vlan accounting
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxsap delete vlan

    configure ipxsap delete vlan [<vlan name> | all]

Description
Disables IPX/SAP on an interface.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VIANS.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example
The following command disables IPX/SAP on the VLAN named accounting:

    configure ipxsap delete vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxsap vlan delay

    configure ipxsap vlan [<vlan name> | all] delay <msec>

**Description**
Configures the time between each SAP packet within an update interval.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>msec</td>
<td>Specifies a delay in milliseconds.</td>
</tr>
</tbody>
</table>

**Default**
The default setting is 55 milliseconds.

**Usage Guidelines**
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

**Example**
The following command sets the time between each SAP packet to 40 milliseconds for the VLAN named accounting:

```
configure ipxsap vlan accounting delay 40
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
configure ipxsap vlan export-filter

configure ipxsap vlan [<vlan name> | all] export-filter [none | access_profile]

**Description**
Assigns an export route filter to an ingress VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no export filters.</td>
</tr>
<tr>
<td>access_profile</td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Only the network ID matching the export filter will be added to the IPX route table.

**Example**
The following command assigns an export route filter to the ingress VLAN named accounting:

```
configure ipxsap vlan accounting export-filter none
```

**History**
This command was introduced in ExtremeWare 4.0; access-profiles modified in version 6.1b20.

**Platform Availability**
This command is available on all “i” series platforms.
configure ipxsap vlan import-filter

configure ipxsap vlan [<vlan name> | all] import-filter [none | access_profile]

**Description**

Assigns an import route filter to an ingress VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies no route filters.</td>
</tr>
<tr>
<td>access_profile</td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Only the network ID matching the import filter will be added to the IPX route table.

**Example**

The following command assigns an import route filter to the ingress VLAN named accounting:

```
configure ipxsap vlan accounting import-filter none
```

**History**

This command was introduced in ExtremeWare 4.0; the `access-profile` keyword was modified in version 6.1.5b20.

**Platform Availability**

This command is available on all “i” series platforms.
configure ipxsap vlan max-packet-size

configure ipxsap vlan [vlan name | all] max-packet-size <number>

Description
Configures the MTU size of the IPX/SAP packets.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>max-packet-size</td>
<td>Specifies the maximum packet size in bytes.</td>
</tr>
<tr>
<td>&lt;number&gt;</td>
<td></td>
</tr>
</tbody>
</table>

Default
The default setting is 432 bytes.

Usage Guidelines
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example
The following command configures an MTU size of 356 bytes for the IPX/SAP packets on the VLAN named accounting:

```
configure ipxsap vlan accounting max-packet-size 356
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
**configure ipxsap vlan trusted-gateway**

`configure ipxsap vlan [<vlan name> | all] trusted-gateway [none | <access_profile>]`

**Description**
Assigns an export SAP service filter to the egress VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan name&gt;</code></td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td><code>all</code></td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td><code>none</code></td>
<td>Specifies no service filters.</td>
</tr>
<tr>
<td><code>access_profile</code></td>
<td>Specifies an access profile name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Only the services matching the trusted-gateway are advertised on the egress VLAN.

**Example**
The following command assigns an export SAP service filter named smith to the VLAN named accounting:

```
configure ipxsap vlan accounting trusted-gateway smith
```

**History**
This command was introduced in ExtremeWare 4.0; access-profiles modified in version 6.1.5b20.

**Platform Availability**
This command is available on all “i” series platforms.
configure ipxsap vlan update-interval

    configure ipxsap vlan [<vlan name> | all] update-interval <time>
    [hold-multiplier <number>]

Description
Configures the update interval and hold multiplier for IPX/SAP updates.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>update-interval &lt;time&gt;</td>
<td>Specifies the update interval time.</td>
</tr>
<tr>
<td>hold-multiplier &lt;number&gt;</td>
<td>Specifies the hold multiplier for IPX/RIP updates.</td>
</tr>
</tbody>
</table>

Default
The default update interval is 60 seconds. The default multiplier is 3.

Usage Guidelines
This setting affects both the periodic update interval of SAP and the aging interval of learned routes.
The default update interval is 60 seconds. The aging period is calculated using the formula
(update-interval * multiplier). The default multiplier is 3. Triggered update is always enabled; therefore,
new information is processed and propagated immediately.

Example
The following command configures an update interval of 30 seconds and a hold multiplier of 2 for the
IPX/SAP updates for the VLAN named accounting:

    configure ipxsap vlan accounting update-interval 30 hold-multiplier 2

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxsap vlan gns-delay

    configure ipxsap vlan <vlan name> gns-delay <msec>

Description
Configures the amount of time the switch waits before answering a Get Nearest Server (GNS) request.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>msec</td>
<td>Specifies a delay in milliseconds.</td>
</tr>
</tbody>
</table>

Default
The switch answers a GNS request as soon as possible (0 milliseconds).

Usage Guidelines
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example
The following command sets a GNS delay time of 20 milliseconds on the VLAN named accounting:

```bash
configure ipxsap vlan accounting gns-delay 20
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure ipxservice add

configure ipxservice add <service_type> <service_name> <netid> <mac_address> <socket> <hops>

**Description**

Adds a static entry to the IPX service table.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_type</td>
<td>Specifies a service type.</td>
</tr>
<tr>
<td>service_name</td>
<td>Specifies a service name.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies the IPX network identifier of the server.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies the MAC address of the server.</td>
</tr>
<tr>
<td>socket</td>
<td>Specifies the IPX port number on the server.</td>
</tr>
<tr>
<td>hops</td>
<td>Specifies the number of hops (for SAP routing purposes).</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Service information may also be entered into the IPX Service Table dynamically, by way of SAP. The `socket` keyword provides access to a particular function on the server.

**Example**

The following command adds the non-advertising server named chalk to the IPX service table, with 0004 as SAP for a file server, 00:AO:C9:17:22:F5 as the MAC address, 0451 as the socket number for a connection request, and 3 as the number of hops to the server:

configure ipxservice add chalk 0004 00:AO:C9:17:22:F5 0451 3

**History**

This command was introduced in ExtremeWare 4.0.

**Platform Availability**

This command is available on all “i” series platforms.
configure ipxservice delete

configure ipxservice delete <service_type> <service_name> <netid> <mac_address> <socket>

Description
Deletes an IPX service from the service table.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>service_type</td>
<td>Specifies a service type.</td>
</tr>
<tr>
<td>service_name</td>
<td>Specifies a service name.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies the IPX network identifier of the server.</td>
</tr>
<tr>
<td>mac_address</td>
<td>Specifies the MAC address of the server.</td>
</tr>
<tr>
<td>socket</td>
<td>Specifies the IPX port number on the server.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The service information is entered into the IPX Service Table in one of the following two ways:

- Dynamically, by way of SAP
- Statically, using the configure ipxservice add command

The socket keyword provides access to a particular function on the server.

Example
The following command deletes the non-advertising server named chalk from the IPX service table, with 0004 as SAP for a file server, 00:AO:C9:17:22:F5 as the MAC address, 0451 as the socket number for a connection request, and 3 as the number of hops to the server.

configure ipxservice delete chalk 0004 00:AO:C9:17:22:F5 0451

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
configure vlan xnetid

configure vlan <vlan name> xnetid <netid> [enet_ii | enet_8023 | enet_8022 | enet_snap]

**Description**
Configures a VLAN to use a particular encapsulation type.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies the IPX network identifier of the server.</td>
</tr>
<tr>
<td>enet_ii</td>
<td>Specifies an Ethernet 2 header.</td>
</tr>
<tr>
<td>enet_8023</td>
<td>Specifies the IEEE 802.3 length field.</td>
</tr>
<tr>
<td>enet_8022</td>
<td>Specifies and IEEE format and includes the IEEE 802.2 LLC header.</td>
</tr>
<tr>
<td>enet_snap</td>
<td>Specifies to add SNAP header to the IEEE 802.2 LLC header.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
Novell NetWare supports four types of frame encapsulation. The ExtremeWare term for each type is shown in Table 36.

**Table 36: IPX Encapsulation Types**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENET_II</td>
<td>The frame uses the standard Ethernet 2 header.</td>
</tr>
<tr>
<td>ENET_8023</td>
<td>The frame includes the IEEE 802.3 length field, but does not include the IEEE 802.2 Logical Link Control (LLC) header. This encapsulation is used by NetWare version 2.x and the original 3.x version.</td>
</tr>
<tr>
<td>ENET_8022</td>
<td>The frame uses the standard IEEE format and includes the IEEE 802.2 LLC header. This encapsulation is used by NetWare version 3.12 and 4.x.</td>
</tr>
<tr>
<td>ENET_SNAP</td>
<td>The frame adds a Subnetwork Access Protocol (SNAP) header to the IEEE 802.2 LLC header.</td>
</tr>
</tbody>
</table>

**Example**
The following command configures the VLAN named Support to use encapsulation type enet_8022:

```
configure vlan Support xnetid A2B5 enet_8022
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
disable ipxrip

disable ipxrip

Description
Disables IPX/RIP on the router.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example
The following disables IPX/RIP on the router:

disable ipxrip

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
disable ipxsap

    disable ipxsap

**Description**
Disables IPX/SAP on the router.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A

**Usage Guidelines**
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

**Example**
The following disables IPX/SAP on the router:

disable ipxsap

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
disable ipxsap gns-reply

    disable ipxsap gns-reply {vlan <vlan name>}

Description
Disables Get Nearest Server (GNS) reply on one or all IPX interfaces.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
ExtremeWare supports the GNS reply function. When a NetID is assigned to the switch, the GNS reply service is automatically enabled. When a station requests a particular service on the network (for example, locating a print server), the station sends a GNS request and the switch responds to the request. If GNS-reply is disabled, the switch drops the request.

Example
The following command disables GNS reply on the IPX VLAN named accounting:

disable ipxsap gns-reply vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
disable type20 forwarding

disable type20 forwarding (vlan <vlan name>)

Description
Disables the forwarding of IPX type 20 packets.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Type 20 packets are NetBIOS inside IPX.

Example
The following command disables the forwarding of IPX type 20 packets for the VLAN named accounting:

disable type20 forwarding vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
enable ipxrip

Description
Enables IPX/RIP on the router.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

Example
The following command enables IPX/RIP on the router:

```
enable ipxrip
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
enable ipxsap

enable ipxsap

Description
Enables IPX/SAP on the router.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
If no VLAN is specified, all VLANs are configured to run IPX/SAP routing. IPX/SAP routing is enabled by default when the IPX VLAN is configured.

Example
The following command enables IPX/SAP on the router:

   enable ipxsap

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
enable ipxsap gns-reply

    enable ipxsap gns-reply {vlan <vlan name>}

**Description**
Enables Get Nearest Server (GNS) reply on one or all IPX interfaces.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
The default setting is enabled.

**Usage Guidelines**
If no VLAN is specified, GNS reply is enabled on all IPX interfaces.

**Example**
The following command enables GNS reply for the IPX VLAN named accounting:

```
enable ipxsap gns-reply vlan accounting
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
enable type20 forwarding

    enable type20 forwarding {vlan <vlan name>}

**Description**
Enables the forwarding of IPX type 20 packets.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
Enabled

**Usage Guidelines**
Type 20 packets are NetBIOS inside IPX.

**Example**
The following command enables the forwarding of IPX type 20 packets for the VLAN named accounting:

```
enable type20 forwarding vlan accounting
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
show ipxconfig

    show ipxconfig {vlan <vlan name>}

**Description**
Displays IPX configuration information for one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
This command is analogous to the `show ipconfig` command for the IP protocol. It displays summary global IPX configuration information followed by per-VLAN information. Information includes enable/disable status for IPX/RIP, IPX/SAP, IPX route sharing, IPX service sharing, and so on.

**Example**
The following command displays the IPX configuration information for the VLAN named accounting:

```
show ipxconfig vlan accounting
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
show ipxfdb

    show ipxfdb {vlan <vlan name> | xnetid <netid>}

Description
Displays the hardware IPX FDB information.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies an IPX network number.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The switch maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in the FDB to decide whether a frame should be forwarded or filtered.

Example
The following command displays the hardware IPX FDB information for the VLAN named accounting:

    show ipxfdb vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
show ipxrip

    show ipxrip {vlan <vlan name>}

Description
Displays IPX/RIP configuration and statistics for one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The IPX/RIP information displayed includes operational and administrative status. It also lists any identified IPX/RIP neighbors, RIP packet statistics, and several other timer settings.

Example
The following command displays the IPX/RIP configuration information and statistics for the VLAN named accounting:

    show ipxrip vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
show ipxroute

    show ipxroute {vlan <vlan name> | xnetid <netid> | origin [static | rip | local]}

Description
Displays the IPX routes in the route table.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies an IPX network number.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies a statically defined route.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies a RIP learned route.</td>
</tr>
<tr>
<td>local</td>
<td>Specifies a local interface.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Route information is entered into the IPX route table in one of the following two ways:

- Dynamically, by way of RIP
- Statically, using the `configure ipxroute add` command

IPX/RIP is automatically enabled when a NetID is assigned to the VLAN. To remove the advertisement of an IPX VLAN, use the `configure ipxroute delete` command.

Example
The following command displays the IPX routes in the route table for the VLAN named accounting:

show ipxroute vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
show ipxsap

    show ipxsap {vlan <vlan name>}

Description
Displays the enable status of IPX/SAP for the VLAN, and its operational and administrative status (including the GNS reply service). It also lists any identified IPX/SAP neighbors, SAP packet statistics, and several other timer settings.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
IPX Commands—"i" Series Platforms Only

show ipxservice

    show ipxservice {vlan <vlan name> | xnetid <netid> | origin [static | sap | local]}

Description
Displays IPX services learned by way of SAP.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies an IPX network number.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The service information is entered into the IPX Service Table in one of the following two ways:

- Dynamically, by way of SAP
- Statically, using the `configure ipxservice add` command

Example
The following command displays IPX/SAP service information for the VLAN named accounting:

```
show ipxservice vlan accounting
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
show ipxstats

    show ipxstats {vlan <vlan name>}

Description
Displays IPX packet statistics for the IPX router, and one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
All VLANs

Usage Guidelines
Displays both RIP and SAP packet statistics.

Example
The following command displays IPX packet statistics for the VLAN named accounting:

    show ipxstats vlan accounting

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
unconfigure ipxrip

    unconfigure ipxrip {vlan <vlan name>}

Description
Resets the IPX/RIP settings on one or all VLANs to the default.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Removes import and export filters, and resets the MTU size, update interval, and inter-packet delay.

Example
The following command returns the VLAN named backbone to its IPX/RIP default settings:
unconfigure ipxrip vlan backbone

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
unconfigure ipxsap

unconfigure ipxsap {vlan <vlan name>}

Description
Resets the IPX/SAP settings on one or all VLANs to the default.

Syntax Description

- **vlan name** Specifies a VLAN name.

Default
N/A

Usage Guidelines
Removes import and export filters, and resets the MTU size, update interval, and inter-packet delay.

Example
The following command resets the IPX/SAP settings on the VLAN named backbone to the defaults:

```
unconfigure ipxsap vlan backbone
```

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
unconfigure vlan xnetid

unconfigure vlan <vlan name> xnetid

**Description**
Removes the IPX NetID of a VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
IPX/RIP is automatically enabled when a NetID is assigned to the VLAN.

**Example**
The following command removes the IPX NetID of the VLAN named accounting:

```
unconfigure vlan accounting xnetid
```

**History**
This command was introduced in ExtremeWare 4.0.

**Platform Availability**
This command is available on all “i” series platforms.
xping

xping {continuous} {size <n>} <netid> <node_address>

Description
Pings an IPX node specified by the network ID and the node address.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>continuous</td>
<td>Specifies that pings are to be sent continuously.</td>
</tr>
<tr>
<td>size &lt;n&gt;</td>
<td>Specifies the ping packet size in bytes.</td>
</tr>
<tr>
<td>netid</td>
<td>Specifies an IPX network number.</td>
</tr>
<tr>
<td>node_address</td>
<td>Specifies the MAC address of the node.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If continuous is not specified, four pings are sent. The default ping packet size is 256 data bytes. The size range is between 1 and 1,484 bytes.

Example
The following command pings IPX node 0010460 with a node address of 00:2b:2a:00:1c:0a:
xping 0010460 00:2b:2a:00:1c:0a

History
This command was introduced in ExtremeWare 4.0.

Platform Availability
This command is available on all “i” series platforms.
ARM Commands—BlackDiamond Switch Only

The Accounting and Routing Module (ARM) is a self-contained module for the BlackDiamond switch. Unlike other BlackDiamond modules, there are no external network interfaces on the ARM. Instead, the ARM provides advanced IP services for the other input/output (I/O) modules installed in the chassis. The ARM contains a powerful set of packet processing resources that operate in a one-armed fashion: receiving frames from the switch fabric, processing the frames, and transmitting the frames back into the switch fabric.

The two main features of the ARM are: IP unicast forwarding with selective longest prefix match and destination-sensitive accounting.

IP unicast packets are routed in the ARM hardware using a longest prefix match algorithm. This differs from the BlackDiamond’s switch fabric, which uses an exact match algorithm. The BlackDiamond’s switch fabric has greater forwarding capacity, but the ARM module has better handling of large numbers (hundreds of thousands) of IP routes to match each packet’s destination IP address. To take advantage of the BlackDiamond switch fabric’s forwarding capacity and the ARM module’s scalability, the ARM module can be configured to use the BlackDiamond switch fabric for some routes, and the ARM’s longest prefix match for others. This feature is called Selective-LPM.

The second feature, destination-sensitive accounting collects statistics that are maintained for forwarded IP traffic to support billing on a destination basis. To configure destination-sensitive accounting, a bin number can be assigned to one or more IP route entries using the ExtremeWare route-map command.

Bin numbers are integers that range from 0-7 and their only intrinsic meaning is to identify a particular set of accounting statistics. Each bin contains a 64-bit count of the number of packets that have been forwarded and a 64-bit count of the number of bytes that have been forwarded. When the ARM or MPLS module forwards an IP packet, the bin number from the forwarding database entry for the IP destination is used to identify the set of counters to be updated.

Eight unique bins are maintained for each of the possible 4096 VLAN IDs. Logically, the bins are organized as a two-dimensional array, with the row index being a VLAN ID and the column index being a bin number. Thus, when an IP frame is forwarded, the input VLAN ID selects the row and the bin number from the forwarding database entry selects the column. The use of input VLAN ID enables billing statistics to be maintained on a per customer basis where the VLAN ID identifies the customer.

This chapter documents the ARM command set. Some commands are new for the ARM; other commands have been enhanced to support the ARM.
Basic Accounting Configuration Information

This section uses several typical usage and configuration schemes to provide a brief overview of the destination-sensitive accounting configuration process as a general context for the detailed command description sections that follow.

In the most basic terms, to enable the accounting function, you must enable the accounting feature, create a customer VLAN ID, enable IP forwarding, and configure the accounting bin using the route map feature.

You use a special set of commands to configure the ARM module to initiate the accounting function.
clear accounting counters

clear accounting counters

Description
Clears (zeroes out) all of the accounting statistics.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
None.

Example
The following command clears (zeroes out) all of the accounting statistics:
clear accounting counters

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure route-map set accounting-index 1 value

configure route-map <route-map> <sequence_number> [add | delete] set accounting-index 1 value <bin_number>

Description
Configures the accounting bin number to be associated with the specified route map entry.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Specifies a route map.</td>
</tr>
<tr>
<td>sequence number</td>
<td>Specifies a specific entry in the route map.</td>
</tr>
<tr>
<td>add</td>
<td>Specifies to add the statement to the route map.</td>
</tr>
<tr>
<td>delete</td>
<td>Specifies to delete the statement from the route map.</td>
</tr>
<tr>
<td>bin_number</td>
<td>Specifies an accounting bin number.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines

- The accounting-index value is always set to 1 for destination-sensitive accounting.
- The route-map parameter identifies a particular route map.
- The sequence_number parameter identifies a specific entry in that route map. The sequence number must be associated with a match statement.
- The set accounting-index 1 value keyword phrase indicates that the following parameter is an accounting bin number.
- The bin_number parameter is an integer between 0—7, and allows you to define the accounting bin number.

Table 37: Set Operation Keywords

<table>
<thead>
<tr>
<th>Command</th>
<th>Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>accounting-index &lt;index&gt; value &lt;value&gt;</td>
<td>Sets the accounting bin number for the route-mapped accounting index. The accounting index value is always set to 1 for destination-sensitive accounting.</td>
</tr>
</tbody>
</table>

Example
The following command configures the accounting bin number to be associated with the specified route map entry:

configure route-map rt40 11 add set accounting-index 1 value 5

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure route-map set iphost-routing

configure route-map <route-map> <sequence-number> [add | delete ] set iphost-routing

Description
Enables or disables Selective-LPM for a specified route-map when the LPM feature is enabled.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Specifies a route map name.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>Specifies a sequence number.</td>
</tr>
<tr>
<td>add</td>
<td>Specifies to add the statement to the route map.</td>
</tr>
<tr>
<td>delete</td>
<td>Specifies to delete the statement from the route map.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command optionally enables or disables Longest Prefix Match (LPM) for the specified route-map. This command may be used to override the VLAN lpm-routing configuration for specific routes. The iphost-routing keyword specifies how packets are to be routed for route-map matched IP prefixes.

If the iphost-routing property is added to a route-map, packets are forwarded to the IP prefixes’ next hop using the hardware host-based IP FDB. The iphost-routing keyword is only significant for routes learned on VLANs that are lpm-routing enabled.

Example
This command enables Selective-LPM and specifies IP-host routing on the route map lpm_map:

configure lpm_map 20 add set iphost-routing

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure route-map set lpm-routing

    configure route-map <route-map> <sequence-number> [add | delete] set lpm-routing

Description
Enables or disables Selective-LPM for a specified route-map when the LPM feature is enabled.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>route-map</td>
<td>Specifies a route map name.</td>
</tr>
<tr>
<td>sequence-number</td>
<td>Specifies a sequence number.</td>
</tr>
<tr>
<td>add</td>
<td>Specifies to add the statement to the route map.</td>
</tr>
<tr>
<td>delete</td>
<td>Specifies to delete the statement from the route map.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command optionally enables or disables Longest Prefix Match (LPM) for the specified route-map. This command may be used to override the VLAN lpm-routing configuration for specific routes. The lpm-routing keyword specifies how packets are to be routed for route-map matched IP prefixes. If the lpm-routing property is added to a route-map, packets are forwarded to the IP prefixes’ next hop by the ARM/MPLS module using LPM routing.

The lpm-routing keyword is only significant for routes learned on VLANs that are not lpm-routing enabled.

Example
This command enables Selective-LPM and specifies lpm-routing on the route map lpm_map:

    configure lpm_map 10 add set lpm-routing

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
disable accounting

disable accounting

Description
Disables the destination-sensitive accounting function.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Destination-sensitive accounting collects statistics that are maintained for forwarded IP traffic to support billing on a destination basis. To configure destination-sensitive accounting, a bin number can be assigned to one or more IP route entries using the ExtremeWare route-map command.

Example
The following command disables the destination-sensitive accounting function:

disable accounting

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
disable ipforwarding lpm-routing

    disable ipforwarding lpm-routing {vlan <vlan name>}

Description
Disables Longest Prefix Match (LPM) routing for the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
When either an ARM or MPLS module is installed in a BlackDiamond switch, the module may be configured to forward IP packets for specified VLANs using LPM routing. If the `vlan name` parameter is omitted, `lpm-routing` is enabled for all configured VLANs, except the management VLAN.

Specifying the `lpm-routing` keyword for the disable command only disables LPM routing; it does not disable IP forwarding. By default, `lpm-routing` is not enabled on the VLAN when IP forwarding is enabled (for example, all VLANs perform host-based IP routing by default).

Example
This command configures LPM and IP-host routing for the `hop1` VLAN:

disable ipforwarding lpm-routing hop1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
disable lpm

disable lpm

Description
Disables Selective-LPM.

Syntax Description
This command has no arguments or variables.

Default
Default is disabled.

Usage Guidelines
None.

Example
The following command disables the Selective-LPM feature:
disable lpm

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
enable accounting

Description
Enables the destination-sensitive accounting function.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Destination-sensitive accounting collects statistics that are maintained for forwarded IP traffic to support billing on a destination basis. To configure destination-sensitive accounting, a bin number can be assigned to one or more IP route entries using the ExtremeWare `route-map` command.

Destination-sensitive accounting, LPM, and SLB are mutually exclusive functions and cannot be simultaneously enabled.

Example
The following command enables the destination-sensitive accounting function:

`enable accounting`

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
enable ipforwarding lpm-routing

   enable ipforwarding lpm-routing {vlan <vlan name>}

Description
Enables Longest Prefix Match (LPM) routing for the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
Default is disabled.

Usage Guidelines
When either an ARM or MPLS module is installed in a BlackDiamond switch, the module may be configured to forward IP packets for specified VLANs using LPM routing. If the \texttt{vlan name} parameter is omitted, lpm-routing is enabled for all configured VLANs, except the management VLAN.

By default, lpm-routing is not enabled on the VLAN when IP forwarding is enabled (for example, all VLANs perform host-based IP routing by default).

Example
This command configures LPM and IP-host routing for the hop2 VLAN:

   enable ipforwarding lpm-routing hop2

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
enable lpm

enable lpm

Description
Enables Selective-LPM routing.

Syntax Description
This command has no arguments or variables.

Default
Default is disabled.

Usage Guidelines
This command alters the state of the Selective-LPM routing feature (which is disabled by default). If Accounting is disabled, non-MPLS traffic to known routes is forwarded by hardware and the MSM CPU is used for slow-path traffic. When LPM is enabled, slow-path traffic is forwarded by the MPLS/ARM module at a faster rate. Also, if LPM is enabled, fast-path traffic to specified vlans or route-maps can be forwarded using longest prefix match on the module without installing IP FDB entries.

Example
The following command enables the Selective-LPM feature:

enable lpm

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
**show accounting**

```
show accounting {vlan <vlan name>}
```

**Description**

Displays accounting statistics for the specified VLAN. If no VLAN is specified, statistics for all VLANs are displayed.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vlan name</code></td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

You can display the accounting statistics for a single VLAN or all VLANs by issuing the `show accounting <vlan name>` command. The `show accounting <vlan name>` command lists the packet and octet counts for each bin number per VLAN. Omitting the VLAN name displays the accounting statistics for all the VLANs.

**Example**

The following command displays accounting statistics for the `vlan1` VLAN:

```
show accounting vlan1
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
show lpm

Description
Shows the status of the LPM feature.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines

Example

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
This chapter describes commands for the Remote Connect feature, which enables Altitude access points (APs) to be linked to a Summit 300-48 switch for image and configuration download without requiring a direct wired connection. The Remote Connect feature requires an Advanced Edge license.

Remote Connect is accomplished by way of virtual port assignments on the Summit 300-48 switch. In addition to the 48 physical ports on the switch (1:1-1:48), the Summit 300-48 has 48 virtual ports (virtual:1-virtual:48) that can be accessed over any physical port connection.

Parameters that are configurable on a physical wireless port are also configurable on all virtual ports. The only exception is the \texttt{ipaddress} parameter. On a physical wireless port, the IP address is manually configured. On a virtual port, the IP address is not configurable, because a remote A300 assigned to a virtual port is required to obtain an IP address from the DHCP Server.

Virtual port numbers can range from 1 to 48; however, a maximum of 24 virtual ports can be configured at one time on a Summit 300-48 switch. Virtual ports are accommodated in the ExtremeWare CLI using the following convention for the \texttt{<port>} variable, where \texttt{n} is the port number:

\begin{center}
\begin{tabular}{|c|c|}
\hline
\texttt{<port>} value & Description & Example \\
\hline
1:n & Physical port, Summit 300-48, Alpine 3800 series & configure wireless ports 1:2 \\
n & Physical port, Summit 300-24 & configure wireless port 2 \\
virtual:n & Virtual port, Summit 300-48 & configure wireless port virtual:2 \\
\hline
\end{tabular}
\end{center}
clear APmgmt redirect-db history

clear APmgmt redirect-db history

Description
Delete the redirect database history log on this switch.

Syntax Description
N/A

Default
N/A

Usage Guidelines
N/A

Example
clear APmgmt redirect-db history

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48 switch with Advanced Edge licensing.
clear APmgmt unknown-ap history

clear APmgmt unknown-ap history

Description
Delete the unknown AP history log on this switch.

Syntax Description
N/A

Default
N/A

Usage Guidelines
N/A

Example
clear APmgmt unknown-ap history

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
configure wireless bind

configure wireless bind [ap-mac | ap-serial | ap-ipaddr]

Description
Indicates the method by which Altitude 300 APs will be identified to this Summit 300-48 Attachment switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-mac</td>
<td>Specifies the MAC address as the binding method.</td>
</tr>
<tr>
<td>ap-serial</td>
<td>Specifies the serial number as the binding method.</td>
</tr>
<tr>
<td>ap-ipaddr</td>
<td>Specifies the IP address as the binding method.</td>
</tr>
</tbody>
</table>

Default
ap-mac

Usage Guidelines
N/A

Example
The following command specifies that MAC address will be used to identify A300s to the Discovery switch.

configure wireless bind ap-mac

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
configure wireless device-db

configure wireless device-db <id number> bind [ap-mac | ap-serial | ap-ipaddr] [attach-switch <ipaddr> | ports <vport>]

**Description**

Binds the A300 that corresponds to the specified device-db table entry ID on the Discovery switch to an Attachment switch or virtual port with the specified binding type. The device-db table is automatically populated.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ap-mac</td>
<td>Specifies the MAC address of the A300.</td>
</tr>
<tr>
<td>ap-serial</td>
<td>Specifies the serial number of the A300.</td>
</tr>
<tr>
<td>ap-ipaddr</td>
<td>Specifies the IP address of the A300.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>Specifies the IP address of the Attachment switch.</td>
</tr>
<tr>
<td>vport</td>
<td>Specifies a virtual port on the switch in the format virtual:n, where n is the virtual port number.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

The device database is used to store information about A300s that are not in the redirect database and not specified by virtual port binding.

**Example**

The following example binds the A300 that corresponds to the device-db table entry 1 on the Discovery switch to the Attachment switch with IP address 10.211.32.202. This command will result in adding an entry for the A300 in the redirect-db table with binding-type specified as ap-mac.

```shell
configure wireless device-db 1 bind ap-mac attach-switch 10.211.32.202
```

The following example binds the A300 that corresponds to the device-db table entry 2 to the virtual port virtual:1 on the same switch with the binding-type specified as ap-serial.

```shell
configure wireless device-db 2 bind ap-serial ports virtual:1
```

**History**

This command was first available in an ExtremeWare7.4.

**Platform Availability**

This command is available on the Summit 300-48 switch.
configure wireless ports bind

configure wireless port <vport> bind [ap-mac <ap-mac> | ap-serial <ap-serial> | ap-ipaddr <ap-ipaddr>]

Description
Assigns the specified A300 to the specified virtual port on this Summit 300-48 Attachment switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vport</td>
<td>Specifies a virtual port on the switch in the format virtual:n, where n is the virtual port number.</td>
</tr>
<tr>
<td>ap-mac</td>
<td>Specifies the MAC address of the A300.</td>
</tr>
<tr>
<td>ap-serial</td>
<td>Specifies the serial number of the A300.</td>
</tr>
<tr>
<td>ap-ipaddr</td>
<td>Specifies the IP address of the A300.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command should follow execution of configure wireless bind [ap-mac | ap-serial | ap-ipaddr].

Example
The following command assigns the A300 with IP address 10.211.32.96 to virtual port 1 on the switch.

config wireless ports virtual:1 bind ap-ipaddr 10.211.32.96

History
This command was first available in an ExtremeWare7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
configure wireless redirect-db

configure wireless redirect-db [add | del] [ap-mac <ap-mac> | ap-serial <ap-serial> | ap-ipaddr <ap-ipaddr>] attach-switch <ipaddr>

Description
Enters a record in the redirect database to assign the A300 to the indicated Attachment switch for configuration, or deletes the assignment.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Adds the specified A300 to the redirect database, assigning it to the Attachment switch indicated in the command.</td>
</tr>
<tr>
<td>del</td>
<td>Removes the redirect database record that assigns the A300 to the indicated Attachment switch.</td>
</tr>
<tr>
<td>ap-mac</td>
<td>Specifies the MAC address of the A300.</td>
</tr>
<tr>
<td>ap-serial</td>
<td>Specifies the serial number of the A300.</td>
</tr>
<tr>
<td>ap-ipaddr</td>
<td>Specifies the IP address of the A300.</td>
</tr>
<tr>
<td>ipaddr</td>
<td>Specifies the IP address of the Attachment switch.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
N/A

Example
The following command creates a redirect database record to assign the A300 with serial number SN-4567890 to the Attachment switch with IP address 10.21.32.200.

configure wireless redirect-db add ap-serial SN-4567890 attach-switch 10.211.32.200

History
This command was first available in an ExtremeWare7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
show APmgmt redirect-db history

show APmgmt redirect-db history

Description
Displays the redirect database history log on this switch.

Syntax Description
N/A

Default
N/A

Usage Guidelines
N/A

Example
The following command lists history information for the redirect database.
show APmgmt redirect-db history

redirect state machine log
1.0.1 serial=03208-00019 status=0xf363e7(OK=0xf363e7)) bootrom ver=2.2.0
redirect db index=0

History
This command was first available in an ExtremeWare7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
show APmgmt unknown-ap history

Description
Displays information detected APs that are not recorded in the redirect database and not assigned to a virtual port.

Syntax Description
N/A

Default
N/A

Usage Guidelines
N/A

Example
The following command lists history information regarding detected A300s that are not in the redirect database.

```
show APmgmt unknown-ap history
unknown ap state machine log
11/11/2004 16:22:52 hello: ip=10.211.37.86: 1026 mac=00:04:96:0D:9E:F0 hw id=Altitude 300-2i hw(ver=1.1.1 serial=04078-00211 status=0xf363e7(OK=0xf363e7)) bootrom ver=2.4.0
```

History
This command was first available in an ExtremeWare7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
show wireless device-db

    show wireless device-db (detail)

Description
Displays device database information.

Syntax Description

| detail | Displays additional information. |

Default
N/A

Usage Guidelines

Example

show wireless device-db

<table>
<thead>
<tr>
<th>ID</th>
<th>Device name</th>
<th>MAC addr</th>
<th>IP:port</th>
<th>Serial num</th>
<th>Last seen</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Altitude-300</td>
<td>00:01:30:F9:AD:70</td>
<td>10.211.32.201:1028</td>
<td>213132</td>
<td>12 seconds</td>
</tr>
</tbody>
</table>

show wireless device-db detail

History
This command was first available in an ExtremeWare7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
show wireless redirect-db

Description
Displays the information in the redirection database.

Syntax Description
N/A

Default
N/A

Usage Guidelines

Example

show wireless redirect-db

<table>
<thead>
<tr>
<th>idx</th>
<th>Key Type</th>
<th>Key value</th>
<th>Att_SW ipaddr</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>AP MacAddr:</td>
<td>00:04:96:1C:01:30</td>
<td>10.211.32.200</td>
</tr>
<tr>
<td>2</td>
<td>AP IPaddr:</td>
<td>10.211.32.230</td>
<td>10.211.32.200</td>
</tr>
<tr>
<td>3</td>
<td>AP Serial:</td>
<td>SN-4567890</td>
<td>10.211.32.200</td>
</tr>
</tbody>
</table>

History
This command was first available in an ExtremeWare 7.4.

Platform Availability
This command is available on the Summit 300-48 switch.
The Asynchronous Transfer Mode (ATM) module is an I/O module for the BlackDiamond 6800 series chassis-based system. The ATM module connects a BlackDiamond 6800 series switch to the ATM infrastructure used by metropolitan area service providers or enterprise customers and operators of server co-location networks.

Key applications for the ATM module are:

- Interconnecting metropolitan area networks across an ATM network infrastructure.
- Interconnecting server co-location network sites directly using ATM links.
- Providing connectivity between a legacy Enterprise ATM network and an Ethernet backbone.

In the first application, the metropolitan area network service provider can build service network sites in various cities, then use ATM modules in a BlackDiamond 6800 series switch to connect those cities to a carrier’s ATM infrastructure.

In the second application, operators of server co-location networks can use ATM modules in BlackDiamond 6800 series switches to create an ATM-based connection between server co-location sites. The result is that their network is simpler to manage, and problems can be isolated and resolved more expediently.

In the third application, a service provider can provide Ethernet-based services by using ATM modules in a BlackDiamond 6800 series switch to connect its enterprise ATM network to an Ethernet backbone.

Extreme Networks offers the ATM module in the following configurations:

- A3cSi: four OC-3c/STM-1 single-mode, intermediate-reach optical interfaces
- A3cMi: four OC-3 multimode, short-reach optical interfaces

This chapter describes the ATM command set. Some commands are new for the PoS modules; other commands have been enhanced to support the ATM modules.
configure atm add pvc

configure atm add pvc <vpi/vci> encap [l2 | ip peer-ipaddress <ipaddress>] vlan <vlan name> ports <portlist>

Description
This command configures PVC on an ATM port.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpi</td>
<td>Specifies the VPI parameter as an integer.</td>
</tr>
<tr>
<td>vci</td>
<td>Specifies the VCI parameter as an integer.</td>
</tr>
<tr>
<td>encap</td>
<td>Specifies the type of encapsulation to be used.</td>
</tr>
<tr>
<td>l2</td>
<td>Specifies Layer-2 encapsulation.</td>
</tr>
<tr>
<td>ip peer-ipaddress</td>
<td>Specifies that the VLAN will carry only routed IP traffic and that LLC encapsulation should be used.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
Before packets can be forwarded over ATM ports, at least one PVC must be configured on the port and mapped to a VLAN. Each PVC must be mapped to one or more VLANs and each mapping must be designated to use the bridged protocol encapsulation or the routed protocol encapsulation. Both encapsulations can be simultaneously used on a PVC as long as they are associated with different VLANs.

The PVC is identified by the specified vpi and vci parameters. The vpi parameter is an integer in the range of 0 through 15. The vci parameter is an integer in the range of 17 through 4095. Both parameters are defined in RFC 2648/1483.

The encap parameter indicates the type of encapsulation that is to be used on the PVC for traffic from the associated VLAN. The l2 keyword is an abbreviation for Layer-2 and indicates the LLC Encapsulation for Bridged Protocols (defined in RFC 2684). The ip keyword indicates that the VLAN will carry only routed IP traffic and that the LLC Encapsulation for Routed Protocols (defined in RFC 2684) should be used.

Example
The following command configures PVC 5/101 on ATM port 1:1 on a VLAN named accounting.

configure atm add pvc 5/102 encap 12 vlan accounting port 1:1
History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available only on the BlackDiamond switch.
configure atm delete pvc

configure atm delete pvc [<vpi / vci> | all] {vlan <vlan name>} ports <portlist>

Description
This command is used to delete a PVC configuration on an ATM port.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpi</td>
<td>Specifies the VPI parameter as an integer. The valid VPI range is from 0 to 15.</td>
</tr>
<tr>
<td>vci</td>
<td>Specifies the VCI parameter as an integer. The valid VCI range is from 17 to 4095</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all ATM ports or all PVCs.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
This command deletes the specified PVC configuration on the specified ATM port(s). The optional vlan parameter may be used to limit the scope of the command to the specified VLAN. The PVC may still exist following command execution if multiple VLANs have been configured to use the PVC. If the vlan parameter is omitted, the PVC configuration is deleted for all VLANs on the specified ATM port(s).

The command can be used to delete configuration information for the PVC identified via the vpi and vci parameters for all PVCs defined for the specified VLAN(s) or port(s). The all keyword may be used as either a portlist parameter to indicate that the command should be applied to all ATM ports or all PVCs. A PVC is completely deleted when there are no longer any VLANs configured for the PVC on a given ATM port.

NOTE
All associated PVCs must be deleted before an ATM port can be removed from a VLAN.

Example
The following command deletes the specified PVC configuration on ATM port 1:1 on a VLAN named accounting.

configure atm delete pvc 5/102 encap l2 vlan accounting port 1:1
**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available only on the BlackDiamond switch.
configure atm scrambling

configure atm scrambling [on | off] ports <portlist>

Description
This command configures an ATM port to scramble the cell payload on a specified ATM port(s).

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables payload data scrambling. Default is on.</td>
</tr>
<tr>
<td>off</td>
<td>Disables payload data scrambling.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies list of ports or slots and ports. May be in the form 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
Enabled

Usage Guidelines
Scrambling is used to improve signal synchronization and the performance of the ATM cell delineation process.

Choose either on or off. Scrambling is enabled by default.

Example
The following command example turns off the scrambling function for port 1 of the ATM module installed in slot 8 of a BlackDiamond switch.

configure atm scrambling off ports 8:1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available only on the BlackDiamond switch.
show atm

    show atm {<portlist>}

Description
This command displays ATM port status.

Syntax Description

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
You can use the optional portlist parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all ports.

By default, the command displays a summary of status information for the specified ports.

The summary of status information includes the following information for each port:

- Values of all port configuration parameters
- Port state
- ATM statistics

The detailed status information includes the summary information plus any ATM statistics. Table 38 describes the ATM receive statistics, and Table 39 describes the ATM transmit statistics.

Table 38: Summary of ATM Receive Statistics

<table>
<thead>
<tr>
<th>Receive Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cells Received</td>
<td>Number of cells received.</td>
</tr>
<tr>
<td>Cells OAM</td>
<td>Number of Operations, Administration, and Maintenance (OAM) cells received.</td>
</tr>
<tr>
<td>Cells Dropped (Congestion)</td>
<td>Number of cells dropped due to insufficient buffers.</td>
</tr>
<tr>
<td>Cells Dropped (Invalid VCC)</td>
<td>Number of cells dropped due to invalid VPI/VCI or AAL-5 header.</td>
</tr>
<tr>
<td>Cells Dropped (HEC)</td>
<td>Number of cells dropped with Header Error Control (HEC) errors. HEC is an 8 bit cyclic redundancy check (CRC) computed on all fields in an ATM header and capable of detecting bit errors. HEC is used for cell delineation.</td>
</tr>
<tr>
<td>PDUs Received</td>
<td>Number of PDUs received.</td>
</tr>
<tr>
<td>PDUs Dropped (CRC)</td>
<td>Number of PDUs discarded due to CRC-32 errors.</td>
</tr>
</tbody>
</table>
### Table 38: Summary of ATM Receive Statistics (Continued)

<table>
<thead>
<tr>
<th>Receive Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PDUs Dropped (Oversized)</td>
<td>Number of PDUs discarded because they were too large.</td>
</tr>
<tr>
<td>PDUs Dropped (Other)</td>
<td>PDUs dropped due to an invalid VLAN ID, Spanning Tree Protocol (STP) state, or invalid encapsulation.</td>
</tr>
<tr>
<td>Section parity errors</td>
<td>Number of parity errors at the section level.</td>
</tr>
<tr>
<td>Line parity errors</td>
<td>Number of parity errors at the line level.</td>
</tr>
<tr>
<td>Path parity errors</td>
<td>Number of parity errors at the path level.</td>
</tr>
<tr>
<td>REI-L event counter</td>
<td>Remote error indication-line events</td>
</tr>
<tr>
<td>REI-P event counter</td>
<td>Remote error indication-path events</td>
</tr>
<tr>
<td>LOS event counter</td>
<td>Loss of signal events</td>
</tr>
<tr>
<td>LOF event counter</td>
<td>Loss of frame events</td>
</tr>
<tr>
<td>LOP event counter</td>
<td>Loss of pointer events</td>
</tr>
<tr>
<td>AIS-L event counter</td>
<td>Alarm indication signal-line events</td>
</tr>
<tr>
<td>AIS-P event counter</td>
<td>Alarm indication signal-path events</td>
</tr>
<tr>
<td>RDI-L event counter</td>
<td>Remote defect identification-line events</td>
</tr>
<tr>
<td>RDI-P event counter</td>
<td>Remote defect identification-path events</td>
</tr>
<tr>
<td>PLM-P event counter</td>
<td>Payload label mismatch-path events</td>
</tr>
<tr>
<td>SF BER event counter</td>
<td>Signal-fail bit-error rate events</td>
</tr>
<tr>
<td>SD BER event counter</td>
<td>Signal-fail bit-error rate events</td>
</tr>
</tbody>
</table>

### Table 39: Summary of ATM Transmit Statistics

<table>
<thead>
<tr>
<th>Receive Statistics</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cells Transmitted</td>
<td>Number of cells transmitted.</td>
</tr>
<tr>
<td>Cells Dropped (Congestion)</td>
<td>Number of cells dropped due to insufficient buffers.</td>
</tr>
<tr>
<td>PDUs Transmitted</td>
<td>Number of PDUs transmitted.</td>
</tr>
<tr>
<td>Section parity errors</td>
<td>Number of parity errors at the section level.</td>
</tr>
<tr>
<td>Line parity errors</td>
<td>Number of parity errors at the line level.</td>
</tr>
<tr>
<td>Path parity errors</td>
<td>Number of parity errors at the path level.</td>
</tr>
<tr>
<td>REI-L event counter</td>
<td>Remote error indication-line events</td>
</tr>
<tr>
<td>REI-P event counter</td>
<td>Remote error indication-path events</td>
</tr>
<tr>
<td>LOS event counter</td>
<td>Loss of signal events</td>
</tr>
<tr>
<td>LOF event counter</td>
<td>Loss of frame events</td>
</tr>
<tr>
<td>LOP event counter</td>
<td>Loss of pointer events</td>
</tr>
<tr>
<td>AIS-L event counter</td>
<td>Alarm indication signal-line events</td>
</tr>
<tr>
<td>AIS-P event counter</td>
<td>Alarm indication signal-path events</td>
</tr>
<tr>
<td>RDI-L event counter</td>
<td>Remote defect identification-line events</td>
</tr>
<tr>
<td>RDI-P event counter</td>
<td>Remote defect identification-path events</td>
</tr>
<tr>
<td>PLM-P event counter</td>
<td>Payload label mismatch-path events</td>
</tr>
<tr>
<td>SF BER event counter</td>
<td>Signal-fail bit-error rate events</td>
</tr>
<tr>
<td>SD BER event counter</td>
<td>Signal-fail bit-error rate events</td>
</tr>
</tbody>
</table>
Example

The following command displays ATM port status for all ports:

`show atm`

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available only on the BlackDiamond switch.
show atm pvc

    show atm [<vpi / vci> | all] {vlan <vlan name>} ports <portlist>

**Description**

This command displays status information for a PVC.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpi</td>
<td>Specifies the VPI parameter as an integer. The valid VPI range is from 0 to 15.</td>
</tr>
<tr>
<td>vci</td>
<td>Specifies the VCI parameter as an integer. The valid VCI range is from 17 to 4095</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies list of ports or slots and ports. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

**Default**

None

**Usage Guidelines**

You can specify a particular PVC to display information for, or you can specify that information for all PVCs be displayed.

Use the optional `vlan` parameter to narrow the range of status information the command displays; otherwise, the command displays status information for all VLANs.

You can use the optional `portlist` parameter to narrow the range of status information the command displays; otherwise, the command displays the status information for all PVCs associated with all ATM ports.

By default, the command displays a summary of status information for the specified PVC.

The summary of status information includes the following information for each PVC:

- Port number
- VPI/VCI
- VLAN IDs on this PVC
- Type of PVC (L2 or IP)
- Peer IP address (for IP PVCs)
- Received octets
- Received packets
- Transmitted octets
- Transmitted packets
Example

The following command example displays all of the PVC status information for a PVC configured on an ATM port in a BlackDiamond switch:

```
show atm pvc 5/101 port 1:1
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available only on the BlackDiamond switch.
PoS Commands—BlackDiamond Switch Only

The Packet over SONET (PoS) modules are I/O modules for the BlackDiamond switch. These modules connect a BlackDiamond 6800 series switch to the SONET infrastructure used by metropolitan area service providers and operators of server co-location networks. (The BlackDiamond 6800 series switch is a chassis-based switch designed to be placed in the core of your network.)

Two key applications for the PoS modules are: interconnecting metropolitan area networks across the SONET network infrastructure, and interconnecting server co-location network sites directly using SONET links.

In the first application, the metropolitan area network service provider can build service network sites in various cities, then use PoS modules in a BlackDiamond switch to connect those cities to a carrier’s SONET infrastructure.

In the second application, operators of server co-location networks can use PoS modules in BlackDiamond switches to create a SONET-based connection between server co-location sites. The result is that their network is simpler to manage, and problems can be isolated and resolved more expediently.

This chapter documents the PoS command set. Some commands are new for the PoS modules; other commands have been enhanced to support the PoS modules.
configure aps

    configure aps <group#> [nonrevert | revert <minutes>]

Description
Configures APS operation in either nonrevertive or revertive switching mode.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>nonrevert</td>
<td>Specifies nonrevertive switching mode when traffic is active on the protection line and the working line becomes operational.</td>
</tr>
<tr>
<td>revert</td>
<td>Specifies revertive switching mode when traffic is active on the protection line and the working line becomes operational.</td>
</tr>
<tr>
<td>minutes</td>
<td>Specifies the wait-to-restore (WTR) period in minutes.</td>
</tr>
</tbody>
</table>

Default
The default mode is nonrevertive switching.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the configuration command applies to. The default mode is nonrevertive switching. This parameter determines what action should be taken when traffic is active on the protection line and the working line becomes operational. In revertive mode, traffic will automatically be switched from the protection line to the working line, after the user-defined wait-to-restore (WTR) period, which may be specified via the minutes parameter. The WTR period is intended to prevent frequent switches due to intermittent errors on the working line; service is restored only if no errors are detected on the working line during the WTR period. The minutes parameter is an integer in the range [0-12]. Conversely, in nonrevertive mode, traffic will remain on the protection line (until either manual intervention or a failure on the protection line forces a switch back to the working line). This parameter is only applicable to SONET ports performing the protection line function.

Example
The following command configures an APS operation on group 1001 in revertive switching mode for 5 minutes:

    configure APS 1001 revert 5

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps add

configure aps <group#> add <port> [working | protection <ip address>]

Description
Adds a SONET port to an APS group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies the SONET port number to be added to the APS group.</td>
</tr>
<tr>
<td>working</td>
<td>Specifies that the port is the working line.</td>
</tr>
<tr>
<td>protection</td>
<td>Specifies that the port is the protection line.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the BlackDiamond switch where working line resides.</td>
</tr>
</tbody>
</table>

Default
By default, no ports are added to an APS group. Ports must be explicitly added using this command for proper APS operation.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the port is to be added to. You also specify the port parameter, which identifies the SONET port that is to be added to the APS group. Additionally, you specify whether the port is designated as the working or protection line. Only one working line and one protection line can be added to an APS group. If the port is designated as the protection line, then you must also specify an IP address (ip address) of the BlackDiamond switch where the working line resides. This IP address is used to send APS control messages to the BlackDiamond switch containing the working line. It is recommended that the configured ip address be associated with an Ethernet VLAN that has loopback mode enabled (to minimize the impact of network outages on APS functionality). It is important that the network connecting working and protection switches always have sufficient bandwidth to support APS control transfers.

In routing configurations, the working line and the protection line should represent the same IP address from a neighboring PPP router's perspective. When the working line and protection line reside in the same BlackDiamond switch, this implies that both ports should be members of the same VLAN. The case where both the working line and the protection line for an APS group reside in the same BlackDiamond switch is the only situation where the PPP IP control protocol (IPCP) can be enabled on multiple SONET ports that are members of the same VLAN. In general, if IPCP is enabled on a SONET, then the port can only be a member of one VLAN, and no others ports can be members of that VLAN.

Example
The following command example adds port 1 of the module installed in slot 8 of the BlackDiamond switch to APS group 1001 as the working line:

config aps 1001 add 8:1 working
History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps authenticate

configure aps <group#> authenticate [off | on <string>]

Description
Configures authentication of APS control messages.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that authentication is turned off.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies authentication is turned on.</td>
</tr>
<tr>
<td>string</td>
<td>Specifies the authentication string used to validate the APS control frames received over an Ethernet link.</td>
</tr>
</tbody>
</table>

Default
The default setting is off.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the authentication command applies to. You also specify whether authentication is to be turned off or turned on. If authentication is being enabled, a text authentication string must also be specified. This string can contain up to eight alphanumerical characters. If the working line and the protection line for an APS group reside in different BlackDiamond switches, then the same string must be configured at both BlackDiamond switches for authentication to work properly. The authentication string is used to validate APS control frames received over an Ethernet link. If authentication fails, the associated APS control frame is discarded.

Example
The following command example enables APS authentication for group 1001, with seer5dog as the authentication string:

```
config aps 1001 authenticate on seer5dog
```

History
This command was first available in ExtremeWare 6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps delete

configure aps <group#> delete <port>

Description
Deletes a SONET port from an APS group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies the port number.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the port is to be deleted from. You also specify the port parameter, which identifies the SONET port that is to be deleted from the APS group. If you delete the working line from a group, it causes a switch to the protection line; however, if you delete an active protection line from a group, it does not initiate a switch to the working line.

Example
The following command example deletes port 1 of the module installed in slot 8 of the BlackDiamond switch from APS group 1001:

```
config aps 1001 delete 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps force

configure aps <group#> force [off | working | protection]

Description
Requests that an APS group be forced to use a specified line as the active line.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that force is disabled.</td>
</tr>
<tr>
<td>working</td>
<td>Specifies that the APS group uses the working line as the active line.</td>
</tr>
<tr>
<td>protection</td>
<td>Specifies that the APS group uses the protection line as the active line.</td>
</tr>
</tbody>
</table>

Default
The default is force off.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the force command applies to. When force working is specified, the command requests that the APS group uses the working line as the active line. Conversely, when force protection is specified, the command requests that the APS group uses the protection line as the active line. A forced switch is a high priority request. Only three events can override a forced switch request: (1) a force off command, (2) a lockout on command (that was either in effect before the force command or issued after the force command), or (3) a signal-fail condition on the protection line. This command is only applicable to SONET ports performing the protection line function. Additionally, the effects of this command are not preserved across a switch reboot.

Example
The following command example forces APS group 1001 to use the protection line as the active line:

    config aps 1001 force protection

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps lockout

configure aps <group#> lockout [off | on]

Description
Controls whether a switch to the protection line is locked out.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;group#&gt;</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that switches from the working line to the protection line are allowed.</td>
</tr>
<tr>
<td>on</td>
<td>Specifies that switches from the working line to the protection line are prohibited.</td>
</tr>
</tbody>
</table>

Default
The default is off.

Usage Guidelines
The group# identifies the APS group that the lockout command applies to. When lockout on is specified, switches from the working line to the protection line are prohibited, until you subsequently issue a lockout off command. The default is lockout off. This command is only applicable to SONET ports performing the protection line function. Additionally, the effects of this command are not preserved across a switch reboot.

Example
The following command example turns on lockout mode for APS group 1001:

cfg aps 1001 lockout on

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps manual

configure aps <group#> manual [off | working | protection]

Description
Manually determines whether an APS group uses its working line or its protection line as the active line.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>off</td>
<td>Specifies that manual switching is disabled, and can be overridden.</td>
</tr>
<tr>
<td>working</td>
<td>Specifies that the APS group uses the working line as the active line.</td>
</tr>
<tr>
<td>protection</td>
<td>Specifies that the APS group uses the protection line as the active line.</td>
</tr>
</tbody>
</table>

Default
The default is manual off.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the command applies to. When manual working is specified, the command requests that the APS group uses the working line as the active line. Conversely, when manual protection is specified, the command requests that the APS group uses the protection line as the active line. One potential use of the manual working command is to switch back to the working line after an error condition has cleared without waiting for the full wait-to-restore period to elapse. A manual switch is a lower priority request than a forced switch. events that can override a manual switch include: (1) a manual off command, (2) a force working or a force protection command, (3) a lockout on command, or (4) a signal-fail or signal degrade line condition. This command is only applicable to SONET ports performing the protection line function. Additionally, the effects of this command are not preserved across a switch reboot.

Example
The following command example configures APS group 1001 to use its working line as the active line:
config aps 1001 manual working

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure aps timers

    configure aps <group#> timers <seconds> <consecutive_misses>

Description
Sets the values of the timers used in the APS hello protocol that is exchanged between the working and protection switches for an APS group.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the amount of time in seconds the protection switch waits between transmissions of hello packets to the working switch.</td>
</tr>
<tr>
<td>consecutive_misses</td>
<td>Specifies the time interval the protection switch will wait before assuming the working switch has failed.</td>
</tr>
</tbody>
</table>

Default
The default values are seconds = 1 and consecutive_misses = 5. These parameters are only applicable to SONET ports performing the protection line function.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the configuration command applies to. The seconds parameter is an integer in the range [1-300] that specifies the amount of time the protection switch waits between transmissions of hello packets to the working switch. The consecutive_misses parameter is an integer in the range [1-100] that controls the time interval the protection switch will wait before assuming that the working switch has failed. If the working switch does not respond within consecutive_misses hello intervals, or (consecutive_misses * seconds) seconds, then the protection switch assumes that the working switch has failed and initiates a line switch.

Example
The following command example configures the timers for APS group 1001 to 1 second and 3 consecutive misses:
config aps 1001 timers 1 3

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure diffserv dscp-mapping ports

configure diffserv dscp-mapping <input_codepoint>/<output_codepoint> ports <portlist> {egress {no-congestion | congestion} | ingress}

Description
Configures a mapping between an input DiffServ code point (DSCP) and an associated output DSCP for the specified PoS or ATM ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input_codepoint</td>
<td>Specifies one of the 64 possible DiffServ code point values as the input code point.</td>
</tr>
<tr>
<td>output_codepoint</td>
<td>Specifies one of the 64 possible DiffServ code point values as the output code point.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>egress</td>
<td>Applies the DSCP mapping to the egress direction.</td>
</tr>
<tr>
<td>no-congestion</td>
<td>Applies the DSCP mapping to the egress mapping table for the non-congested state.</td>
</tr>
<tr>
<td>congestion</td>
<td>Applies the DSCP mapping to the egress mapping table for the congested state.</td>
</tr>
<tr>
<td>ingress</td>
<td>Applies the DSCP mapping to the ingress direction.</td>
</tr>
</tbody>
</table>

Default
By default, all the tables are initialized such that DSCPs are not altered by the mapping operations; for example, an input DSCP value of n is always mapped to an output DSCP value of n. Additionally, dscp-mapping is performed without regard to whether diffserv examination is enabled on the port.

Usage Guidelines
Three DSCP mapping tables are supported per SONET port. One of the tables is used in the ingress direction and two are used for egress flows (onto the SONET link). The two egress tables are for the congested and non-congested states, as determined by the RED algorithm (in other words, the congested state is when the average queue length is greater than the minimum RED threshold). If RED is not enabled on the SONET port, then the egress congested-state mapping table is not used.

The tables are very simple. In the ingress direction, the input DSCP of a packet received from the SONET link is replaced with an output DSCP before the packet is forwarded. The replacement is straightforward; the input DSCP is used as an index into a 64-entry table that contains the output DSCPs associated with each of the input DSCP values. The operation is similar in the egress direction, with the DSCP mapping occurring before the packet is transmitted onto the SONET link(s). The mapping operation is performed after the packet has been assigned to a QoS profile. One potential use of the DSCP mapping capability is reconciliation of varying DiffServ policies at the boundary between autonomous systems (for example, at the boundary between two ISPs). The availability of different tables for the congested/non-congested states is useful for marking operations that increase the drop probability of packets during times of congestion, as discussed in the DiffServ assured forwarding (AF) RFC.
PoS Commands—BlackDiamond Switch Only

This command is currently only applicable to SONET ports. If the no-congestion/congestion keywords are omitted, the mapping is applied to the egress tables for both states. If the egress/ingress keywords are omitted, the mapping is assumed to apply to the egress direction, and a symmetrical mapping (with the input_codepoint and output_codepoint reversed) is automatically configured in the ingress direction.

Example
The following command example configures the congested-state mappings for DSCPs 10 (AF11):

```
configure diffserv dscp-mapping 10/12 egress congestion
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure dot1q tagmapping ports

configure dot1q tagmapping <input_vlanid/output_vlanid> ports <portlist> {egress {priority <priority>} | ingress {priority <priority>}}

Description
Configures the VLAN tag mapping attributes for a PoS or ATM port.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>input_vlanid</td>
<td>Specifies VLAN ID of the input to be mapped.</td>
</tr>
<tr>
<td>output_vlanid</td>
<td>Specifies the VLAN ID of the output to be mapped.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>ingress</td>
<td>Indicates that the mapping is to be applied to input frames received from the PPP link.</td>
</tr>
<tr>
<td>egress</td>
<td>Indicates that the mapping is to be applied to input frames going to the PPP link.</td>
</tr>
<tr>
<td>priority</td>
<td>Allows you to set the 802.1p priority value.</td>
</tr>
</tbody>
</table>

Default
The default is to initialize the tables so the VLAN IDs are not altered by the mapping operations (for example, an input VLAN ID of n is always mapped to an output VLAN ID of n), and the frame priority is preserved.

Usage Guidelines
This command is only applicable when BCP is enabled on the port. Currently, the command is only supported for PoS ports. Two mapping tables are supported per PoS port. One of the tables is used in the egress direction and the other table is used in the ingress direction. Each of the tables enable an input VLAN ID to be mapped to an output VLAN ID, which can be useful in reconciling policy differences at customer/service provider boundaries. The egress keyword indicates that the mapping is to be applied to frames received from the switch backplane before transmission onto the PoS link(s). Conversely, the ingress keyword indicates that the mapping is to be applied to input frames received from the PoS link. The mappings are applied following classification to a QoS profile.

Frames containing the specified input_vlanid are altered such that the VLAN ID is set to the specified output_vlanid before the frame is forwarded. The tables also allow the option of preserving the 802.1p priority or overwriting the priority field with a configured value. The priority keyword indicates that the 802.1p priority field is to be set to the value of the priority parameter. Omission of the priority keyword indicates that the 802.1p priority of the frame is to be preserved. If the egress/ingress keywords are omitted, the specified mapping is applied to the egress direction, and a symmetrical mapping (with the input_vlanid and output_vlanid reversed) is automatically configured in the ingress direction. The input_vlanid and output_vlanid parameters are integers in the range [1-4095]. The priority parameter is an integer in the range [0-7].
Example
The following command configures the tagmapping attributes for input VLAN ID 30 and output VLAN ID 130 for port 1 of the module installed in slot 8 for the input frames from the PPP link:

`configure dot1q tagmapping 30/130 port 8:1 ingress`

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure dot1q tagnesting ports

configure dot1q tagnesting {<vlanid> | <vlanid_range>} [off | pop | push <new_vlanid> {priority <priority>}] ports <portlist> {egress | ingress}

**Description**
Configures the VLAN tag nesting attributes for a PoS or ATM port. Currently, the command is only supported for PoS and ATM ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlanid</td>
<td>Specifies that the tag nesting will be performed on the frames containing the VLAN ID given.</td>
</tr>
<tr>
<td>vlanid_range</td>
<td>Specifies that the tag nesting will be performed on the frames containing VLAN ID values in the given range.</td>
</tr>
<tr>
<td>off</td>
<td>Disables tag nesting.</td>
</tr>
<tr>
<td>pop</td>
<td>Deletes a tag from the frame.</td>
</tr>
<tr>
<td>push</td>
<td>Adds a tag to the frame.</td>
</tr>
<tr>
<td>new_vlanid</td>
<td>Specifies the VLAN ID of the tag to be added or deleted from the frame.</td>
</tr>
<tr>
<td>priority</td>
<td>Allows you to set the 802.1p priority value.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>egress</td>
<td>Specifies that the tag operations are to be performed to the PPP link.</td>
</tr>
<tr>
<td>ingress</td>
<td>Specifies that the tag operations are to be performed from the PPP link.</td>
</tr>
</tbody>
</table>

**Default**
By default, tag nesting is off for all VLAN IDs. If the **egress/ingress** keywords are omitted, the direction defaults to **egress**. Additionally, if the **egress/ingress** keywords are omitted and a tag push operation is configured, a corresponding tag pop operation is automatically configured for the **ingress** direction. Similarly, if the **egress/ingress** keywords are omitted and tag nesting is configured off, it is disabled in both directions.

**Usage Guidelines**
The command provides support for nested 802.1Q tags by allowing a tag push/pop attribute to be associated with a VLAN ID. The push attribute indicates that a new tag is to be added to the frame, while the pop attribute indicates that the top-level tag is to be removed from the frame. The **push** keyword indicates that a new tag is to be added to frames containing the specified **vlanid** or one of the VLAN IDs in the specified **vlanid_range**. The syntax of the **vlanid_range** parameter is **start_vlanid-end_vlanid**. Omission of the **vlanid/vlanid_range** parameter indicates that the command settings should be applied to all VLAN IDs. For push operations, the new tag added to frames contains the specified **new_vlanid**.

The **pop** keyword indicates that the top-level tag is to be removed from frames when the tag contains any of the specified VLAN IDs. Tag operations may be performed in either **egress** (to the PoS link) or **ingress** directions.

When a new tag is pushed, an option is available to allow the 802.1p priority of the frame to be either preserved or set to a configured value. The priority keyword indicates that the 802.1p priority field is to
be set to the value of the priority parameter. Omission of the `priority` keyword indicates that the 802.1p priority of the frame is to be preserved. The `vlanid` parameters are integers in the range [1-4095]. The `priority` parameter is an integer in the range [0-7].

This command is only applicable when BCP is enabled on the port. Furthermore, tag push operations are applicable to egress frames only when the port is configured to transmit tagged frames for the associated VLAN. The tag-nesting operations are only applicable to ingress frames that contain a VLAN tag. The tag-nesting operations are applied after classification to a QoS profile. The default PPP MRU is sufficient for a single level of tag nesting (where the frame contains two VLAN tags) between two Extreme switches; jumbo frame support must be enabled if higher levels of VLAN tag nesting are needed.

The DiffServ/RED functions are not performed by PoS ports when frames contain nested tags (in other words, more than one tag).

**Example**

The following command adds VLAN 140 to the frame for port 1 of the module installed in slot 8 for input frames from the PPP link:

```bash
configure dot1q tagnesting push 140 port 8:1 ingress
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure flowstats export add

configure flowstats export {<group#>} add [<ip address> | <hostname>] <udp_port>

**Description**
Configures the flow-collector devices to which NetFlow datagrams are exported.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export &lt;group#&gt;</td>
<td>Specifies a particular export distribution group on a per-filter basis. Identifies the set of flow collector devices to which records for flows matching the filter are to be exported.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the flow-collector destination.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the flow-collector destination.</td>
</tr>
<tr>
<td>udp_port</td>
<td>Specifies the UDP port number of the flow-collector destination.</td>
</tr>
</tbody>
</table>

**Default**
By default, no flow-collector destinations are configured.

**Usage Guidelines**
A flow-collector destination is identified by either an IP address and UDP port #, or by a hostname and UDP port #, to which NetFlow export datagrams are transmitted. The command allows flow-collector destinations to be added. Up to 8 flow-collector destinations can be configured for each group, and up to 32 groups can be defined per switch. The optional `group#` parameter, which identifies the specific group the destination is being configured for, is an integer in the range [1–32]. The `group#` defaults to 1 if the parameter is omitted. At least one flow-collector destination must be configured for NetFlow datagrams to be exported to a group.

When multiple flow-collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations. This NetFlow-distribution feature enables a scalable collection architecture that is able to accommodate high volumes of exported data. The distribution algorithm ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that flow records for both the ingress and egress directions of a TCP or UDP connection are exported to the same collector (when both flows traverse the same SONET link and both filters are configured to export to the same group).

**Example**
The following command adds a flow-collector destination of 10.1.1.88 for group 5 using UDP port 2025 to which NetFlow datagrams are exported:

```
configure flowstat export 5 add 10.1.1.88 2025
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.
Platform Availability

This command is available on the BlackDiamond switch only.
configure flowstats export delete

configure flowstats export {<group#>} delete [<ip address> | <hostname>] <udp_port>

Description
Configures the flow-collector devices to which NetFlow datagrams are exported.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>export &lt;group#&gt;</td>
<td>Specifies a particular export distribution group on a per-filter basis. Identifies the set of flow collector devices to which records for flows matching the filter are to be exported.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies the IP address of the flow-collector destination.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the host name of the flow-collector destination.</td>
</tr>
<tr>
<td>udp_port</td>
<td>Specifies the UDP port number of the flow-collector destination.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
A flow-collector destination is identified by either an IP address and UDP port #, or by a hostname and UDP port #, to which NetFlow export datagrams are transmitted. The command allows flow-collector destinations to be deleted. Up to 8 flow-collector destinations can be configured for each group, and up to 32 groups can be defined per switch. The optional group# parameter, which identifies the specific group the destination is being configured for, is an integer in the range [1–32]. The group# defaults to 1 if the parameter is omitted. At least one flow-collector destination must be configured for NetFlow datagrams to be exported to a group.

When multiple flow-collectors are configured as members of the same group, the exported NetFlow datagrams are distributed across the available destinations. This NetFlow-distribution feature enables a scalable collection architecture that is able to accommodate high volumes of exported data. The distribution algorithm ensures that all the records for a given flow are exported to the same collector. The algorithm also ensures that flow records for both the ingress and egress directions of a TCP or UDP connection are exported to the same collector (when both flows traverse the same SONET link and both filters are configured to export to the same group).

Example
The following command deletes a flow-collector destination of 10.1.1.88 for group 5 to which NetFlow datagrams are exported:

```
configure flowstat export 5 delete 10.1.1.88 2025
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.
Platform Availability

This command is available on the BlackDiamond switch only.
configure flowstats filter ports

configure flowstats filter <filter#> {aggregation} {export <group#>} ports <portlist> [ingress | egress] <filterspec>

Description
Configures a flow record filter for the specified SONET ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>filter#</td>
<td>The filter# parameter is an integer in the range from 1 to 8 that operates with either the ingress or egress keyword to identify the filter that is being defined.</td>
</tr>
<tr>
<td>aggregation</td>
<td>Reduces the volume of exported data, use this optional keyword to maintain a single set of statistics for all the flows that match the specified filter.</td>
</tr>
<tr>
<td>export &lt;group#&gt;</td>
<td>Specifies a particular export distribution group on a per-filter basis. Identifies the set of flow collector devices to which records for flows matching the filter are to be exported.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>ingress</td>
<td>Use this keyword to specify that the filter being defined in the command is one of the eight filters to be applied to ingress flows.</td>
</tr>
<tr>
<td>egress</td>
<td>Use this keyword to specify that the filter being defined in the command is one of the eight filters to be applied to egress flows.</td>
</tr>
</tbody>
</table>
| filterspec    | Each filter is defined using a value/filtermask pair for each of the five components in the following sequence: (destination IP address, source IP address, destination port number, source port number, protocol) in the form: [

{dest-ip <ipaddress_value/ipaddress_filtermask>}
{source-ip <ipaddress_value/ipaddress_filtermask>}
{source-port <port_value/port_filtermask>}
{protocol <protocol_value@protocol_filtermask>}

| match-all-flows | match-no-flows |

The ipaddress_filtermask, port_filtermask, and protocol_filtermask parameters are configured using hexadecimal notation. You can also use either the match-all-flows keyword or the match-no-flows keyword in place of settings for the five components. The match-all-flows keyword adjusts the value/filtermask settings for all the components to 0/0 such that the filter matches any flow. The match-no-flows keyword adjusts the value/filtermask settings for all the components such that the filter does not match any flow. |

Default
By default, filter#1 is configured to match-all-flows, and the remaining filters are configured to match-no-flows. The group# defaults to 1 if the parameter is omitted.
Usage Guidelines

The command allows a port to be configured to selectively maintain statistics for only those flows that match the specified filters. Sixteen filters are supported for each port, eight filters for ingress flows and another eight filters for egress flows. The filter# parameter and either the ingress or egress keyword are specified to identify the filter that is being configured. The filter# parameter is an integer in the range [1–8]. The filters are comprised of a value/filtermask pair for each component of the {destination IP address, source IP address, destination port number, source port number, protocol} 5-tuple. Conceptually, the filters work by ANDing the contents of each 5-tuple component of a forwarded flow with the associated masks from filter#1. Statistics are maintained if the results of the AND operations match the configured filter values for all fields of the 5-tuple. If there is no match, then the operation is repeated for filter#2, and so on. If there is no match for any of the filters, then statistics are not maintained for the flow. Filters for any/all of the 5-tuple components can be configured with a single command.

The filterspec parameter also supports the match-all-flows and match-no-flows keywords. The match-all-flows keyword adjusts the settings such that the filter matches any flow (that is, the value/filtermask pairs are set to 0/0 for all the 5-tuple components), while the match-no-flows keyword adjusts the settings such that the filter does not match any flow.

The optional aggregation keyword may be used to indicate that a single set of statistics is to be maintained for all the flows that match the filter, which can substantially reduce the volume of exported data. A particular export distribution group may also be specified on a filter-basis. The group# parameter identifies the set of collector devices that records for flows matching the filter are to be exported to.

Example

The following command example configures a filter to collect statistics on ingress flows destined for 192.168.1.1 from the 192.169.0.0/16 subnet with a destination port of 80 using protocol 6:

```
config flowstats filter 1 export 1 ports all ingress
   dest-ip 192.168.1.1/FFFFFFFF source-ip 192.169.0.0/FFFF0000
   dest-port 80/FFFF source-port 0/0 protocol 6/FF
```

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch only.
configure flowstats source ipaddress

configure flowstats source ipaddress <ip address>

Description
Configures the IP address that is to be used as the source IP address for NetFlow datagrams to be exported.

Syntax Description

| ip address | Specifies the source IP address to be used as the source for NetFlow datagrams to be exported. |

Default
Normal.

Usage Guidelines
No NetFlow datagrams will be exported until the source ip address is configured. Flow-collector devices may use the source IP address of received NetFlow datagrams to identify the switch that sent the information. It is recommended that the configured ip address be associated with a VLAN that has loopback mode enabled.

Example
The following command example specifies that the IP address 192.168.100.1 is to be used as the source IP address for exported NetFlow datagrams:
configure flowstats source ipaddress 192.168.100.1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20 for the PoS module only.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ports tunnel hdlc

configure ports <portlist> tunnel hdlc [off | mpls]

Description
Enables tunneling for HDLC encapsulated frames from a SONET port through an MPLS network.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the SONET port number(s).</td>
</tr>
<tr>
<td>off</td>
<td>Disables HDLC tunneling.</td>
</tr>
<tr>
<td>mpls</td>
<td>Enables an MPLS TLS-tunnel.</td>
</tr>
</tbody>
</table>

Default
The default is off.

Usage Guidelines
The ingress SONET port encapsulates the entire HDLC frame (including the HDLC header and FCS) inside an Ethernet/MPLS header. The egress SONET port strips the Ethernet/MPLS header and forwards the HDLC frame. HDLC idle bytes (x7E) are not tunneled, but runts and aborted frames are. HDLC control bytes are destuffed on ingress and stuffed on egress.

When a SONET port is configured for HDLC tunneling, PPP should not be configured on the port (BCP and IPCP should be off). Furthermore, the port should be the only port in a VLAN and a MPLS TLS-tunnel should be configured for this VLAN. The payload inside HDLC could be PPP or some other HDLC-encapsulated protocol. SONET APS (automatic protection switching) is supported between tunneled PoS ports on the same module or different modules in the same switch. APS for tunneled ports is not supported for ports on different switches.

Example
The following command example configures an HDLC tunnel, and applies to a PoS module installed in slot 1 of a BlackDiamond switch:

```
configure ports 1:4 tunnel hdlc mpls
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ppp ports

configure ppp [bcp [on | off] | ipcp [on {peer-ipaddress <ip address>} | off]] ports <portlist>

Description
Configures the network control protocol that will run on the specified PPP ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bcp</td>
<td>Specifies bridging control protocol for the port.</td>
</tr>
<tr>
<td>ipcp</td>
<td>Specifies IP control protocol for the port.</td>
</tr>
<tr>
<td>on</td>
<td>Enables the designated protocol on the port.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the designated protocol on the port.</td>
</tr>
<tr>
<td>peer-ipaddress</td>
<td>Allows you to configure IP address of the peer router.</td>
</tr>
<tr>
<td>ip address</td>
<td>Specifies IP address of the peer router.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
By default, BCP is enabled on all PoS ports. (However, ports 2 and 4 of OC-3c modules are not members of any VLANs by default; all other ports are members of the default VLAN by default.)

Usage Guidelines
The bcp keyword represents the bridging control protocol (BCP), and the ipcp keyword represents the IP control protocol. IPCP and BCP are mutually exclusive configuration options for a given port (that is, they cannot both be enabled simultaneously on the same port). Generally, when IPCP is enabled on a port, the port must be a member of one and only one VLAN. Furthermore, no other ports can be members of this VLAN, and IP routing is the only protocol supported on the VLAN. The one exception to this rule occurs when SONET automatic protection switching (APS) is enabled. A single VLAN can contain two IPCP-enabled ports if they are members of the same APS group.

The peer-ipaddress keyword provides an option to configure the IP address of the peer router. This can be useful with peer routers that do not advertise their IP address using the IPCP IP address configuration option (for example, Juniper routers). If the peer router does advertise an IP address via IPCP, the configured peer-ipaddress is ignored.

BCP enables Ethernet MAC frames to be transported across a PPP link. Thus, any protocol can be transported across a BCP connection. Essentially, BCP enables the PPP link to appear as an Ethernet LAN segment to the rest of the switch. Therefore, the port may be a member of multiple VLANs, and frames can be either bridged or routed onto the link. There are restrictions regarding which ports can be bridged together (in other words, they may be members of the same VLAN) on the OC-3 PoS Module. Ports 1 and 2 on the same OC-3 module cannot be bridged together (unless they are members of the same APS group). Additionally, ports 3 and 4 on the same OC-3 module cannot be bridged together (unless they are members of the same APS group). There are no similar restrictions regarding bridging ports together on the OC-12 PoS Module.

PoS operation requires at least one Ethernet I/O module be operational in the chassis. IPCP cannot be enabled on a port unless BCP is off, and vice versa. IPCP is recommended when a PoS port only carries
routed IP traffic (because IPCP imposes less header overhead, the maximum link throughput is higher than with BCP).

**Example**

The following command example configures BCP on the PPP port, and applies to a PoS module installed in slot 1 of a BlackDiamond switch:

```plaintext
configure ppp bcp off port 1:4
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.
configure ppp authentication ports

configure ppp authentication [off | chap | pap | chap-pap] ports <portlist>

Description
Configures authentication on the specified PPP ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Disables authentication</td>
</tr>
<tr>
<td>chap</td>
<td>Authenticates the peer using the challenge handshake authentication protocol (CHAP).</td>
</tr>
<tr>
<td>pap</td>
<td>Authenticates the peer using the password authentication protocol.</td>
</tr>
<tr>
<td>chap-pap</td>
<td>Specifies that either CHAP or PAP may be used to authenticate the peer.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default is authentication off.

Usage Guidelines
When off is specified, the peer is not authenticated. When chap is specified, the peer is authenticated using the challenge handshake authentication protocol (CHAP). When pap is specified, the peer is authenticated via the password authentication protocol (PAP). Specification of chap-pap indicates that either CHAP or PAP may be used to authenticate the peer.

Example
The following command example turns on CHAP authentication for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```bash
cfg_ ppp authentication chap ports 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.
configure ppp delayed-down-time ports

configure ppp delayed-down-time <seconds> ports <portlist>

Description
Configures the delayed-down-time interval used by PPP for the specified ports.

Syntax Description

| seconds | Specifies interval for delayed-down-time in seconds. |
| portlist | Specifies the port number(s). |

Default
The default value is 1 second.

Usage Guidelines
The delayed-down-time interval is the amount of time that PPP waits before declaring a port down after a physical link failure has been detected. A non-zero value is useful when recovery from the link failure is fast (for example, when APS is enabled on a SONET port). In this case, APS may be able to recover from the link failure fast enough that there is no need to perturb the logical connection with the peer PPP entity, which minimizes network down time. A non-zero value is desirable when APS is configured at either end of the link. The delayed-down-time parameter is configured in seconds, with a valid range of [0–20].

Example
The following command example sets the delayed-down-time interval to 2 seconds for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp delayed-down-time 2 ports 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ppp echo ports

    configure ppp echo [<seconds> <consecutive_misses> | off] ports <portlist>

Description
Configures the link maintenance protocol on the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>seconds</td>
<td>Specifies the amount of time in seconds between transmissions of echo-request packets.</td>
</tr>
<tr>
<td>consecutive_misses</td>
<td>Controls the amount of time that PPP waits for a reply.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the link maintenance protocol.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The link maintenance protocol is off by default.

Usage Guidelines
When link maintenance is enabled and the port is receiving no packets, echo-request packets are transmitted over the link on a periodic basis. The seconds parameter in an integer in the range [1–300] that specifies the amount of time between transmissions of echo-request packets. The consecutive_misses parameter is an integer in the range [1–100] that controls the amount of time that PPP waits for a reply. If an echo-reply is not received within an interval of duration (consecutive_misses * seconds) seconds, the link is brought down. The link maintenance protocol may be disabled using the off keyword.

Example
The following example enables link maintenance on port 1 of a PoS module in slot 8 and sets seconds to 3 and consecutive misses to 10:
config ppp echo 3 10 ports 8:1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ppp pos checksum ports

    configure ppp pos checksum [32 | 16] ports <portlist>

Description
Configures the size of the HDLC Frame Check Sequence (FCS) to be used on the specified SONET ports.

Syntax Description

| 16 or 32 | Specifies the size of the HDLC frame check sequence (either 32 bits or 16 bits). |
| portlist | Specifies the port number(s). |

Default
The default is a 32-bit FCS.

Usage Guidelines
The two choices are a 32-bit FCS or a 16-bit FCS. RFC 2615 recommends that a 32-bit FCS be used.

Example
The following command example sets the FCS to 16 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

    config ppp pos checksum 16 ports 8:1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ppp pos scrambling ports

configure ppp pos scrambling [on | off] ports <portlist>

Description
Specifies whether the payload data should be scrambled on the specified ports. RFC 2615 recommends that the SONET payload be scrambled.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>on</td>
<td>Enables scrambling.</td>
</tr>
<tr>
<td>off</td>
<td>Disables scrambling.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default is scrambling on.

Usage Guidelines
The option of disabling scrambling is provided for backward compatibility with an earlier (now obsoleted) PoS standard specified in RFC 1619. Scrambling was introduced in RFC 2615 to alleviate potential security problems where malicious users might generate packets with bit patterns that create SONET synchronization problems.

Example
The following command example turns off the scrambling function for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config ppp pos scrambling off ports 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ppp quality ports

configure ppp quality [off | <required_percent> {<seconds>}] ports <portlist>

Description
Configures the Link Quality Monitoring (LQM) protocol on the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Disables link quality monitoring protocol.</td>
</tr>
<tr>
<td>required_percent</td>
<td>Specifies required link drop percentage for link quality management (LQM).</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies how often (in seconds) the quality reports are to be received from</td>
</tr>
<tr>
<td></td>
<td>the peer LQM entity.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default value of seconds is 30. By default, LQM is off.

Usage Guidelines
LQM periodically transmits counts of packets/octets that were transmitted, along with counts of packets/ octets that were successfully received. This information enables LQM to determine the percentage of data that is being dropped due to poor link quality. If the drop percentage is greater than (100 - required_percent), all network-layer protocols running over the link are brought down. You may want to bring a poor-quality link down when an alternate network path exists, or when billing is based on the amount of data transmitted. The required_percent parameter is an integer in the range [1–99]. The seconds parameter is an integer in the range [1–300] that determines how often quality reports are to be received from the peer LQM entity (that is, the reporting interval). Specifying the seconds parameter is optional. It can take up to seven reporting intervals for LCP to bring a link down. If the link quality subsequently improves, LCP will automatically bring the link back up; this type of service restoration will take a minimum of 7 reporting intervals.

Example
The following example enables the LQM protocol on port 1 of a PoS module in slot 3 and sets required_percent to 95. Because no value is specified for the optional seconds parameter, the command uses the default of 30 seconds:

```
config ppp quality 95 ports 3:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure ppp user ports

configure ppp user <name> {encrypted} {<password>} ports <portlist>

Description
Configures the user name and password that the specified PPP port uses in the event the PPP peer requests authentication.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies user name for PPP peer authentication requests.</td>
</tr>
<tr>
<td>encrypted</td>
<td>This parameter option should not be entered.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for PPP peer authentication requests.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default value of both name and password is extreme.

Usage Guidelines
The name is also sent when a port transmits a CHAP authentication request. The implementation responds to either CHAP or PAP authentication requests issued by the peer regardless of whether the port is configured to authenticate the peer. The name parameter is a string with a length in the range of [1–32] characters. The password parameter is also a character string, with a maximum length of 32 characters. If no password is provided on the command line, then you are prompted to enter the password twice (with the second time serving as a confirmation). You should not enter the encrypted parameter option (it is used by the switch when generating an ASCII configuration).

Example
The following command example sets the name to titus and sets the password to 1Afortune for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

config ppp user "titus" "1Afortune" ports 8:1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the on the BlackDiamond switch. A similar command is available on the Alpine switch.
**configure qosprofile**

```
configure qosprofile <qosprofile> {minbw <percent>} {maxbw <percent>} {priority <level>} {minbuf <percent>} {maxbuf <percent>} {<portlist>} {egress | ingress}
```

**Description**

Configures a QoS profile.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qosprofile</td>
<td>Specifies the QoS profile to be configured.</td>
</tr>
<tr>
<td>minbw</td>
<td>Specifies the minimum percentage of the bandwidth available for transmissions from the profile.</td>
</tr>
<tr>
<td>maxbw</td>
<td>Specifies the maximum percentage of the bandwidth that can be used for transmissions from the profile.</td>
</tr>
<tr>
<td>priority</td>
<td>Specifies which traffic is scheduled when bandwidth is still available after the minimum requirements of all profiles have been satisfied.</td>
</tr>
<tr>
<td>level</td>
<td>Specifies the priority level (low, lowHi, normal, normalHi, medium, mediumHi, high, or highHi).</td>
</tr>
<tr>
<td>minbuf</td>
<td>This keyword is not applicable to SONET ports.</td>
</tr>
<tr>
<td>maxbuf</td>
<td>This keyword is not applicable to SONET ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>egress</td>
<td>Specifies that the flow is from the SONET port.</td>
</tr>
<tr>
<td>ingress</td>
<td>Specifies that the flow is to the SONET port.</td>
</tr>
</tbody>
</table>

**Default**

Normal.

**Usage Guidelines**

The optional egress and ingress keywords have been added to support the PoS module. These new keywords are currently only applicable to PoS ports. The PoS modules support eight egress queues and eight ingress queues per port, and the scheduling parameters for these queues are controlled by QoS profiles qp1-qp8 (in other words, queue #0 is controlled by qp1, queue #1 by qp2, and so on). The portlist parameter allows QoS profiles to be customized on a SONET-port basis, while the egress and ingress keywords enable even finer customization (down to a particular egress or ingress queue on a given port). If the egress and ingress keywords are omitted, then the configured parameters apply to the egress queue associated with the specified qosprofile.

The minbw parameter is an integer in the range [0–100] that specifies the minimum percentage of the bandwidth that must be available for transmissions from the profile. The sum of the minbw parameters across all eight profiles cannot exceed 90%.

The maxbw parameter is also an integer in the range [1–100] that specifies the maximum percentage of the bandwidth that can be used for transmissions from the profile. The priority level may be set to low, lowHi, normal, normalHi, medium, mediumHi, high, or highHi. The priority determines which traffic is scheduled when bandwidth is still available after the minimum requirements of all profiles have been satisfied.
The `minbuf` and `maxbuf` keywords are not applicable to PoS ports.

**Example**
The following command configures the QoS profile in the egress direction, with a minimum bandwidth of 10 percent and a maximum of 20 percent:

```
config qosprofile qp8 minbw 10 maxbw 20 2:1-2:2 egress
```

**History**
This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support the PoS module.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure red

configure red [drop-probability | low-drop-probability | high-drop-probability] <percent> {ports <portlist>}

**Description**
Configures the RED drop probability for a specified port.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>drop-probability</td>
<td>Specifies both the high and low drop probability rates.</td>
</tr>
<tr>
<td>low-drop-probability</td>
<td>Sets the low drop probability rate.</td>
</tr>
<tr>
<td>high-drop-probability</td>
<td>Sets the high drop probability rate.</td>
</tr>
<tr>
<td>percent</td>
<td>Specifies the percentage for the drop probability.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

**Default**
For PoS ports, both the low and high drop-probabilities default to 10%.

**Usage Guidelines**
The optional **low-drop-probability**, **high-drop-probability**, and **ports** keywords have been added to support the PoS module. Currently, these new keywords are only supported for SONET ports. Omission of the **ports** keyword indicates that the setting is to be applied to all ports.

The drop probability is specified as a percentage, where the **percent** parameter is an integer in the range [1–100]. The implementation provides weighted RED (WRED) functionality via support for two different drop probabilities: a low-drop-probability and a high-drop-probability. The DSCPs of IP packets indicate whether the packet should be dropped with low probability or high probability, and the appropriate percentage is then applied if WRED is active. WRED is only applied to IP packets, and the **configure diffserv examination code-point** command supports complete flexibility in assigning DSCPs to the two different drop-probability levels. The configured mapping of DSCPs to drop-probability levels is used by WRED even if **diffserv examination** is disabled on the port.

The **drop-probability** keyword indicates that the specified percentage should be used for both the low and high drop-probabilities, which effectively disables WRED and reverts to standard RED operation. RED is active when the average queue length is between the minimum and maximum thresholds. In this region, the probability that a given packet is dropped increases linearly up to the configured drop probability at the maximum threshold. All packets are dropped when the average queue length exceeds the maximum threshold.

**Example**
The following command configure a RED high drop-probability of 20% on the SONET ports:

```plaintext
config red high-drop-probability 20 ports 2:1-2:2
```
History
This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

Platform Availability
This command is available on the BlackDiamond switch only.
configure red min-threshold ports

   configure red min-threshold <percent> ports <portlist>

Description
Configures the minimum queue length threshold for RED operation on the specified PoS ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>percent</td>
<td>Specifies the percentage for the minimum queue length threshold for RED operation.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
By default, min-threshold is 10% for PoS ports.

Usage Guidelines
When this threshold is exceeded, the RED algorithm is activated. Currently, the command is only applicable to PoS ports. The ports keyword allows the threshold parameter to be configured on a PoS-port basis. The min-threshold is specified as a percentage, where the percent parameter is an integer in the range [1–100]. For PoS ports, the minimum threshold is a percentage of 1000 packet buffers, and the maximum threshold is set to minimum ((3 * minimum threshold buffers), maximum available buffers). The settings for both the minimum and maximum thresholds, in terms of number of buffers, are displayed by the show ports info command.

Example
The following command configures minimum queue length threshold of 50 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
configure red min-threshold 50 port 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure sonet clocking ports

configure sonet clocking [line | internal] ports <portlist>

**Description**

Configures the clocking source for the specified SONET ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>Sets the line clocking on the specified port.</td>
</tr>
<tr>
<td>internal</td>
<td>Sets internal clocking on the specified port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

**Default**

The default setting is internal.

**Usage Guidelines**

The clock is recovered from the received bitstream when line clocking is configured.

**Example**

The following command example selects line clocking for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet clocking line ports 8:1
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure sonet framing ports

configure sonet framing [sonet | sdh] ports <portlist>

Description
Configures the framing type for the specified SONET ports.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>sonet</td>
<td>Sets the framing type to SONET.</td>
</tr>
<tr>
<td>sdh</td>
<td>Sets the framing type to SDH.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default setting is sonet.

Usage Guidelines
You can configure each port for framing that complies with either the SONET standard or the SDH standard. SONET is primarily an American standard; SDH is the international version.

Example
The following command example selects SDH framing for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet framing sdh ports 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure sonet loop

configure sonet loop [internal | line | off] ports <portlist>

Description
Configures loopback options for the specified SONET port(s).

Syntax Description

<table>
<thead>
<tr>
<th>internal</th>
<th>Sets the signal to be looped back onto the receive interface.</th>
</tr>
</thead>
<tbody>
<tr>
<td>line</td>
<td>Sets the signal to be looped back onto the transmit interface.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the loopback setting. Default is off.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default setting is off.

Usage Guidelines
SONET loopback is only available on OC-12 ports. Configuring loopback on a SONET port may be useful for diagnostics or network troubleshooting. When internal loopback is configured, the transmitted signal is looped back onto the receive interface. When line loopback is configured, the received signal is looped back onto the transmit interface.

Example
The following command configures loopback on SONET port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet loop internal ports 8:1
```

History
This command was first available in ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure sonet signal label ports

configure sonet signal label [auto | <hex_octet>] ports <portlist>

Description
Configures the signal label value for the specified SONET ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Enables the signal label field to be automatically set.</td>
</tr>
<tr>
<td>hex_octet</td>
<td>Allows you to set the signal label field to a particular hex octet value.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

Default
The default is auto, where the value of the signal Label field is automatically set based on standard conventions for the given payload type.

Usage Guidelines
The signal label field occupies one byte of the path overhead associated with each SONET frame. It is used to indicate the type of contents carried in the SPE. For example, 0x16 indicates scrambled PPP/HDLC, while 0xCF indicates unscrambled PPP/HDLC. The default may be overridden by specifying a particular hex octet that is to be used instead, where hex octet is a hexadecimal integer in the range [0–xFF]. It may be necessary to specify a particular hex octet in order to interoperate with implementations that do not follow the standard conventions for the signal label field.

Example
The following command example sets the Signal Label to the hexadecimal value CF for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```bash
config sonet signal label CF ports 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure sonet threshold signal degrade ports

    configure sonet threshold signal degrade <error_rate> ports <portlist>

**Description**

Configures the signal degrade threshold for the specified SONET ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>error_rate</td>
<td>Sets the threshold for the bit error rate for the SONET line.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

**Default**

The default is $10^{-6}$.

**Usage Guidelines**

A signal degrade (SD) event is generated if the bit error rate (BER) for the SONET line exceeds the configured threshold. If automatic protection switching (APS) is enabled on the port, a SD event will initiate a line switch. The `error_rate` parameter is an integer in the range [5-9], where the SD BER is $10^{-error_rate}$. The default value of the `error_rate` parameter is 6, which equates to a SD BER of $10^{-6}$, or 1 per million.

**Example**

The following command example sets the Signal Degrade threshold value to 8 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```plaintext
config sonet threshold signal degrade 8 ports 8:1
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure sonet threshold signal fail ports

configure sonet threshold signal fail <error_rate> ports <portlist>

Description
Confugures the signal failure threshold for the specified SONET ports.

Syntax Description

| error_rate | Sets the signal failure threshold for the SONET ports. |
| portlist   | Specifies the port number(s).                        |

Default
The default is $10^{-5}$.

Usage Guidelines
A signal failure (SF) event is generated if the bit error rate (BER) for the SONET line exceeds the configured threshold. A SF event brings the port down. If automatic protection switching (APS) is enabled on the port, a SF event will initiate a line switch. The error_rate parameter is an integer in the range [3-5], where the SF BER is $10^{-error_rate}$. The default value of the error_rate parameter is 5, which equates to a SF BER of $10^{-5}$, or 1 per hundred thousand.

Example
The following command example sets the signal fail threshold value to 3 for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```bash
config sonet threshold signal fail 3 ports 8:1
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
configure sonet trace path ports

```
configure sonet trace path <id_string> ports <portlist>
```

**Description**
Configures the path trace identifier string for the specified SONET ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>id_string</th>
<th>Specifies the path trace identifier string for the SONET ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

**Default**
The default is null.

**Usage Guidelines**
Path trace is a maintenance feature of SONET. One byte of the path overhead associated with each SONET frame is used to carry information identifying the originating path terminating equipment (PTE). The `id_string` parameter is a string that may contain up to 64 characters (which always includes a carriage return and a line feed character at the end). By default, `id_string` contains an IP address assigned to the VLAN that the port is a member of. This IP address is represented in dotted-decimal notation. If no IP address is assigned to the port's VLAN, `id_string` defaults to a string of 64 NULL characters. When SONET framing is configured, a 64-character string is repetitively transmitted, one character per frame. If the configured string is less than 64 characters, it is padded with NULL characters. Operation is similar when SDH framing is configured, except that the maximum string length is 15 characters. If necessary, the configured `id_string` is truncated to 15 characters.

**Example**
The following command example sets the path trace identifier to the string `parador` for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet trace path parador ports 8:1
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure sonet trace section ports

    configure sonet trace section [id_byte | string id_string]
    ports <portlist>

**Description**

Configures the section trace identifier for the specified SONET ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id_byte</td>
<td>Configures the ID byte section trace identifier for the specified SONET port.</td>
</tr>
<tr>
<td>id_string</td>
<td>Configures the ID string section trace identifier for the specified SONET port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
</tbody>
</table>

**Default**

The default is 1 for SONET, null for SDH.

**Usage Guidelines**

Section trace is a maintenance feature of SONET. One byte of the section overhead associated with each SONET frame is used to carry information identifying the transmitting equipment. The section trace identifier has two forms: an id_byte and an id_string. The id_byte parameter is an integer in the range [0-255], with a default value of 1. The id_string parameter is a string that may contain up to 15 characters. By default, id_string contains 15 NULL characters. The id_byte parameter is only applicable when SONET framing is configured. In this case, the configured id_byte value is transmitted in each SONET frame. Analogously, the id_string parameter is only applicable when SDH framing is configured. SDH framing repetitively cycles through a 15-character string, sending one character per frame. If the configured string is less than 15 characters, it is padded with NULL characters.

**Example**

The following command example sets the section trace identifier to the string 1800wombat for port 1 of the PoS module installed in slot 8 of the BlackDiamond switch:

```
config sonet trace section string 1800wombat ports 8:1
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only.
create account pppuser

create account pppuser <username> {encrypted} {<password>}

Description
Creates a local database entry that can be used to authenticate a PPP peer.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Specifies the user name used for authentication.</td>
</tr>
<tr>
<td>encrypted</td>
<td>This parameter should not be used with SONET ports.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password used for authentication.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Authentication responses include a username. When a response is received, the database is searched for an entry with the specified username. The associated password is then used to validate the authentication response. This is a new application of the existing `create account` command. The `pppuser` keyword is new. The `username` parameter is a string with a length in the range [1-32] characters. The `password` parameter is also a character string, with a maximum length of 32 characters. If no password is provided on the command line, then you are prompted to enter the password twice (with the second time serving as a confirmation). You should not enter the `encrypted` parameter option (it is used by the switch when generating an ASCII configuration).

Example
The following command example sets the authentication database name to `stretch` and sets the password to `baserunner` for the BlackDiamond switch:

```
create account pppuser stretch baserunner
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch. A similar command is available on the Alpine switch.
create aps

create aps <group#>

**Description**

Creates an APS group with the specified group number.

**Syntax Description**

<table>
<thead>
<tr>
<th>group#</th>
<th>Specifies the APS group# to which the command applies.</th>
</tr>
</thead>
</table>

**Default**

N/A.

**Usage Guidelines**

You specify the `group#` parameter, which is an integer in the range [1-65535]. The `group#` is used to identify the APS group. An APS group includes one working line and one protection line. The working line and protection line can reside on the same BlackDiamond switch or two different BlackDiamond switches. The group numbers must be unique across all BlackDiamond switches that are cooperating to provide the APS function. The group numbers must also be used in a consistent manner across BlackDiamond switches. For example, if the working line is assigned to `group#` 1 on BlackDiamond #1, and the associated protection line resides on BlackDiamond #2, then the protection line must also be assigned to group #1 on BlackDiamond #2. The `group#` is used to identify the partner (in other words, working or protection) line in Ethernet messages exchanged by BlackDiamond switches that are cooperating to provide the APS function.

**Example**

The following command example creates APS group 1001 on the BlackDiamond switch:

```
create aps 1001
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only.
delete account pppuser

   delete account pppuser <username>

Description
Deletes an entry in the local PPP authentication database.

Syntax Description

| username | Specifies the user name used for authentication. |

Default
N/A.

Usage Guidelines
Deletes a user from the PPP authentication database. Existing links already authenticated are not affected by this command.

Example
The following command example removes the entry for stretch from the authentication database:

delete account pppuser stretch

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch. A similar command is available on the Alpine switch.
delete aps

    delete aps <group#>

Description
Deletes the specified APS group.

Syntax Description

| group# | Specifies the APS group# to which the command applies. |

Default
N/A.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group to delete.

Example
The following command example deletes APS group 1001:

delete aps 1001

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
**disable aps**

**Description**
Disables the APS function for an entire switch.

**Syntax Description**
This command has no arguments or variables.

**Default**
APS is disabled by default.

**Usage Guidelines**
If APS is disabled, interfaces configured as protection lines will not carry any traffic.

**Example**
To disable the APS function for the entire switch, use the following command:
```
disable aps
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**
This command is available on the BlackDiamond switch only.
disable red ports queue

\[ \text{disable red ports } \text{<portlist>} \text{ queue } \text{<queue#>} \]

**Description**
Disables RED on the specified ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>queue#</th>
</tr>
</thead>
<tbody>
<tr>
<td>Specifies the port number(s). May be in the form 1, 2, 3-5, 2-5, 2-6-8.</td>
<td>Specifies the queue for which the RED function is disabled. This parameter is supported for the PoS module only.</td>
</tr>
</tbody>
</table>

**Default**
Disabled.

**Usage Guidelines**
The queue keyword has been added to support the PoS module. Currently, this new keyword is only applicable to PoS ports. The keyword allows the RED function to be selectively enabled on an individual queue basis. The queue# parameter is an integer in the range [0-7]. If the queue keyword is omitted, then the command applies to all egress queue numbers for the PoS port(s). RED is not supported on the ingress queues.

**Example**
The following command disables RED for all PHBs except the EF PHB:

disable red ports 2:1-2:2 queue 8

**History**
This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

**Platform Availability**
The general form of this command is available on all platforms. The optional queue parameter is available only on the PoS module on a BlackDiamond switch.
enable aps

enable aps

Description
Enables the APS function for an entire switch.

Syntax Description
This command has no arguments or variables.

Default
APS is disabled by default.

Usage Guidelines
If APS is enabled, interfaces configured as protection lines can carry traffic.

Example
To enable the APS function for the entire switch, use the following command:

```
enable aps
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
enable red ports queue

   enable red ports <portlist> queue <queue#>

**Description**

Enables RED on the specified PoS ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>queue#</td>
<td>Specifies the queue for which the RED function is enabled.</td>
</tr>
</tbody>
</table>

**Default**

By default, RED is disabled.

**Usage Guidelines**

The `queue` keyword has been added to support the PoS module. Currently, this new keyword is only applicable to PoS ports. The keyword allows the RED function to be selectively enabled on an individual queue basis. The `queue#` parameter is an integer in the range [0-7]. If the `queue` keyword is omitted, then the command applies to all egress queue numbers for the PoS port(s). (RED is not supported on the ingress queues.)

**Example**

The following command enables RED for all PHBs except the EF PHB:

```
enable red ports 2:1-2:2
```

**History**

This command was modified in an ExtremeWare IP Technology Services Release based on v6.1.5b20 to support PoS modules.

**Platform Availability**

The general form of this command is available on all platforms. The optional queue parameter is available only on the PoS module on a BlackDiamond switch.
show accounts pppuser

Description
Display the PPP user accounts database.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
Use this command to examine the entries in the PPP user accounts database, used for authentication when a link is initiated from a remote peer.

Example
The following command displays the PPP accounts database:
show accounts pppuser

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.
**show aps**

`show aps {<group#>} {detail}`

**Description**
Displays APS group status information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>group#</td>
<td>Specifies the APS group# to which the command applies.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays more detailed status information for the APS groups.</td>
</tr>
</tbody>
</table>

**Default**
By default, the command shows summarized status for the APS group(s).

**Usage Guidelines**
The user can optionally specify a `group#` parameter, which is an integer in the range [1-65535]. The `group#` identifies a particular APS group for which status is to be shown. Alternatively, you can enter `show aps` with no parameters to obtain status for all configured APS groups. More detailed status information can be obtained for the APS group(s) by specifying the detail parameter.

Summary status includes the following information for each APS group:

- Provisioned values of all APS configuration parameters, including SONET port numbers and whether the ports are performing the working or protection line function.
- An indication of whether the line associated with each configured port is active or inactive from an APS perspective, along with a timestamp indicating when the last APS state change occurred.
- An indication of whether a signal fail (SF) or signal degrade (SD) event due to an excessive bit error rate (BER) currently exists on the line associated with each configured port, along with a timestamp indicating when the last such error occurred. (Note that the BER thresholds that cause SF and SD events may be specified as part of configuring a SONET port.)
- Counts of the number of SF and SD events initiated by each configured port due to an excessive BER.
- Count of the number of APS authentication failures (that is, a count of the number of received APS control packets that have been discarded due to authentication failures).

Detailed status includes the information reported in the summary status along with additional status and management counters. Detailed status only applies to ports performing the protection line function.

Detailed management counters reported for each protection-line port include:

- Automatic line switches initiated by working-line switch
- Automatic line switches initiated by protection-line switch
- Automatic line switches initiated by ADM
- Line switches initiated due to external commands (for example, force or manual switch command)
- Line switches completed successfully
- Hello protocol failures (this count is included as a component of the automatic line switches initiated by protection-line switch counter)
- APS mode mismatch failures (occurs when the ADM indicates that it is provisioned for the \( 1:n \) APS architecture, or when the ADM indicates that it is provisioned for unidirectional-switching mode)
- Protection switching byte failures (occurs when the received K1 byte is either inconsistent or contains an invalid request code)
- Channel mismatch failures (occurs when the channel number in the transmitted K1 byte does not match the channel number in the received K2 byte)
- Far-end protection line failures (occurs when a signal fail request code is received on the protection line)

Additional detailed status information reported for each protection-line port includes:
- Current contents of received K1 and K2 bytes
- Contents of K1 and K2 bytes that are currently being transmitted
- An indication of whether an APS mode mismatch failure is currently active
- An indication of whether a protection switching byte failure is currently active
- An indication of whether a channel mismatch failure is currently active
- An indication of whether a Far-end protection line failure is currently active

**Example**

The following command displays APS group status information:

```
show aps
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**

This command is available on the BlackDiamond switch only.
show flowstats

show flowstats {<portlist> | export {<group#>} {detail}}

Description
Displays status information for the flow statistics function.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>export</td>
<td>Displays status information for export groups, which are configured on a switch-wide basis.</td>
</tr>
<tr>
<td>group#</td>
<td>Use this optional parameter with the export keyword to display status information for a specific export group. If you do not specify a value for the group# parameter, the export keyword by itself displays status information for all export groups.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays detailed export group status information.</td>
</tr>
</tbody>
</table>

Default
By default, the command shows summarized status.

Usage Guidelines
The portlist parameter can be used to specify the SONET port(s) for which status is to be shown. Alternatively, you can specify the export keyword to obtain status for export groups, which are configured on a switch-wide basis. Status can be obtained for a specific export group, identified by the group# parameter, or for all export groups by omitting the group# parameter. Status can be obtained for all ports by omitting both the portlist parameter and the export keyword (in other words, by simply entering show flowstats with no parameters). More detailed export group status information may be obtained by specifying the detail parameter.

Summary status for a port includes the following information:
- Values of all flow statistics configuration parameters
- Count of flow records that have been exported
- Counts of the number of packets/bytes for which flow statistics were not maintained due to insufficient resources

Summary status for an export group port includes the following information:
- Values of all configuration parameters
- State of each export destination device

Detailed status for an export group includes the information reported in the summary status along with the following additional management counters:
- Counts of flow records that have been exported to each flow-collector destination
- Counts of the number of times each flow-collector destination has been taken out of service due to health-check failures
Example
The following command displays status information for the flow statistics function:
show flowstats

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
show ppp

    show ppp {<portlist>} {detail}

Description
Displays status information for PPP ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>detail</td>
<td>Displayed more detailed status information for the PPP ports.</td>
</tr>
</tbody>
</table>

Default
By default, the command shows summarized status for the PPP port(s).

Usage Guidelines
The portlist parameter can be used to specify the port(s) for which status is to be shown. Alternatively, you can enter show ppp with no parameters to obtain status for all PPP ports. More detailed status information can be obtained for the PPP port(s) by specifying the detail parameter.

Summary status includes the following information for each PPP port:
- Values of all PPP configuration parameters
- Physical link status
  - operational
  - down
- LCP state
- IPCP/BCP state
- EDPCP state
- MPLSCP state
- OSINLCP state
- link packet and octet counters

Detailed status includes the information reported in the summary status along with the following additional status and management counters:
- Detailed link status
  - PPP link phase
- Detailed LCP status
  - LCP options negotiated (local and remote)
  - LCP packet counters
  - number of link-down events due to PPP maintenance
- Detailed authentication status
— remote username (if applicable)
— CHAP/PAP packet counters

- Detailed IPCP/BCP status
  — options negotiated (local and remote)
  — packet counters
  — MPLSCP/OSINLCP status

- Detailed LQM status
  — statistics from last received LQR (Link Quality Report)
  — time since last received LQR
  — LQR packet counters
  — number of link-down events due to LQM
  — MPLSCP
  — OSINLCP

**Example**
The following command displays status information for the PPP ports:

```
show ppp
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

**Platform Availability**
This command is available on the BlackDiamond switch only. A similar command is available on the Alpine switch.
show sonet

    show sonet {<portlist>} {detail}

Description
Displays SONET port status.

Syntax Description

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>detail</td>
<td>Displays more detailed status information for the ports.</td>
</tr>
</tbody>
</table>

Default
By default, the command shows summarized status for the port(s).

Usage Guidelines
You can use the portlist parameter to specify which SONET port(s) you want to display the status for. You can also omit the portlist parameter to obtain status for all SONET ports. More detailed status information can be obtained for the port(s) by specifying the detail parameter. Summary status includes the following information for each port:

- Values of all port configuration parameters
- State of the port
- Identification of all currently active events

Example
The following command displays the SONET port status:

    show sonet

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
unconfigure aps

    unconfigure aps <group#>

Description
Resets the APS group configuration parameters to their default values.

Syntax Description

| group# | Specifies the APS group# to which the command applies. |

Default
N/A.

Usage Guidelines
You specify the group# parameter, which is an integer in the range [1-65535]. The group# identifies the APS group that the command applies to. The command does not affect the ports that have been added to the APS group. The command does cancel any outstanding lockout, force, or manual switch requests.

Example
The following command example resets the configuration parameters of APS group 1001 to their default values:

    unconfig aps 1001

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
unconfigure diffserv dscp-mapping ports

    unconfigure diffserv dscp-mapping ports <portlist>

**Description**

Resets the DSCP mapping tables for the specified PoS ports to their default values.

**Syntax Description**

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies the port number(s).</th>
</tr>
</thead>
</table>

**Default**

N/A.

**Usage Guidelines**

Three DSCP mapping tables are supported per SONET port. One of the tables is used in the ingress direction and two are used for egress flows (onto the SONET link). The two egress tables are for the congested and non-congested states, as determined by the RED algorithm (in other words, the congested state is when the average queue length is greater than the minimum RED threshold). If RED is not enabled on the SONET port, then the egress congested-state mapping table is not used.

The tables are very simple. In the ingress direction, the input DSCP of a packet received from the SONET link is replaced with an output DSCP before the packet is forwarded. The replacement is straightforward; the input DSCP is used as an index into a 64-entry table that contains the output DSCPs associated with each of the input DSCP values. The operation is similar in the egress direction, with the DSCP mapping occurring before the packet is transmitted onto the SONET link(s). The mapping operation is performed after the packet has been assigned to a QoS profile. One potential use of the DSCP mapping capability is reconciliation of varying DiffServ policies at the boundary between autonomous systems (for example, at the boundary between two ISPs). The availability of different tables for the congested/non-congested states is useful for marking operations that increase the drop probability of packets during times of congestion, as discussed in the DiffServ assured forwarding (AF) RFC.

This command is currently only applicable to SONET ports.

**Example**

The following command resets the DSCP mapping tables for port 1, slot 8 of a BlackDiamond switch to their default values:

```
unconfigure diffserv dscp-mapping port 8:1
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.
Platform Availability

This command is available on the BlackDiamond switch only.
unconfigure ppp ports

unconfigure ppp ports <portlist>

Description

Resets the PPP configuration parameters for the specified ports to their default values.

Syntax Description

| portlist | Specifies the port number(s). |

Default

N/A.

Usage Guidelines

By default, BCP is enabled on all PoS ports. (However, ports 2 and 4 of OC-3c modules are not members of any VLANs by default; all other ports are members of the default VLAN by default.)

Example

The following command resets the PPP configuration parameters for port 1, slot 8 of a BlackDiamond switch to the default values:

unconfigure ppp ports 8:1

History

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability

This command is available on the BlackDiamond switch. A similar command is available on the Alpine switch.
unconfigure sonet ports

unconfigure sonet ports <portlist>

Description
Resets the configuration parameters of the specified SONET port to their default values.

Syntax Description

| portlist | Specifies the port number(s). |

Default
N/A.

Usage Guidelines
The following are the SONET port default values:

| clock setting | internal |
| Framing | sonet |
| signal label | auto, where the value of the signal Label field is automatically set based on standard conventions for the given payload type. |
| threshold signal degrade | $10^{-6}$ |
| threshold signal fail | $10^{-5}$ |
| trace path | null |
| trace section | 1 for SONET, null for SDH |

Example
The following command resets the configuration parameters for port 1, slot 8 of a BlackDiamond switch to the default values:

unconfigure sonet ports 8:1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.5b20.

Platform Availability
This command is available on the BlackDiamond switch only.
This chapter describes the following commands:

- Commands for configuring T1, E1, and T3 WAN links.
- Point-to-Point Protocol (PPP) and Multilink PPP (MLPPP) commands for WAN links.
- Commands to display and monitor WAN links.

Extreme Networks WAN modules allow you to pass Ethernet traffic over technologies originally developed for telecommunications. T1, E1, and T3 links have all been used to pass voice traffic over telecommunications networks for many years. Now you can pass data traffic with these modules developed specifically for the Extreme Networks Alpine 3800 family of switches.

To pass data traffic over these modules, the traditional T1, E1, or T3 parameters are configured, and then PPP is used to pass the Ethernet data across the link.
configure multilink add

configure multilink <groupname> add ports <portlist>

Description
Adds ports to a multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Param</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to add ports to a previously created multilink group. All ports added to a multilink group must be added as tagged ports. If the first port added to a multilink group is already configured for PPP, the multilink group will inherit the configuration of the first port. Any other ports added to the link will be configured to match the multilink configuration.

Only T1 or E1 ports can be added to multilink groups.

Example
The following command add ports the previously created multilink group “example_1”:

```
configure multilink example_1 add ports 2:1-2:4
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform when a WAN module is installed.
configure multilink delete

configure multilink <groupname> delete ports <portlist>

Description
Deletes ports from a multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to delete ports from a previously created multilink group.

Example
The following command deletes a port from the multilink group example_1:
configure example_1 delete ports 2:3

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform when a WAN module is installed.
configure ports clock source

configure ports <portlist> [t1 | e1 | t3] clock source [internal | line]

Description
Configures the clock source for WAN links.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>A list of ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Specifies the internal clock.</td>
</tr>
<tr>
<td>line</td>
<td>Specifies clock derived from line signal.</td>
</tr>
</tbody>
</table>

Default
By default the clock source is derived from the line.

Usage Guidelines
The clock is used to synchronize data transmission across a WAN link. Generally, one end of the link provides the master clock, and the other end of the link recovers the clock from the signal on the line. If needed, an internal clock is available.

If the clock source is configured as “line“, but the clock cannot be recovered from the signal on the line, the hardware will use the internal clock instead.

Example
The following command sets the clock source to internal:

```
configure ports 4:2 t1 clock source internal
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports e1 framing

configure ports <portlist> e1 framing [crc4 | no-crc4]

Description
Configure framing for E1 links.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>crc4</td>
<td>Specifies CRC4 framing.</td>
</tr>
<tr>
<td>no-crc4</td>
<td>Specifies No-CRC4 framing.</td>
</tr>
</tbody>
</table>

Default
CRC4 framing is enabled by default.

Usage Guidelines
Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. The two choices for E1 framing are CRC4 and No-CRC4.

Example
The following command sets framing to CRC4 for the E1 ports:

```
configure ports 3:1-3:4 e1 framing crc4
```

History
This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports e1 receivergain

    configure ports <portlist> e1 receivergain [-12 | -43] db

Description
Configures E1 receiver gain to improve link performance.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>A list of ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>db</td>
<td>Specifies the receiver gain in decibels. Only the values above are allowed.</td>
</tr>
</tbody>
</table>

Default
The default value is -12 db.

Usage Guidelines
The receiver gain for E1 links can be configured to improve performances of the link. Changing the receiver gain can help to receive the E1 signal or to reduce crosstalk. Receiver gain is only configurable for E1 links. For T1 links see “configure multilink add” on page 2176 and for T3 links see “configure ports t1 framing” on page 2185.

Example
The following command configures the receiver gain:
configure ports 2:2 e1 receivergain -43 db

History
This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports e1 timeslots

configure ports <portlist> el timeslots <timeslots>

Description
Select the E1 timeslots to use for transmitting data.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>timeslots</td>
<td>Specifies the data timeslots. Timeslot numbers range from 1 to 31.</td>
</tr>
</tbody>
</table>

Default
All timeslots are used by default.

Usage Guidelines
The E1 signal is divided into thirty-two timeslots, numbered 0 through 31. The first timeslot (0) is reserved and cannot be used to transmit data. The timeslot numbered 16 is often used for voice phone calls in installations that combine voice and data. For installations that use the full E1 bandwidth for data communications, you will not need to configure which timeslots are used. For installations that do not use the total E1 bandwidth, your E1 provider will tell you which timeslots to use.

A timeslot list uses a dash to represent a range of numbers and a comma to separate single numbers or ranges. Valid timeslots range from 1 to 31.

Example
The following command specifies timeslots 1 through 15 and 17 through 31 for the E1 port 1 on slot 4:

```bash
configure ports 4:1 e1 timeslots 1-15,17-31
```

History
This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports snmp alert

configure ports <portlist> [t1 | e1 | t3] snmp alert [enable | disable]

Description
Enable and disable the sending of SNMP alerts for WAN links to the SMMi.

Syntax Description

| portlist | A list of ports.

Default
SNMP alerts are enabled by default.

Usage Guidelines
If the WAN module hardware detects a red, yellow, or blue alarm, the alarms are displayed by using a show command. See the command “show ports alarms” on page 2221. Additionally, the module can be configured to send an SNMP alert to the SMMi in the switch when red, yellow, or blue alarms are detected. If the module is configured to send SNMP alerts, and the switch is configured to send SNMP trap messages, then the switch will send a message to any SNMP trap receivers that have been configured. To configure SNMP trap receivers, and for more information about configuring SNMP in ExtremeWare, see the ExtremeWare Software User Guide.

The module can also be configured not to send an SNMP alert to the SMMi. Any red, yellow, or blue alarms will not be reported to the SNMP trap receivers.

Example
The following command disables snmp alerts from a port:

configure ports 4:1 t1 snmp alert disable

History
This command was originally available as “configure ports t1 alarms” in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added and the command was changed to “configure ports snmp alert” in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports t1 cablelength

configure ports <portlist> t1 cablelength [{0 | -7.5 | -15 | -22.5} db | [133 | 266 | 399 | 533 | 655] feet]

Description
Control T1 transmitter signal level for different cable lengths.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>A list of ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>feet</td>
<td>Specifies the cable length in feet. Only the values above are allowed.</td>
</tr>
<tr>
<td>db</td>
<td>Specifies the transmitter attenuation in decibels. Only the values above are allowed.</td>
</tr>
</tbody>
</table>

Default
The default setting is 133 feet.

Usage Guidelines
For short haul connections (less than 1000 feet) the transmitter level for T1 is set by selecting a cable length in feet, from the following values: 133, 266, 399, 533 or 655. Choose the next higher value if the cable length provided by your service provider does not match one of these values. For example, choose 133 for a 50 foot cable and 533 for a 450 foot cable. The default value is 133, which corresponds to cables in the range of 0-133 feet.

For longer distances (up to 6000 feet) T1 equipment uses more sensitive receivers, and crosstalk is more likely to occur. Under these conditions, the transmitter level is set by selecting a transmitter attenuation level in dB from the following values: -22.5, -15, -7.5, or 0.

From lowest to highest transmitter level, use the following values for the configure port t1 cablelength command: -22.5 db, -15 db, -7.5 db, 0 db, 133 feet, 266 feet, 399 feet, 533 feet, and 655 feet.

Example
The following command sets the cablelength for all T1 ports:
configure ports 2:1-2:4 t1 cablelength 533 feet

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when the applicable WAN module is available.
configure ports t1 fdl

configure ports <portlist> t1 fdl [off | att | ansi]

**Description**

Configures facility data link (FDL) for T1 links.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>att</td>
<td>Specifies ATT 54016 FDL.</td>
</tr>
<tr>
<td>ansi</td>
<td>Specifies T1.403 FDL.</td>
</tr>
</tbody>
</table>

**Default**

FDL is off.

**Usage Guidelines**

Facility data link (FDL) for T1 links uses twelve bits in the ESF frame to signal information about line and connection status. Since FDL is only meaningful for ESF framing, FDL settings are ignored when a port is configured for SF framing.

The two T1 standards supported for FDL are ATT, described by the ATT 54016 specification, and ANSI, described by the T1.403 standard.

**Example**

The following command enables ATT FDL on four T1 links:

```
configure ports 4:1-4:4 t1 fdl att
```

**History**

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports t1 framing

configure ports <portlist> t1 framing [esf | sf]

Description
Configure framing for T1 links.

Syntax Description

<table>
<thead>
<tr>
<th>Description</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>esf</td>
<td>Specifies ESF framing.</td>
</tr>
<tr>
<td>sf</td>
<td>Specifies SF framing.</td>
</tr>
</tbody>
</table>

Default
ESF framing is enabled by default.

Usage Guidelines
Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. The two choices for T1 framing are Super Frame (SF), also known as D4, and Extended Super Frame (ESF). The ESF scheme is a newer standard and is enabled by default. To choose the T1 framing scheme, use the following command:

If you choose to use SF framing, you should disable yellow alarm detection for the T1 line. SF framing may generate false yellow alarms. See the command “configure ports snmp alert” on page 2182 to disable yellow alarms.

Example
The following command sets framing to SF for the T1 ports:

configure ports 3:1-3:4 t1 framing sf

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports t1 lbdetect

configure ports <portlist> t1 lbdetect [off | inband]

Description
Configures inband loopback detection on T1 links.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>A list of ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>inband</td>
<td>Specifies inband loopback detection.</td>
</tr>
</tbody>
</table>

Default
By default, loopback detection is off.

Usage Guidelines
When inband loopback detection is enabled, a specific sequence of data in the signal payload from the remote end of the T1 link will cause the local end to enter network line loopback mode and send any received signal back to the remote end.

Inband loopback detection is only possible if facility data link (FDL) is enabled and configured as “ATT”. See the command “configure ports t1 fdl” on page 2184 for more information.

Example
The following command enables inband loopback detection:
configure ports 4:1-4:2 t1 lbdetect inband

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports t1 linecoding

configure ports <portlist> t1 linecoding [b8zs | ami]

Description
Configures the linecoding convention for T1 links.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>b8zs</td>
<td>Specifies B8ZS linecoding.</td>
</tr>
<tr>
<td>ami</td>
<td>Specifies AMI linecoding.</td>
</tr>
</tbody>
</table>

Default
The default linecoding is B8ZS.

Usage Guidelines
The two choices for linecoding standards are bipolar eight zero suppression (B8ZS) or alternate mark inversion (AMI).

Example
The following command sets the linecoding to AMI:
```
configure ports 2:3,2:4 t1 linecoding ami
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports t1 yellow

    configure ports <portlist> t1 yellow [detection | generation | both | off]

Description
Configure detection and generation of yellow alarms.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>A list of ports.</th>
</tr>
</thead>
</table>

Default
Both detection and generation of yellow alarms is enabled by default.

Usage Guidelines
A yellow alarm occurs on a device when its signal is not received at the remote end. It is also called a Remote Alarm Indication (RAI). You can disable detection and generation of yellow alarms for a T1 port. When SF framing is used, yellow alarm detection and generation should be set to off, because detection of yellow alarms is not reliable when data traffic is transmitted with SF framing (data traffic often contains bit combinations that do not occur for encoded voice traffic).

Example
The following command enables only the detection of yellow alarms:

```plaintext
configure ports 3:1-3:4 t1 yellow detection
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ports t3 cablelength

configure ports <portlist> t3 cablelength [349 | 900] feet

Description
Control T3 transmitter signal level for different cable lengths.

Syntax Description

<table>
<thead>
<tr>
<th>Portlist</th>
<th>A list of ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Feet</td>
<td>Specifies the cable length in feet. Only the values above are allowed.</td>
</tr>
</tbody>
</table>

Default
The default setting is 349 feet.

Usage Guidelines
The transmitter level for T3 is set by selecting a cable length in feet, from the following values: 349 or 900. Choose the next higher value if the cable length provided by your service provider does not match one of these values. For example, choose 349 for a 50 foot cable and 900 for a 450 foot cable. The default value is 349, which corresponds to cables in the range of 0-349 feet.

Example
The following command sets the cablelength for the T3 port:
configure ports 2:1 t3 cablelength 900 feet

History
This command was first available in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when the applicable WAN module is available.
configure ports t3 framing

configure ports <portlist> t3 framing [c-bit | m13]

Description
Configure framing for a T3 link.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>c-bit</td>
<td>Specifies C-Bit framing.</td>
</tr>
<tr>
<td>m13</td>
<td>Specifies M13 framing.</td>
</tr>
</tbody>
</table>

Default
C-Bit framing is enabled by default.

Usage Guidelines
Framing is used to synchronize data transmission on the line. Framing allows the hardware to determine when each packet starts and ends. The two choices for T3 framing are C-Bit and M13.

Example
The following command sets framing to M13 for the T3 port:

```
configure ports 3:1 t3 framing m13
```

History
This command was first available in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure ppp

configure ppp [bcp [on | off] | ipcp [on | off]] [ports <portlist> | multilink <groupname>]

Description
Configures the network control protocol (encapsulation) that will run on the specified PPP/MLPPP WAN ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bcp</td>
<td>Specifies bridging control protocol for the port.</td>
</tr>
<tr>
<td>ipcp</td>
<td>Specifies IP control protocol for the port.</td>
</tr>
<tr>
<td>on</td>
<td>Enables the designated protocol on the port.</td>
</tr>
<tr>
<td>off</td>
<td>Disables the designated protocol on the port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default
By default, BCP is enabled on all WAN ports.

Usage Guidelines
The packets passed over the PPP/MLPPP link can use either bridged or routed encapsulation. You would use bridged packets if you plan to have more than one VLANs span the link. You would use routed packets if the link connects two different routed networks or separate VLANs.

Using bridged packets allows the VLAN tags to be carried across the PPP/MLPPP link. Bridged packets are transported using the PPP Bridging Control Protocol (BCP), described in RFC 2878, except in the case of Legacy BCP, described below. When the encapsulation is set to BCP, 802.1Q and 802.1p information is preserved and transported across the link.

Routed packets are transported across a PPP/MLPPP link using IP Control Protocol (IPCP), described in RFC 1332. This is the encapsulation that is familiar to most users of PPP. The routed packets do not contain Ethernet headers so cannot preserve VLAN tags. However, the WAN ports still must be added as tagged ports to the VLAN that contains them. The module uses the tags internally and strips them off before the packets are transmitted. The IP addresses used for the PPP/MLPPP link are taken from the IP address assigned to the VLAN at each end of the link. The VLAN that contains the IPCP encapsulated PPP/MLPPP ports cannot contain other ports. In other words, the only ports allowed in the VLAN are those that make up the IPCP encapsulated link. There can only be one VLAN spanning an IPCP-encapsulated link.

You must have one and only one encapsulation type configured on a PPP/MLPPP link. Setting BCP encapsulation off implies that IPCP encapsulation is on. The default setting is BCP encapsulation on and IPCP encapsulation off.

Legacy BCP. Some routers supported by other vendors implemented BCP using an older standard, RFC 1638. For interoperability, the Extreme Networks implementation supports both standards. The limitation with RFC 1638-based BCP is that 802.1Q tags are not supported. So Legacy BCP cannot
support multiple VLANs or preserve 802.1p priority across the PPP link. Both types of BCP can operate over single and multilink PPP.

When BCP is negotiated over a link, RFC 2878 BCP is initially proposed. If the peer only supports Legacy BCP (RFC 1638), then the link is made using Legacy BCP. Since the WAN module ports are always configured as tagged ports, the VLAN tag is removed in the egress direction and inserted in the egress direction when BCP is operating in Legacy mode.

There is no Legacy BCP specific configuration, and the display for the command `show ppp info` is identical for BCP and Legacy BCP. To determine if the link is using Legacy BCP, use the following command:

```
show log warning
```

and look for the message:

```
BCP: Legacy BCP UP; Only a single VLAN over BCP is supported
```

**Example**

The following command example configures IPCP on a PPP port, and applies to a WAN module installed in slot 1 of an Alpine switch:

```
configure ppp ipcp on port 1:4
```

**History**

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
configure ppp authentication

configure ppp authentication [off | chap | pap | chap-pap] [ports <portlist> | multilink <groupname>]

Description
Configures authentication on the specified PPP ports or MLPPP multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>off</td>
<td>Disables authentication.</td>
</tr>
<tr>
<td>chap</td>
<td>Authenticated the peer using the challenge handshake authentication protocol (CHAP).</td>
</tr>
<tr>
<td>pap</td>
<td>Authenticated the peer using the password authentication protocol.</td>
</tr>
<tr>
<td>chap-pap</td>
<td>Specifies that first CHAP is used, then PAP, if CHAP fails to authenticate the peer.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>groupname</td>
<td>Specifies the multilink group.</td>
</tr>
</tbody>
</table>

Default
The default is authentication off.

Usage Guidelines
When off is specified, the peer is not authenticated. When chap is specified, the peer is authenticated using the challenge handshake authentication protocol (CHAP). When pap is specified, the peer is authenticated via the password authentication protocol (PAP). Specification of chap-pap indicates that CHAP is first used, then PAP, if CHAP fails to authenticate the peer.

Example
The following command example turns on CHAP authentication for the multilink group m1_remote:

configure ppp authentication chap multilink m1_remote

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
configure ppp user

    configure ppp user <name> {encrypted} {<password>} [ports <portlist> | multilink <groupname>]

Description
Configures the user name and password that the specified PPP/MLPPP link uses if the peer requests authentication.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>Specifies user name for PPP peer authentication requests.</td>
</tr>
<tr>
<td>encrypted</td>
<td>This parameter option should not be entered.</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password for PPP peer authentication requests.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies the port number(s).</td>
</tr>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default
By default, there is no value set for name or password.

Usage Guidelines
The name is also sent when a port transmits a CHAP authentication request. The implementation responds to either CHAP or PAP authentication requests issued by the peer regardless of whether the port is configured to authenticate the peer. The name parameter is a string with a length in the range of [1–32] characters. The password parameter is also a character string, with a maximum length of 32 characters. If no password is provided on the command line, then you are prompted to enter the password twice (with the second time serving as a confirmation). You should not enter the encrypted parameter option (it is used by the switch when generating an ASCII configuration).

Example
The following command example sets the name to titus and sets the password to 1Afortune for the multilink group m_link1:

```bash
configure ppp user "titus" "1Afortune" multilink m_link1
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
configure qosprofile min-bps

configure qosprofile <qosprofile> min-bps <bps> [k | m] max-bps <bps> [k | m] {priority <level>} [ports <portlist> | multilink <multilink name>]

Description
Modifies the default QoS profile parameters for T1 and E1 modules.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qosprofile</td>
<td>Specifies a QoS profile name.</td>
</tr>
<tr>
<td>min-bps</td>
<td>Specifies a minimum bandwidth for this queue. The default setting is 0.</td>
</tr>
<tr>
<td>k</td>
<td>Specifies Kbps.</td>
</tr>
<tr>
<td>m</td>
<td>Specifies Mbps.</td>
</tr>
<tr>
<td>max-bps</td>
<td>Specifies the maximum bandwidth this queue is permitted to use. The default setting is 1536 Kbps.</td>
</tr>
<tr>
<td>level</td>
<td>Specifies a service priority setting. Settings are low and high. The default setting is low. Available in egress mode only.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>multilink name</td>
<td>Specifies a multilink.</td>
</tr>
</tbody>
</table>

Default
- Minimum bandwidth—0 Kbps
- Maximum bandwidth—1536 Kbps
- Priority—low

Usage Guidelines

This command sets the software egress QoS for T1 and E1 modules, using units of bps of bandwidth, instead of percentages of bandwidth.

For WAN QoS only two priority levels are available, low and high. Software queues are scheduled based on priority, minimum bandwidth, and maximum bandwidth. Only one queue can have high priority.

The high priority queue is flushed on every scheduling round. Minimum bandwidth is ignored for this queue. Throughput is policed based on the maximum bandwidth value. Policing prevents packets from entering a queue that is receiving traffic from the backplane too fast. The remaining bandwidth is shared by all other queues based on the minimum bandwidth setting of each queue. In other words, the high priority queue takes up all the bandwidth up to its max-bps setting, while the low priority queues share all the remaining bandwidth.
**Example**

The following command configures the QoS profile parameters of QoS profile `qp5` for specific ports on a T1 or E1 module:

```
configure qosprofile qp5 min-bps 64 k max-bps 512 k priority high ports 2:1,2:3
```

**History**

This command was available in ExtremeWare 7.1.0.

**Platform Availability**

This command is available for T1 and E1 modules.
configure qosprofile wanqos maxbuf

configure qosprofile <qosprofile> wanqos maxbuf <count> [ports <portlist> | multilink <multilink name>]

**Description**
Sets the maximum queue depth for T1 and E1 modules.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>qosprofile</td>
<td>Specifies a QoS profile name.</td>
</tr>
<tr>
<td>count</td>
<td>Specifies a maximum buffer size this queue. The default setting is 0.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of ports or slots and ports to which the parameters apply. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>multilink name</td>
<td>Specifies a multilink.</td>
</tr>
</tbody>
</table>

**Default**
By default, 256 packet buffers are assigned to the high priority queue.

**Usage Guidelines**
This command sets the software egress queue buffers for T1 and E1 modules.

For WAN QoS, each port has 256 packet buffers of 1900 bytes. The buffers are shared among the eight queues. Use a small number for low latency. Use a large number for best effort on bursty traffic.

**Example**
The following command configures the QoS maximum buffer of QoS profile qp5 to 128 for ports 2:1 and 2:3:

configure qosprofile qp5 wanqos maxbuf 128 ports 2:1,2:3

**History**
This command was available in ExtremeWare 7.1.0.

**Platform Availability**
This command is available for T1 and E1 modules.
configure vlan add multilink

    configure vlan <vlan name> add multilink <groupname>

Description

Adds an MLPPP multilink group to a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Specifies a previously created VLAN.</td>
</tr>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

Add an MLPPP group to a VLAN to transport traffic across the link. A multilink group configured for BCP encapsulation can transport more than one VLAN’s traffic (see “configure ppp user” on page 2194 for details).

Example

The following command adds the multilink group *marmots* to the VLAN *corporate*:

```shell
configure corporate add ml_remote
```

History

This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability

This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure vlan delete multilink

configure vlan <vlan name> delete multilink <groupname>

Description
Deletes an MLPPP multilink group from a VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Specifies a previously created VLAN.</td>
</tr>
<tr>
<td>groupname</td>
<td>Specifies a previously added multilink group.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Remove an MLPPP group from a VLAN to stop transporting that VLAN’s traffic across the link.

Example
The following command deletes the multilink group ml_remote from the VLAN corporate:

```
configure corporate delete ml_remote
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
configure wanqos egress map dot1p_priority

configure wanqos egress map dot1p_priority <priority> to qosprofile <QoS profile>

Description
Change the default mapping of dot1p values to software egress queues.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>priority</td>
<td>Specifies a dot1p priority.</td>
</tr>
<tr>
<td>qosprofile</td>
<td>Specifies a QoS profile name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

WAN QoS uses dot1p value to map directly to software egress queues. Use this command to change the default mapping and map several dot1p values to the same software queue. This can simplify configuration (two to three classes of service instead of eight) and improve egress burst tolerance because each queue can have a larger number of buffers. Set the maximum buffer size to one for unused queues.

To set the maximum buffer size on queues, use the following command:

configure qosprofile <qosprofile> wanqos maxbuf <count> [ports <portlist> | multilink <multilink name>]

Example

The following command maps dot1p priority 5 to QoS profile qp7:
configure wanqos egress map dot1p_priority 5 to qosprofile qp7

History

This command was available in ExtremeWare 7.1.0.

Platform Availability

This command is available for T1 and E1 modules.
create account pppuser

create account pppuser <username> {encrypted} {<password>}

Description
Creates a local database entry that can be used to authenticate a PPP peer.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>username</td>
<td>Specifies the user name used for authentication.</td>
</tr>
<tr>
<td>encrypted</td>
<td>This parameter should not be used (see below).</td>
</tr>
<tr>
<td>password</td>
<td>Specifies the password used for authentication.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
When the remote end initiates the link, the local end must verify the authentication information. The local end maintains a database of authorized user accounts and passwords. Use this command to add a user to the database. You should not enter the encrypted parameter option (it is used by the switch when generating an ASCII configuration).

Example
The following command example adds an entry to the authentication database. A username stretch with password baserunner is added to the database:
create account pppuser stretch baserunner

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
create multilink

create multilink <groupname>

Description
Creates an MLPPP multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies the multilink group name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to create a multilink group. Like the `create vlan` command, the `multilink` keyword must be used when creating the multilink group. Once the group is created, ExtremeWare recognizes the group name as a multilink group, so the `multilink` keyword is not needed in other commands that manipulate multilink groups.

Example
The following command creates the multilink group `ml_remote`:

```
create multilink ml_remote
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
delete account pppuser

    delete account pppuser <username>

Description
Deletes an entry in the local PPP authentication database.

Syntax Description

| username | Specifies the user name used for authentication. |

Default
N/A

Usage Guidelines
Deletes a user from the PPP authentication database. Existing links already authenticated are not affected by this command.

Example
The following command example removes the entry for stretch from the authentication database:

```
delete account pppuser stretch
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
delete multilink

dele te multilink <groupname>

Description
Deletes an MLPPP multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies the multilink group name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to delete a multilink group.

Example
The following command deletes the multilink group *ml_remote*:

delete multilink ml_remote

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release. This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
disable multilink

disable multilink <groupname>

Description
Disables an MLPPP multilink group.

Syntax Description

| groupname | Specifies the multilink group name. |

Default
N/A

Usage Guidelines
Use this command to disable a multilink group. The multilink group will stop transporting traffic across the link.

Example
The following command disables the multilink group ml_remote:

disable multilink ml_remote

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
disable ports loopback

disable ports <portlist> [t1 | e1 | t3] loopback

Description
Disables the current loopback mode and returns port to normal function.

Syntax Description

| portlist          | A list of ports. |

Default
Loopback is disabled by default.

Usage Guidelines
Use this command to return the near and remote side of a T1, E1, or T3 link form loopback mode to normal mode.

You can also use the following command to return the remote T1 or T3 port to normal mode from loopback mode:

```
enable ports <portlist> [t1 | t3] loopback remote loopdown
```

If you add a 10/100 port as a loopback port and delete it, autonegotiation is set to off.

Example
The following command blah:
```
disable ports 2:1-2:4 t1 loopback
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.
T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
disable wanqos

disable wanqos {ports <portlist> | multilink <groupname>}

**Description**
Disables WAN QoS for T1 and E1 ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>groupname</td>
<td>A multilink group name.</td>
</tr>
</tbody>
</table>

**Default**
WAN QoS is disabled by default.

**Usage Guidelines**
This command disables WAN QoS for T1 and E1 links. There is no equivalent command for T3 links.

**Example**
The following command disables WAN QoS on ports 1:1 and 1:3:

disable wanqos ports 1:1,1:3

**History**
This command was first available in ExtremeWare 7.1.0.

**Platform Availability**
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
enable multilink

    enable multilink <groupname>

Description
Enables an MLPPP multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies the multilink group name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to enable a multilink group.

Example
The following command enables the multilink group ml_remote:

```
enable multilink ml_remote
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
enable ports loopback

    enable ports <portlist> [t1 | e1 | t3] loopback [local | network line]

Description
Enables the near-end local and network line loopback modes.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>local</td>
<td>Specifies local loopback.</td>
</tr>
<tr>
<td>network line</td>
<td>Specifies network line loopback.</td>
</tr>
</tbody>
</table>

Default
Loopback is disabled by default.

Usage Guidelines
Use this command to enable local and network line loopback modes on the local port for T1, E1, and T3 links.

T1 links also support an additional mode, network payload loopback. Use the following command for network payload loopback mode:

enable ports <portlist> t1 loopback network payload

For remote loopback modes, use the command:

enable ports <portlist> [t1 | t3] loopback remote [line | payload | loopdown]

Example
The following command enables network line loopback mode on all the ports of an E1 module:

enable ports 4:1-4:4 e1 loopback network line

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.
T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
enable ports loopback remote

   enable ports <portlist> [t1 | t3] loopback remote [line | payload | loopdown]

Description
Enables and disables remote loopback modes for T1 and T3 ports.

Syntax Description

| portlist | A list of ports. |

Default
Loopback is disabled by default.

Usage Guidelines
This command enables and disables remote loopback for T1 and T3 links. There is no equivalent command for E1 links.

The `loopdown` keyword is used to disable loopback at the remote end.

Example
The following command causes the remote end of a T3 link to enter payload loopback mode:

```
enable ports 3:1 t3 loopback remote payload
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
enable ports t1 loopback network payload

   enable ports <portlist> t1 loopback network payload

Description
Enables network payload loopback mode on T1 links.

Syntax Description

| portlist          | A list of ports. |

Default
Loopback is disabled by default.

Usage Guidelines
Use this command to enable network payload loopback modes on the local port for T1 links. This mode is not available for E1 and T3 links.

WAN links also support additional modes, local and network line loopback. Use the following command for these modes:

   enable ports <portlist> [t1 | e1 | t3] loopback [local | network line]

For remote loopback modes, use the command:

   enable ports <portlist> [t1 | t3] loopback remote [line | payload | loopdown]

Example
The following command enables network payload loopback mode on a T1 link:

   enable ports 4:3 t1 loopback network payload

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
enable vman termination

   enable vman termination {ports <portlist> | multilink <groupname>}

**Description**

Enables VMAN termination for T1 and E1 ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>groupname</td>
<td>A multilink group name.</td>
</tr>
</tbody>
</table>

**Default**

VMAN termination is disabled by default.

**Usage Guidelines**

This command enables VMAN termination for T1 and E1 links. There is no equivalent command for T3 links.

**Example**

The following command enables VMAN termination on ports 1:1 and 1:3:

```
enable vman termination ports 1:1,1:3
```

**History**

This command was first available in ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the Alpine 3800 series platform, when a WAN module is installed.
enable wanqos

enable wanqos {ports <portlist> | multilink <groupname>}

Description
Enables WAN QoS for T1 and E1 ports.

Syntax Description

<table>
<thead>
<tr>
<th>Port</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>A list of ports.</td>
</tr>
<tr>
<td>groupname</td>
<td>A multilink group name.</td>
</tr>
</tbody>
</table>

Default
WAN QoS is disabled by default.

Usage Guidelines
This command enables WAN QoS for T1 and E1 links. There is no equivalent command for T3 links.

When WAN QoS is enabled, egress traffic is sorted into eight software egress queues for each T1 or E1 port.

Example
The following command enables WAN QoS on ports 1:1 and 1:3:

```
enable wanqos ports 1:1,1:3
```

History
This command was first available in ExtremeWare 7.1.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
restart multilink

    restart multilink <groupname>

Description
Restarts an MLPPP multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>groupname</th>
<th>Specifies the multilink group name.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
Use this command to restart a multilink group. This command is the equivalent of disabling and then enabling a multilink group. You would use this command if you have changed any configuration parameters of the MLPPP group. The changed configuration does not take effect until you disable then enable the link, or until you restart the link.

Example
The following command restarts the multilink group ml_remote:
restart multilink ml_remote

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show accounts pppuser

Description
Display the PPP user accounts database.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
Use this command to examine the entries in the PPP user accounts database, used for authentication when a link is initiated from a remote peer.

Example
The following command displays the PPP accounts database:

```
show accounts pppuser
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show multilink

    show multilink <groupname>

Description
Displays the configuration of the multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to display the ports in a multilink group, and the PPP configuration of the group.

Example
The following command displays the configuration for the multilink group m_remote1:

```
show multilink m_remote1
```  

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show multilink alarms

   show multilink <groupname> [t1 | e1] alarms {detail}

Description
Displays alarms for a multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Use this command to display alarms that may have been received on any of the ports that make up a multilink group. To display alarms on a T3 link, use the command:

show ports <portlist> t3 alarms

Example
The following command displays the alarms for T1 ports in the multilink group ml_example:

show multilink ml_example t1 alarms

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show multilink e1 errors

```
show multilink <groupname> e1 errors near-end [totals | intervals | current]
```

**Description**
Displays the current and past port error statistics for E1 multilink groups.

**Syntax Description**
- `groupname`: Specifies a previously created multilink group.

**Default**
N/A

**Usage Guidelines**
For an E1 multilink group, you can display errors from the near-end only.
Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For T1 multilink group errors, use the following command:

```
show multilink <groupname> t1 errors [near-end | far-end] [totals | intervals | current]
```

**Example**
The following command displays the E1 multilink group errors detected on the near-end during the current interval for the multilink group `m_example1`:

```
show multilink m_example1 e1 errors near-end current
```

**History**
This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show multilink stats

    show multilink <groupname> stats {detail}

Description
Displays multilink statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Display the statistics of a multilink group.

Example
The following command displays the detailed statistics for the multilink group \textit{m\_remote1}:

```
show multilink m\_remote1 stats detail
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show multilink t1 errors

    show multilink <groupname> t1 errors [near-end | far-end] [totals | intervals | current]

**Description**
Displays the current and past error statistics for T1 multilink groups.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;groupname&gt;</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

**Default**
N/A

**Usage Guidelines**
For T1 multilink groups, you can display errors from the near-end or the far-end.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For errors on E1 multilink groups, use the following command:

    show multilink <groupname> e1 errors near-end [totals | intervals | current]

**Example**
The following command displays the T1 errors detected on the near-end during the current interval:

    show ports t1 errors near-end current

**History**
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ports alarms

    show ports {mgmt | <portlist>} {t1 | e1 | t3} alarms

Description
Displays real-time port alarms.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, alarms are displayed for all ports.

Example
The following command displays the alarms for T1 ports in:

    show ports 2:1-2:4 t1 stats

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.
T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ports configuration

show ports {mgmt | <portlist>} [t1 | e1 | t3] configuration

Description
Displays the port configuration and status.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, configuration and status are displayed for all ports.

Example
The following command displays the T1 configuration and status of one port:
show ports 4:1 t1 configuration

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ports errors

show ports {mgmt | <portlist>} [t1 | t3] errors [near-end | far-end] [totals | intervals | current]

Description
Displays the current and past port errors for T1 and T3 links.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, errors are displayed for all ports.

For the T1 and T3 ports, you can display errors from the near-end or the far-end.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For E1 errors, use the following command:

show ports <portlist> e1 errors near-end [totals | intervals | current]

Example
The following command displays the T1 errors detected on the near-end during the current interval:

show ports t1 errors near-end current

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ports e1 errors

  show ports {mgmt | <portlist>} e1 errors near-end [totals | intervals | current]

Description
Displays the current and past port errors for E1 links.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, errors are displayed for all ports.

For an E1 port, you can display errors from the near-end only.

Display the total errors detected, errors detected per interval in the past, or errors detected in the current interval.

For T1 and T3 errors, use the following command:

show ports <portlist> [t1 | t3] errors [near-end | far-end] [totals | intervals | current]

Example
The following command displays the E1 errors detected on the near-end during the current interval:
show ports e1 errors near-end current

History
This command was first available in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ports info

    show ports {mgmt | <portlist>} [t1 | e1 | t3] info

Description
Displays the port configuration and status.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Element</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, information is displayed for all ports.

Example
The following command displays the T1 information for a single port:
```
show ports 4:2 t1 info
```

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.
T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ports stats

    show ports {mgmt | <portlist>} {t1 | e1 | t3} stats

Description
Displays real-time port statistics.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mgmt</td>
<td>Specifies the management port. Supported only for switches that provide a management port.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify a port number or range of ports, statistics are displayed for all ports.

Example
The following command displays the statistics for the T1 ports in slot 2:

    show ports 2:1-2:4 t1 stats

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
E1 support was added in ExtremeWare v6.1.8w3.0.1b56 WAN technology release.
T3 support was added in ExtremeWare v6.1.8w3.0.1b61 WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed.
show ppp

    show ppp {<portlist>}

**Description**
Displays status information for PPP ports.

**Syntax Description**

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8. |

**Default**
By default, the command shows summarized status for all PPP port(s).

**Usage Guidelines**
The `portlist` parameter can be used to specify the port(s) for which status is to be shown. Alternatively, you can enter `show ppp` with no parameters to obtain status for all PPP ports.

**Example**
The following command displays status information for all PPP ports:

```
show ppp
```

**History**
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
show ppp info

    show ppp info {<portlist>}

Description
Displays the PPP connection status for selected WAN ports.

Syntax Description

| portlist        | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:* , 2:5, 2:6-2:8. |

Default
By default, the command displays PPP connection status for all WAN ports.

Usage Guidelines
The portlist parameter can be used to specify the port(s) for which PPP connection status is to be shown. Alternatively, you can enter show ppp info with no parameters to obtain PPP connection status for all WAN ports.

Example
The following command displays PPP connection status for all WAN ports:

show ppp info

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
unconfigure ppp

unconfigure ppp [ports <portlist> | multilink <groupname>]

Description
Resets the configuration on the specified WAN ports or multilink group.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>Specifies the port number(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>groupname</td>
<td>Specifies a previously created multilink group.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The ports or multilink group PPP configuration is reset to the default, BCP encapsulation with no authentication required.

Example
The following command example resets the PPP parameters of all the ports in the multilink group m_remote1 to BCP and no authentication:

unconfigure ppp m_remote1

History
This command was first available in ExtremeWare v6.1.5w2.01WAN technology release.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the Alpine 3800 series platform, when a WAN module is installed. A similar command is available on the BlackDiamond switch.
The High-Density Gigabit Ethernet modules (also known as “3” series modules and Triumph modules) are I/O modules for both the Alpine 3800 series and the BlackDiamond 6800 series chassis-based systems. These modules support bi-directional traffic management to control the rate of information that flows into (ingress) or out of (egress) a switched network from one individual network port.

The “3” series modules are designed for metro service providers and enterprise environments. In a service provider environment, service providers can control the flow of data on a per customer basis. In an enterprise environment, businesses can use these modules to control user access or where desktop or server interfaces require high-density Gigabit Ethernet capability.

The “3” series modules also support the QoS functions, commands, and configurations described in Chapter 7.

**NOTE**

*The 10GX3 module does not support the enhanced QoS functions described in this chapter.*

This chapter documents the “3” series I/O module command set.
abort diagnostics cable

Description
Discontinues the running of the Cable Diagnostics Module (CDM) to obtain cable diagnostics values for selected physical ports of the system.

Syntax Description
This command has no syntax or values.

Default
None

Usage Guidelines
This command aborts the running of cable diagnostics for selected physical ports of the system. To enable auto-diagnostics collection for selected ports, use the `enable diagnostics cable` command. To disable auto-diagnostics collection for selected ports, use the `disable diagnostics cable` command. To set the starting time for auto-diagnostics collection for selected ports, use the `configure diagnostics cable` command. To manually run cable diagnostics, use the `run diagnostics cable` command. To view cable diagnostics data, use the `show diagnostics cable` command.

Example
The following command disables automatic running of cable diagnostics for all ports.

disable diagnostics cable port all

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on “3” series I/O modules only.
configure application examination ports

    configure {application examination} <application name>  [add | delete] ports [<portlist> | all]

Description
Adds or deletes an existing application examination rule to or from the specified “3” series ports.

Syntax Description

<table>
<thead>
<tr>
<th>application name</th>
<th>Specifies the name string associated with the rule to configure.</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Specifies to add an application examination rule to the specified ports.</td>
</tr>
<tr>
<td>delete</td>
<td>Specifies to delete an application examination rule from the specified ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:* , 2:5 , 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all “3” series ports.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
Up to 60 application examination rules can be associated with each port.

Example
The following command adds an application examination rule, TCP20, to ports 2:6 through 2-8:
    configure application examination TCP20 add ports 2:6-2:8

The following command also adds an application examination rule to ports 2:6 through 2-8. The keywords “application examination” are optional.
    configure TCP20 add ports 2:6-2:8

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available on “3” series I/O modules only.
configure diagnostics cable

configure diagnostics cable time <time> {reset-port-on-failure [enable | disable]}

Description
Creates a template for automatically running the Cable Diagnostics Module (CDM) to obtain cable diagnostics values for the physical ports of the system.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>time &lt;time&gt;</td>
<td>Specifies the start time for the automatic running of the cable diagnostics.</td>
</tr>
<tr>
<td></td>
<td>The time must be entered in hh:mm:ss format.</td>
</tr>
<tr>
<td>reset-port-on-failure</td>
<td>Specifies whether a port must be restarted if the diagnostics run results in</td>
</tr>
<tr>
<td>[enable</td>
<td>disable]</td>
</tr>
<tr>
<td></td>
<td>must be restarted after a failure; disabling this feature leaves the port</td>
</tr>
<tr>
<td></td>
<td>disabled after a failure. By default, the value is set to enable.</td>
</tr>
</tbody>
</table>

Default
Reset-port-on-failure is enabled by default.

Usage Guidelines
This command sets the starting time for the automatic running of the CDM to obtain cable diagnostics values for the physical ports of the system. To enable auto-diagnostics collection for selected ports, use the enable diagnostics cable command. To disable auto-diagnostics collection for selected ports, use the disable diagnostics cable command. To manually run cable diagnostics, use the run diagnostics cable command.

If reset-port-on-failure is set to disable (the default setting), then a port that has been disabled prior to running diagnostics will be left disabled after the diagnostics run has completed. As a result, the status LED associated with the failed port will continue to blink. To stop the blinking of the status LED, you must explicitly enable the port.

You cannot issue this command while the cable diagnostics process is in progress.

To view cable diagnostics data, use the show diagnostics cable command.

Example
The following command configures automatic running of the Cable Diagnostics Module (CDM) to start at 2:30 AM, and restarts the port if the auto-diagnostics run results in a port failure.

configure diagnostics cable time 02:30:00 reset-port-on-failure enable

History
This command was first available in ExtremeWare 7.3.0.
Platform Availability
This command is available on “3” series I/O modules only.
configure diffserv ingress replacement ports

configure diffserv ingress replacement low-priority code-point <number> high-priority code-point <number> ports [<portlist> | all] {<Ingress QoS profile>}

Description
Configures the optional overwriting of the DiffServ code point portion of the IP TOS field for ingress traffic.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>low priority code-point number</td>
<td>Specifies the low-priority DiffServ code point (IP TOS) value to use to overwrite low-priority ingress traffic. The default is 0. The range is 0 to 63.</td>
</tr>
<tr>
<td>high priority code-point number</td>
<td>Specifies the high-priority DiffServ code point (IP TOS) value to use to overwrite high-priority ingress traffic. The default is 0. The range is 0 to 63.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:* , 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all “3” series ports.</td>
</tr>
<tr>
<td>Ingress QoS profile</td>
<td>Specifies an ingress QoS profile: IQP1 through IQP8.</td>
</tr>
</tbody>
</table>

Default
The default values for both the low-priority and high-priority code points are 0.

Usage Guidelines
This command allows the overwriting of the upper 6 bits of the IP TOS field. The lower 2 bits of the TOS field passes through unchanged.

You can specify different code point values for both high-priority (below the committed-rate) and low-priority (above the committed-rate) traffic on each port or each ingress QoS profile on each port.

DiffServ ingress replacement is only done on IP Ethernet II (Ethertype) encapsulated frames. Frames that are IPX, LLC, or SNAP encapsulated are passed through with no DiffServ code point alterations.

You must enable low-priority and high-priority DiffServ ingress replacement on the specified ports before you can overwrite low-priority or high-priority traffic. To enable low-priority and high-priority DiffServ ingress replacement, use the command:

enable diffserv ingress replacement [low-priority | high-priority] ports [<portlist> | all] {<Ingress QoS profile>}

The “3” series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

If you do not specify an ingress QoS profile, all ingress QoS profiles for the indicated ports are affected.
**Example**

The following command configures the low-priority to 5 and the high-priority to 10 on all ports for all ingress QoS profiles:

```
configure diffserv ingress replacement low-priority code-point 5 high-priority code-point 10 ports all
```

**History**

This command was first available in ExtremeWare 7.1.

**Platform Availability**

This command is available on “3” series I/O modules only.
configure ports egress-rate-limit

    configure ports <portlist> egress-rate-limit [percent <percent> | rate <bps> [k | m]]

**Description**

Configures a maximum egress rate limit on the specified "3" series ports.

**Syntax Description**

- **portlist**: Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
- **percent**: Specifies the maximum percentage of bandwidth allowed for all egress traffic for each selected port. The default is 100. The range is 0 to 100.
- **bps**: Specifies the maximum kilobits per second (kbps) or megabits per second (mbps) allowed for all egress traffic for each selected port.
  - k—kbps (the range is 0-1000000)
  - m—mbps (the range is 0-1000)

**Default**

100 percent

**Usage Guidelines**

If you use the percent parameter to configure the egress rate limit, you must use an integer.

The rate <bps> range is:

- kbps—0 to 1000000
- mbps—0 to 1000

This setting is independent of any "i" series egress rate-limiting configurations that you have on the switch and is applied to the aggregate bandwidth after the "i" series per-queue egress rate-limiting.

**Example**

The following command sets the maximum egress rate limit on slot 1, port 1 to 100 mbps:

```
configure ports 1:1 egress-rate-limit rate 100 m
```

**History**

This command was first available in ExtremeWare 7.1.

**Platform Availability**

This command is available on "3" series I/O modules only.
configure qosprofile ingress

configure qosprofile ingress <Ingress QOS profile> [minbw <percent> % | committed-rate <bps> [k | m] peak-rate <bps> [k | m]] red-threshold <percent> % maxbuf <percent> % ports [<portlist> | all]

Description
Modifies the default ingress QoS profile parameters.

Syntax Description

<table>
<thead>
<tr>
<th>Ingress QoS profile</th>
<th>Specifies an ingress QoS profile: IQP1 through IQP8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>minbw</td>
<td>Specifies the minimum bandwidth percentage for this queue. The default setting is 0. The range is 0 to 100.</td>
</tr>
<tr>
<td>maxbw</td>
<td>Specifies the maximum bandwidth percentage for this queue. The default setting is 100. The range is 0 to 100.</td>
</tr>
<tr>
<td>committed-rate</td>
<td>Specifies the minimum bandwidth for this queue in either kilobits per second (kbps) or megabits per second (mbps). k—kbps (the range is 0 – 1000000) m—mbps (the range is 0 – 1000)</td>
</tr>
<tr>
<td>peak-rate</td>
<td>Specifies the maximum bandwidth for this queue in either kilobits per second (kbps) or megabits per second (mbps). k—kbps (the range is 0-1000000) m—mbps (the range is 0-1000)</td>
</tr>
<tr>
<td>red-threshold</td>
<td>Random Early Drop (RED) specifies the ingress queue fill percentage when the “3” series module begins to randomly discard packets as the queue fill percentage approaches the maximum queue size. The default setting is 100. The range is 0 to 100.</td>
</tr>
<tr>
<td>maxbuf</td>
<td>Specifies the ingress queue size as a percentage of the maximum size available. The range is 0 to 100. The default is 100.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all “3” series ports.</td>
</tr>
</tbody>
</table>

Default
- Minimum bandwidth—0%
- Maximum bandwidth—100%
- RED threshold—100%
- Maximum buffer percent—100%

Usage Guidelines
The sum of the committed rate and the equivalent rate for the configured minbw percent for all ingress queues on a port must not exceed the following:
- 250 mpbs for 4:1 oversubscribed platforms (GM-16T³, GM-16X³, and G24T³)
- 500 mpbs for 2:1 oversubscribed platforms (G16X³)
Example
The following command configures the ingress QoS profile parameters of ingress QoS profile IQP1 for slot 1, port 1:

```
configure qosprofile ingress iqpl committed-rate 250 m peak-rate 1000 m red-threshold 100 % maxbuf 100 % ports 1:1
```

History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is available on "3" series I/O modules only.
**configure qostype ingress priority**

```plaintext
configure qostype ingress priority [diffserv | dot1p | vlan | application] <qos-priority (0-15)>
```

**Description**
Configures the relative priority among the different ingress queue selection criteria.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>diffserv</td>
<td>Specifies the priority of the ingress queue based on DiffServ information. The default is 3.</td>
</tr>
<tr>
<td>dot1p</td>
<td>Specifies the priority of the ingress queue based on dot1p information. The default is 1.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies the priority of the ingress queue based on VLAN information. The default is 2.</td>
</tr>
<tr>
<td>application</td>
<td>Specifies the priority of the ingress queue selection based on application examination rules (IP protocol number and TCP/UDP port numbers). The default is 5.</td>
</tr>
<tr>
<td>qos-priority (0-15)</td>
<td>Specifies a priority value in the range of 0-15 (15 is the highest priority).</td>
</tr>
</tbody>
</table>

**Default**
- diffserv—3
- dot1p—1
- vlan—2
- application—5

**Usage Guidelines**

Ingress QoS types with a greater value take higher precedence.

The queue selection criteria with the highest priority, if enabled in the received packet, is used first, followed by the remaining criteria in descending order.

The priority range is 0-15 (15 is the highest priority). Each queue selection criteria must have a unique priority; no two selection criteria can have the same priority range.

All VLANs are set to the default ingress QoS profile *none*.

Congestion can cause ingress traffic to be dropped on oversubscribed "3" series I/O modules. Ingress QoS allows received traffic with different VLAN priority values, different DiffServ code points (IP TOS), or from different VLANS to be classified to up to eight different ingress queues. This allows for specified traffic types to be queued separately so they remain unaffected by congestion in other ingress queues.

To configure which DiffServ code points map to which ingress QoS profiles, use the command:
```
configure diffserv examination code-point <code-point> qosprofile <qosprofile> ports [<portlist> | all]
```

By default, DiffServ mapping is enabled on "3" series ports.
To disable the DiffServ mapping of an ingress IP packet to be examined to select a QoS profile, use the command:

disable diffserv examination [portlist | all]

**NOTE**

*Untagged packets are always dot1q vlan tagged internally. Therefore, ingress classification based on dot1p is always valid if there are no higher priority classifications that are valid. Configuring the ingress qostype priority for “dot1p” above any other classification method will effectively disable that classification. Untagged packets get their dot1p vlan priority bits set to the value configured by configure vlan <vlan> qosprofile <QoS Profile Name> and configure port <port> qosprofile <QoS Profile Name>.*

**Example**

The following command forces dot1p QoS to take a higher precedence over VLAN QoS (with a default priority of 2):

configure qostype ingress priority dot1p 4

**History**

This command was first available in ExtremeWare 7.0.1.

This command was modified in ExtremeWare 7.2 to support the new ingress queue selection criteria for application examination.

**Platform Availability**

This command is available on “3” series I/O modules only.
configure vlan qosprofile ingress

configure vlan <vlan name> qosprofile ingress [<Ingress QOS profile> | none]

Description
Configures a VLAN to use a specific ingress QoS profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>Ingress QoS profile</td>
<td>Specifies an ingress QoS profile: IQP1 through IQP8.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that traffic from this VLAN is not associated with any ingress queue based on VLAN ID.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
Use this command when the ingress QoS type priority is VLAN-based for a given received packet.

The `none` keyword allows VLAN priority ingress queue selection to put higher priority frames into a different queue so they do not get discarded during ingress port congestion.

All VLANs are set to the default ingress QoS profile `none`.

To display the ingress QoS profile mapping for a VLAN, use the command:

```
show vlan
```

The “3” series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

Example
The following command configures the VLAN `sales` to use ingress QoS profile `iqp2`:

```
configure vlan sales qosprofile ingress iqp2
```

History
This command was first available in ExtremeWare 7.0.1.

Platform Availability
This command is available on “3” series I/O modules only.
**create application examination**

```create application examination <application name> [ip-protocol <number> | [tcp-port | udp-port] <number> match [source-only | dest-only | source-or-dest] ] [<Ingress QOS profile> | none] precedence <(1-65000)>```  

**Description**

Configures ingress queue classification based on application QoS.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application name</td>
<td>Specifies the name string to associate with this rule.</td>
</tr>
<tr>
<td>ip-protocol</td>
<td>Specifies that a match will be attempted on the IP protocol number in the received packets.</td>
</tr>
<tr>
<td>tcp-port</td>
<td>Specifies that a match will be attempted on the TCP port numbers in the received packets.</td>
</tr>
<tr>
<td>udp-port</td>
<td>Specifies that a match will be attempted on the UDP port numbers in the received packets.</td>
</tr>
<tr>
<td>source-only</td>
<td>Specifies that when doing TCP or UDP comparisons, only source port numbers will be compared.</td>
</tr>
<tr>
<td>dest-only</td>
<td>Specifies that when doing TCP or UDP comparisons, only destination port numbers will be compared.</td>
</tr>
<tr>
<td>source-or-dest</td>
<td>Specifies that when doing TCP or UDP comparisons, both source and destination port numbers will be compared. The match is successful if either source or destination port equals the specified port number.</td>
</tr>
<tr>
<td>Ingress QoS profile</td>
<td>Specifies an ingress QoS profile name to associate with any ingress packets matching this rule.</td>
</tr>
<tr>
<td>none</td>
<td>Traffic matching this rule will not be associated with any ingress queue based on application examination.</td>
</tr>
<tr>
<td>precedence</td>
<td>Specifies the precedence value for this rule. If an incoming packets matches multiple rules, the precedence number is used to determine which rule to apply (lower number = higher precedence).</td>
</tr>
</tbody>
</table>

**Default**

None

**Usage Guidelines**

This command configures ingress queue classification based on application QoS (IP protocol number, TCP ports, or UDP ports). This command is similar to the existing `configure diffserv examination` except that it has more arguments and can overlap on the same ports, so an application name is used to identify each rule. The `none` instead of IQoS profile means that AQoS is not used for queue classification for the matching packets and the next lower ingress qosType priority (queue classification) is used. Precedence is required, since a match on multiple rules is possible. Up to 1,000 application examination rules can be created.

**Example**

The following command creates an application examination rule, TCP20, which will assign ingress TCP traffic with a destination port number of 20 to the ingress qosprofile IQP3 with a precedence value of 100:

```create application examination TCP20 tcp-port 20 match dest-only iqp3 precedence 100```
History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available on “3” series I/O modules only.
delete application examination

    delete {application examination} <application name>

**Description**

Deletes a previously configured application examination rule.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>application name</td>
<td>Specifies the name string to associate with this rule.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command deletes a previously configured application examination rule.

**Example**

The following command deletes the application examination rule:

```
delete application examination TCP20
```

**History**

This command was first available in ExtremeWare 7.2.

**Platform Availability**

This command is available on "3" series I/O modules only.
disable application examination ports

disable application examination ports [<portlist | all]

Description
Disables application examination rules on specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>portlist</th>
<th>all</th>
</tr>
</thead>
</table>
| Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8. | Specifies all “3” series ports.

Default
Disabled

Usage Guidelines
This command disables application examination rules on specified ports.

Example
The following command disables application examination rules on ports 2:6 through 2:8:
disable application examination ports 2:6-2:8

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available on “3” series I/O modules only.
disable diagnostics cable

_disable diagnostics cable port [<portlist> | all]

**Description**
Disables the automatic running of the Cable Diagnostics Module (CDM) to obtain cable diagnostics values for selected physical ports of the system.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Specifies one or more slots and ports. May be in the form 2:* , 2:5, 2:6-2:8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Specifies all “3” series ports.</td>
</tr>
</tbody>
</table>

**Default**
None

**Usage Guidelines**
This command disables the automatic running of cable diagnostics for selected physical ports of the system. This command also purges the cable diagnostics values for the selected ports from the CDM data structures.

To enable auto-diagnostics collection for selected ports, use the `enable diagnostics cable` command. To set the starting time for auto-diagnostics collection for selected ports, use the `configure diagnostics cable` command. To manually run cable diagnostics, use the `run diagnostics cable` command. To abort cable diagnostics current in progress, use the `abort diagnostics cable` command.

You cannot issue this command while the cable diagnostics process is in progress.

To view cable diagnostics data, use the `show diagnostics cable` command.

**Example**
The following command disables automatic running of cable diagnostics for all ports.

disable diagnostics cable port all

**History**
This command was first available in ExtremeWare 7.3.0.

**Platform Availability**
This command is available on “3” series I/O modules only.
disable diffserv ingress replacement ports

disable diffserv ingress replacement [high-priority | low-priority | low-and-high-priority] ports [<portlist> | all] {<Ingress QoS profile>}

Description
Disables the optional overwriting of the DiffServ code point portion of the (IP TOS) field for ingress traffic.

Syntax Description

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>high-priority</td>
<td>Specifies DiffServ replacement for high-priority traffic (traffic received below the committed-rate configured for the Ingress QoS profile).</td>
</tr>
<tr>
<td>low-priority</td>
<td>Specifies DiffServ replacement for low-priority traffic (traffic received above the committed-rate configured for the Ingress QoS profile).</td>
</tr>
<tr>
<td>low-and-high-priority</td>
<td>Specifies DiffServ replacement for both high-priority and low-priority traffic.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:* , 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all &quot;3&quot; series ports.</td>
</tr>
<tr>
<td>Ingress QoS profile</td>
<td>Specifies an optional ingress QoS profile: IQP1 through IQP8.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
The "3" series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

You can disable replacement for high-priority, low-priority, or low- and high-priority traffic for all ingress QoS profiles on the specified ports or a selected ingress QoS profile on the specified ports.

Example
The following command disables low-priority DiffServ replacement for all "3" series ports in all ingress QoS profiles:

disable diffserv ingress replacement low-priority ports all

History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is available on "3" series I/O modules only.
disable flow-control ports

    disable flow-control ports [<portlist> | all]

Description
Disables 802.3x flow control on "3" series ports.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all &quot;3&quot; series ports.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
If you disable flow control, use the following keywords:

- portlist to specify an individual "3" series port or a group of "3" series ports
- all to specify all "3" series ports

If you disable flow control on a "3" series port, the port does not advertise flow control support during auto-negotiation. Flow control is auto-negotiated and is disabled if both ports do not support it.

Example
The following command disables flow control on slot 2, ports 1 through 4:

disable flow-control ports 2:1-2:4

History
This command was first available in ExtremeWare 7.0.1.

Platform Availability
This command is available on "3" series I/O modules only.
enable application examination ports

```
enable application examination ports [<portlist | all]
```

**Description**
Enables application examination rules on specified ports.

**Syntax Description**

<table>
<thead>
<tr>
<th>Portlist</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*; 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all “3” series ports.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Guidelines**
This command enables application examination rules on specified ports.

**Example**
The following command enables application examination rules on ports 2:6 through 2:8:
```
enable application examination ports 2:6-2:8
```

**History**
This command was first available in ExtremeWare 7.2.

**Platform Availability**
This command is available on “3” series I/O modules only.
enable diagnostics cable

    enable diagnostics cable port [<portlist> | all]

Description
Enables the automatic running of the Cable Diagnostics Module (CDM) to obtain cable diagnostics values for selected physical ports of the system.

Syntax Description

```
portlist     Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.
all          Specifies all "3" series ports.
```

Default
None

Usage Guidelines
This command enables the automatic running of cable diagnostics for selected physical ports of the system. To set the starting time for auto-diagnostics collection for selected ports, use the `configure diagnostics cable` command. To disable auto-diagnostics collection for selected ports, use the `disable diagnostics cable` command. To manually run cable diagnostics, use the `run diagnostics cable` command. To abort cable diagnostics current in progress, use the `abort diagnostics cable` command.

You cannot issue this command while the cable diagnostics process is in progress.

To view cable diagnostics data, use the `show diagnostics cable` command.

Example
The following command enables automatic running of cable diagnostics for all ports.
```
enable diagnostics cable port all
```

History
This command was first available in ExtremeWare 7.3.0.

Platform Availability
This command is available on "3" series I/O modules only.
enable diffserv ingress replacement ports

enable diffserv ingress replacement [high-priority | low-priority | low-and-high-priority] ports [<portlist> | all] {<Ingress QoS profile>}

**Description**
Enables the optional overwriting of the DiffServ code point portion of the (IP TOS) field for ingress traffic.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>high-priority</td>
<td>Specifies DiffServ replacement for high-priority traffic (traffic received below the committed-rate configured for the Ingress QoS profile).</td>
</tr>
<tr>
<td>low-priority</td>
<td>Specifies DiffServ replacement for low-priority traffic (traffic received above the committed-rate configured for the Ingress QoS profile).</td>
</tr>
<tr>
<td>low-and-high-priority</td>
<td>Specifies DiffServ replacement for both high-priority and low-priority traffic.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all “3” series ports.</td>
</tr>
<tr>
<td>Ingress QoS profile</td>
<td>Specifies an optional ingress QoS profile: IQP1 through IQP8.</td>
</tr>
</tbody>
</table>

**Default**
Disabled

**Usage Guidelines**
If you enable DiffServ ingress replacement before you configure a code point, the default code point is 0. To configure a code point for both the low-priority and high-priority traffic, use the command:

```
configure diffserv ingress replacement low-priority code-point <number> high-priority code-point <number> ports [<portlist> | all] {<Ingress QoS profile>}
```

You can enable DiffServ ingress replacement for:

- Both high-priority and low-priority traffic on the specified ports or each ingress QoS profile on the specified ports.
- Either high-priority or low-priority traffic for all ingress QoS profiles on the specified ports or a selected ingress QoS profile on the specified ports.

The “3” series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

**Example**
The following command enables low-priority DiffServ replacement for all “3” series ports in all ingress QoS profiles:

```
enable diffserv ingress replacement low-priority ports all
```

**History**
This command was first available in ExtremeWare 7.1.
Platform Availability

This command is available on "3" series I/O modules only.
enable flow-control ports

enable flow-control ports [<portlist> | all]

Description
Enables 802.3x flow control on "3" series ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*; 2:5; 2:6-2:8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all &quot;3&quot; series ports.</td>
</tr>
</tbody>
</table>

Default
Disabled

Usage Guidelines
Since "3" series modules are oversubscribed to the module switch fabric, traffic can congest. Flow control allows you to stop incoming traffic when too much congestion occurs.

Flow control sends a PAUSE frame to the transmitter when traffic approaches the congestion threshold for a specific queue. The PAUSE frame is sent before the queue overflows, so throughput is slightly reduced when flow control is enabled. Flow control is auto-negotiated and is disabled if both ports do not support it.

If you enable flow control, use the following keywords:

- portlist to specify an individual port or a group of ports
- all to specify all "3" series ports

Example
The following command enables flow control on slot 2, ports 1 through 4:

```
enable flow-control ports 2:1-2:4
```

History
This command was first available in ExtremeWare 7.0.1.

Platform Availability
This command is available on "3" series I/O modules only.
run diagnostics cable

    run diagnostics cable port [<portlist> | all]

Description
Initiates the Cable Diagnostics Module (CDM) to obtain cable diagnostics values for the physical ports of the system.

Syntax Description

<table>
<thead>
<tr>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:* , 2:5, 2:6-8.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all &quot;3&quot; series ports.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
Use this command to obtain the following cable diagnostics data for each selected port:

- Time and date of test
- Cable length
- Pair status
- Pair skew
- Pair swap
- Fault len
- Polarity
- Speed

To view cable diagnostics data, use the show diagnostics cable command.

To enable auto-diagnostics collection for selected ports, use the enable diagnostics cable command. To set the starting time for auto-diagnostics collection for selected ports, use the configure diagnostics cable command. To disable auto-diagnostics collection for selected ports, use the disable diagnostics cable command. To abort cable diagnostics current in progress, use the abort diagnostics cable command.

You cannot issue this command while the cable diagnostics process is in progress.

Example
The following command starts the Cable Diagnostics Module (CDM) to obtain cable diagnostics values for ports 2:4 through 2:7:

run diagnostics cable port 2:4-2:7

History
This command was first available in ExtremeWare 7.3.0.
**Platform Availability**

This command is available on “3” series I/O modules only.
show application examination

    show {application examination} {<application name>}

Description
Displays configured application examination rules.

Syntax Description

| application name | Specifies the name string associated with the application examination rule. |

Default
N/A

Usage Guidelines
This command displays previously configured application examination rules. The keywords “application examination” are optional. If an application examination rule is not specified, all created rules will be displayed.

Example
The following command displays all configured application examination rules:

show application examination TCP20

Following is sample output from this command:

<table>
<thead>
<tr>
<th>IP</th>
<th>TCP/UDP</th>
<th>Name</th>
<th>Typ</th>
<th>Port</th>
<th>Match</th>
<th>Prt</th>
<th>Q</th>
<th>Prec</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP20</td>
<td>tcp</td>
<td>6</td>
<td>20</td>
<td>dst</td>
<td>IQP3</td>
<td>100</td>
<td></td>
<td></td>
<td>4:1, 4:2, 4:3, 4:4, 4:5, 4:6</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4:7, 4:8, 4:9, 4:10, 4:11, 4:12</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4:13, 4:14, 4:15, 4:16, 4:17, 4:18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>4:19, 4:20, 4:21, 4:22, 4:23, 4:24</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available on “3” series I/O modules only.
show diagnostics cable

show diagnostics cable {ports {<portlist> | all}} {mode {auto | manual | both} {detail}

Description
Displays cable diagnostics information currently stored in the Cable Diagnostics Module (CDM) data structures.

Syntax Description

| portlist | Specifies one or more slots and ports. May be in the form 2:*; 2:5; 2:6-2:8. |
| all      | Specifies all “3” series ports. The default value is all. |
| mode auto| Specifies that cable diagnostics data collected automatically should be displayed. The default is “both.” |
| mode manual | Specifies that cable diagnostics data collected manually should be displayed. The default is “both.” |
| mode both | Specifies that cable diagnostics data collected automatically and manually should be displayed. The default is “both.” |
| detail   | Specifies that cable diagnostics data should be displayed in detail format. The default format is summary. |

Default

- ports—all: If the optional ports keyword is not used, the show listing includes all ports.
- mode—both: If the optional mode keyword is not used, data collected from both the last manual run and the last automatic run are displayed.
- detail—detail: If the optional detail keyword is not used, a summary listing is generated.

Usage Guidelines
Use this command to display or print the following cable diagnostics data for each selected port:

- Time and date of test
- Cable length (meters)
- Pair status
- Pair skew
- Pair swap
- Fault length (meters)
- Polarity
- Speed (Mbps)

You can configure the CDM to obtain diagnostics information automatically through the configure diagnostics cable command; or you can manually obtain cable diagnostics at any time by issuing the run diagnostics cable command. You can use the show diagnostics cable command to view cable diagnostics data captured from either the latest CDM manual run or automatic run; or you can view data captured from both the manual and automatic runs.
To enable auto-diagnostics collection for selected ports, use the `enable diagnostics cable` command. To disable auto-diagnostics collection for selected ports, use the `disable diagnostics cable` command. To set the starting time for auto-diagnostics collection for selected ports, use the `configure diagnostics cable` command. To manually run cable diagnostics, use the `run diagnostics cable` command.

Example

The following command displays cable diagnostics information in detail format for ports 1 through 3 on slot 6:

```
show diagnostics cable port 6:1-6:3 detail
```

Following is sample detailed diagnostic output from this command:

```
========================================================
Manual Diagnostics Collected @ Thu Jan 29 02:48:29 2004
========================================================

<table>
<thead>
<tr>
<th>Port</th>
<th>Speed (Mbps)</th>
<th>Avg Len (meters)</th>
<th>Pair</th>
<th>Fault Loc</th>
<th>Skew (ns)</th>
<th>Polarity Status</th>
<th>Channel-AB</th>
<th>Channel-CD</th>
<th>Diagnostic-Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:1</td>
<td>1000</td>
<td>10</td>
<td>1-2</td>
<td>No Fault</td>
<td>8 ns</td>
<td>Unknown</td>
<td>Ok</td>
<td>No-Swap</td>
<td>Unknown Manual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3-6</td>
<td>No Fault</td>
<td>0 ns</td>
<td>Unknown</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4-5</td>
<td>No Fault</td>
<td>8 ns</td>
<td>Unknown</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7-8</td>
<td>No Fault</td>
<td>8 ns</td>
<td>Unknown</td>
<td>Ok</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:2</td>
<td>1000</td>
<td>5</td>
<td>1-2</td>
<td>6</td>
<td></td>
<td>Unknown</td>
<td>Positive Open</td>
<td>Swap</td>
<td>Unknown Manual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3-6</td>
<td>6</td>
<td></td>
<td>Unknown</td>
<td>Negative Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4-5</td>
<td>6</td>
<td></td>
<td>Unknown</td>
<td>Positive Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7-8</td>
<td>5</td>
<td></td>
<td>Unknown</td>
<td>Positive Open</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6:3</td>
<td>1000</td>
<td>6</td>
<td>1-2</td>
<td>0</td>
<td></td>
<td>Unknown</td>
<td>Imp-Err</td>
<td>Unknown</td>
<td>Unknown Manual</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3-6</td>
<td>0</td>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4-5</td>
<td>0</td>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Open</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>7-8</td>
<td>0</td>
<td></td>
<td>Unknown</td>
<td>Unknown</td>
<td>Open</td>
<td></td>
</tr>
</tbody>
</table>

The following command displays cable diagnostics information in summary format for port 1 on slot 6:

```
show diagnostics cable port 6:1
```

Following is sample summary diagnostic output from this command:

```
========================================================
Manual Diagnostics Collected @ Fri Jan 16 03:41:54 2004
========================================================

<table>
<thead>
<tr>
<th>Port</th>
<th>Speed (MB)</th>
<th>Pair</th>
<th>Cable Diagnostic-Mode</th>
</tr>
</thead>
<tbody>
<tr>
<td>6:1</td>
<td>1000</td>
<td>1-2</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>3-6</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4-5</td>
<td>Ok</td>
</tr>
<tr>
<td></td>
<td></td>
<td>7-8</td>
<td>Ok</td>
</tr>
</tbody>
</table>
```

History

This command was first available in ExtremeWare 7.3.0.
Platform Availability
This command is available on “3” series I/O modules only.
show ports egress-rate-limit

    show ports {<portlist>} egress-rate-limit

Description
Displays the maximum egress rate limit on the specified “3” series ports.

Syntax Description

| portlist | Specifies one or more slots and ports. May be in the form 2:* , 2:5, 2:6-2:8. |

Default
N/A

Usage Guidelines
Depending on the port egress rate limit configuration, the maximum port bandwidth is displayed in the numeric rate (kbps or mbps) or the percentage rate.

This command applies only to “3” series I/O modules; the rate you configure is applicable to the aggregate of all outgoing traffic on a port.

This display is independent of any “i” series egress rate-limiting configurations that you have on the switch.

Example
The following command displays the maximum egress rate limit:

show ports egress-rate-limit

Following is sample output from this command:

<table>
<thead>
<tr>
<th>PORT</th>
<th>Egress-Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>2:1</td>
<td>100 %</td>
</tr>
<tr>
<td>2:2</td>
<td>100 %</td>
</tr>
<tr>
<td>2:3</td>
<td>100 %</td>
</tr>
<tr>
<td>2:4</td>
<td>1000 k</td>
</tr>
<tr>
<td>2:5</td>
<td>100 %</td>
</tr>
<tr>
<td>2:6</td>
<td>100 %</td>
</tr>
<tr>
<td>2:7</td>
<td>100 %</td>
</tr>
<tr>
<td>2:8</td>
<td>100 %</td>
</tr>
<tr>
<td>2:9</td>
<td>100 %</td>
</tr>
<tr>
<td>2:10</td>
<td>100 %</td>
</tr>
<tr>
<td>2:11</td>
<td>100 %</td>
</tr>
<tr>
<td>2:12</td>
<td>100 %</td>
</tr>
<tr>
<td>2:13</td>
<td>100 %</td>
</tr>
<tr>
<td>2:14</td>
<td>100 %</td>
</tr>
<tr>
<td>2:15</td>
<td>100 %</td>
</tr>
<tr>
<td>2:16</td>
<td>100 %</td>
</tr>
</tbody>
</table>
History
This command was first available in ExtremeWare 7.1.

Platform Availability
This command is available on “3” series I/O modules only.
show ports ingress stats

    show ports {<portlist>} ingress stats {detail}

Description
Displays real-time ingress statistics for one or more “3” series ports.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies more detailed information per ingress queue.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The “3” series I/O modules support eight ingress QoS profiles (IQP1 - IQP8).

High-priority packets are packets received below the configured ingress committed rate, and
low-priority packets are packets received above the committed-rate.

View these statistics to analyze usage trends and to maximize network efficiency.

If you do not specify the detail keyword, the output indicates the following:

- **Port Number**
- **Link Status**—The current status of the link. Options are:
  - Ready (R): The port is ready to accept a link.
  - Active (A): The link is present at this port.
  - Disabled (D): The link is disabled at this port.
  - Not Present (NP): The link is not present at this port.
- **High Priority Bytes**—Sum, per port, of the bytes forwarded for received high-priority packets (traffic received below the committed rate configured for the ingress QoS profile).
- **Low Priority Bytes**—Sum, per port, of the bytes forwarded for received low-priority packets (traffic received above the committed rate configured for the ingress QoS profile).
- **Received Total Bytes**—The total number of bytes that were received by the port.
- **Receive Bytes Dropped**—Total number of bytes dropped for this port.
- **Total Percent Dropped**—Percentage of incoming bytes dropped due to oversubscription congestion or ingress rate limiting. Displayed with a precision of 1/100 of a percent.
- **Transmit XOFF**—Total number of XOFF flow control packets sent from this port.

If you specify the detail keyword, the following additional information is displayed per ingress queue:

- **Queue**—One of eight ingress queue names for this port.
- **High Priority Bytes**—Sum, per ingress queue, of the bytes forwarded for received high-priority packets.
- **Low Priority Bytes**—Sum, per ingress queue, of the bytes forwarded for received low-priority packets.
- **Total Percent Dropped**—Percentage of incoming bytes on this queue dropped due to oversubscription congestion. This is determined using cumulative counters, so is not a rate. This will be displayed with a precision of 1%.
- **Byte Rates**—The following three rate values will always either add up to 0% or 100%:
  - **High Priority Percentage**—The ratio of high priority traffic forwarded on this queue to the total bytes received on this queue.
  - **Low Priority Percentage**—The ratio of low priority traffic forwarded on this queue to the total bytes received on this queue.
  - **Dropped Percentage**—Percentage of receive bytes dropped by this queue relative to the total number of bytes input to this queue.

**Example**

The following command displays real-time ingress statistics for slot 1, port 1:

```plaintext
show ports 1:1 ingress stats
```

Following is sample output from this command:

```plaintext
Port Statistics                                       Thu Jul 10 08:24:50 2003
Port   Link     High Pri      Low Pri     Rx Total     Rx Drop      %       Tx
Status        Bytes        Bytes        Bytes       Bytes   Drop     Xoff
================================================================================
1:1    R          500          400         1000        100  10.00       5
```

The following command displays real-time ingress statistics for slot 1, port 1 and per ingress queue:

```plaintext
show ports 1:1 ingress stats detail
```

Following is sample output from this command:

```plaintext
Port Statistics                                       Thu Jul 10 08:24:50 2003
Port   Link     High Pri      Low Pri     Rx Total     Rx Drop      %       Tx
Status        Bytes        Bytes        Bytes       Bytes   Drop     Xoff
================================================================================
1:1    R          500          400         1000        100  10.00       5
```

```plaintext
Queue     High Pri     Low Pri   Total % |---------- RATES -----------|
Bytes       Bytes   Dropped  High Pri   Low Pri   Dropped
=======================================================================
IQP1          500           0       0 %     100 %       0 %       0 %
IQP2            0         400      20 %       0 %      80 %      20 %
IQP3            0           0       0 %       0 %       0 %       0 %
IQP4            0           0       0 %       0 %       0 %       0 %
IQP5            0           0       0 %       0 %       0 %       0 %
IQP6            0           0       0 %       0 %       0 %       0 %
IQP7            0           0       0 %       0 %       0 %       0 %
IQP8            0           0       0 %       0 %       0 %       0 %
```
History
This command was first available in ExtremeWare 7.0.1.

Platform Availability
This command is available on “3” series I/O modules only.
show qosprofile ingress

  show qosprofile ingress {<Ingress QoS profile>} {<portlist>}

Description
Displays ingress QoS profiles.

Syntax Description

<table>
<thead>
<tr>
<th>Ingress QoS profile</th>
<th>Specifies an ingress QoS profile: IQP1 through IQP8.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
If you do not specify an ingress QoS profile, all ingress QoS profiles for the specified ports are displayed.

The units displayed are the same units that you used when you configured the ingress QoS profile.

Example
The following command displays ingress QoS profile information for all ingress QoS profiles on slot 1:

show qosprofile ingress 1:*

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Queue</th>
<th>MinBw %/</th>
<th>Committed-Rate</th>
<th>MaxBw %/</th>
<th>Peak-Rate</th>
<th>RED %</th>
<th>MaxBuf %</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>IQP1</td>
<td>1000 k</td>
<td>1000 m</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP2</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP3</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP4</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP5</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP6</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP7</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP8</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td>1:2</td>
<td>IQP1</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP2</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP3</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP4</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP5</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
<tr>
<td></td>
<td>IQP6</td>
<td>0 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td>100 %</td>
<td></td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 7.1.
Platform Availability

This command is available on "3" series I/O modules only.
show qostype ingress priority

Description
Displays ingress QoS priority settings.

Syntax Description
This command has no syntax or values.

Default
N/A

Usage Guidelines
None

Example
The following command displays the ingress QoS traffic grouping priority settings for this switch:
show qostype ingress priority

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Ingress QoS Type</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>5</td>
</tr>
<tr>
<td>Diffserv</td>
<td>3</td>
</tr>
<tr>
<td>Vlan</td>
<td>2</td>
</tr>
<tr>
<td>Dot1p</td>
<td>1</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 7.0.1.

This command was modified in ExtremeWare 7.2 to include the application criteria.

Platform Availability
This command is available on “3” series I/O modules only.
unconfigure diffserv ingress replacement ports

    unconfigure diffserv ingress replacement ports [<portlist> | all]

**Description**
Resets the optional overwriting of the DiffServ code point portion of the IP TOS field for ingress traffic to its defaults.

**Syntax Description**

| portlist | Specifies one or more slots and ports. May be in the form 2:* , 2:5, 2:6-2:8. |
| all      | Specifies all “3” series ports.                                        |

**Default**
N/A

**Usage Guidelines**
Use this command to reset the low-priority and high-priority code point values to 0 and to disable DiffServ ingress replacement.

**Example**
The following command resets the DiffServ code points to their defaults:
unconfigure diffserv ingress replacement ports all

**History**
This command was first available in ExtremeWare 7.1.

**Platform Availability**
This command is available on “3” series I/O modules only.
unconfigure qostype ingress priority

Description
Restores all ingress QoS settings to their defaults.

Syntax Description
This command has no syntax or values.

Default
N/A

Usage Guidelines
Resets the ingress traffic groupings to the following:
• application—5
• diffserv—3
• dot1p—1
• vlan—2

Example
The following command resets the Ingress QoS traffic grouping priorities:
unconfigure qostype ingress priority

History
This command was first available in ExtremeWare 7.0.1.
This command was modified in ExtremeWare 7.2 to include the application criteria.

Platform Availability
This command is available on “3” series I/O modules only.
Power over Ethernet (PoE) is an effective method of supplying 48 VDC power to certain types of powered devices (PDs) through Category 5 or Category 3 twisted pair Ethernet cables. Powered devices include the Altitude 300 wireless port, IP telephones, laptop computers, web cameras, and other devices. With PoE, a single Ethernet cable supplies power and the data connection, reducing costs associated with separate power cabling and supply. PoE for ExtremeWare includes a method of detection to assure that power is delivered only to devices that meet the IEEE 802.3af specification for PoE.

**NOTE**

PoE features are supported only by the Summit 300 series switches, the Summit 400-24p switch, and the Alpine FM-32Pi PoE Module.

**Summary of PoE Software Features**

The Alpine FM-32Pi PoE Module, Summit 300 series switches, and Summit 400-24p switch support the following PoE software features:

- Configuration and control of the power distribution for PoE at the system (slot) level (Alpine FM-32Pi module only)
- Configuration and control of the power distribution for PoE at the port level
- Real-time detection of powered devices on the line
- Monitor and control of PoE fault conditions
- Support for configuring and monitoring PoE status at the port level
- Management of an over-subscribed power budget

**Port Power Management**

When you connect PDs, the PoE device automatically discovers and classifies those that are AF-compliant. The following functions are supported for delivering power to specific ports:

- Enabling the port for discovery and classification
- Enabling power delivery to a discovered device
Power Over Ethernet Commands—Summit 300 and 400-24p Switches and Alpine PoE Module

- Enforcing port power limits by denying power to a device that exceeds the power limit
- Enforcing class limits by denying power to a device that exceeds the class limit
- Reporting and tracking port power faults
- Managing power budgets and allocation

In addition, the Summit 300-24 and Summit 400-24p switches also support legacy devices that are not 802.3AF compliant.

For more conceptual information about configuring and managing PoE, see the ExtremeWare Software User Guide.
clear inline-power connection-history slot

    clear inline-power connection-history slot <slot_number>

Description

Clears the port connection history for the specified slot.

NOTE

This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switches.

Syntax Description

<table>
<thead>
<tr>
<th>slot_number</th>
<th>Specifies the slot for which the port connection history is cleared.</th>
</tr>
</thead>
</table>

Default

N/A

Usage Guidelines

None

Example

The following command clears the port connection history for slot 2:

clear inline-power connection-history slot 2

History

This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability

This command is available only on the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.
clear inline-power fault ports

    clear inline-power fault ports <portlist>

Description
Clears the fault condition on the specified ports.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
None

Example
The following command clears the fault condition for port 3:

```
clear inline-power fault ports 3
```

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available on the Alpine FM-32Pi PoE Module, the Summit 300 series switches, and the Summit 400-24p switch.
clear inline-power stats
clear inline-power stats ports

For the Alpine series I/O modules:
    clear inline-power stats ports <portlist>

For the Summit 300-48 switch:
    clear inline-power stats <portlist>

Description
Clears the inline statistics for the selected port to zero.

Syntax Description

| portlist | Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 2:*, 2:5, 2:6-2:8. |

Default
N/A

Usage Guidelines
Use this command to clear all the information displayed by the show inline-power stats ports <portlist> command.

Example
The following command clears the inline statistics for ports 1-8 on slot 1:
    clear inline-power stats ports 1:1-1:8

On a Summit 300 switch, the equivalent command is:
    clear inline-power stats 1-8

The following command displays cleared inline power configuration information for ports 1-8 in slot 1:
    show inline-power stats ports 1:1-1:8

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Class</th>
<th>Absent</th>
<th>InvSig</th>
<th>Denied</th>
<th>OverCurrent</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:2</td>
<td>delivering class0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:3</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:4</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:5</td>
<td>searching</td>
<td>------</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:6</td>
<td>delivering class3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:7</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:8</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
History

This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability

This command is available on the Alpine FM-32Pi PoE Module, the Summit 300 series switches, and the Summit 400-24p switch.
configure inline-power backup-source

configure inline-power backup-source [internal | none] slot <slot_number>

Description
Configures the backup power supply for the external 48V power source.

**NOTE**
This command is available only for the Alpine FM-32Pi PoE Module.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>internal</td>
<td>Specifies that the internal power supply will serve as the backup power supply if the external 48V power source loses power.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that there is no backup power supply if the external 48V power source loses power. In this case, the ports will not be able to provide power.</td>
</tr>
<tr>
<td>slot_number</td>
<td>Specifies the slot for which the backup power supply is being configured.</td>
</tr>
</tbody>
</table>

Default
None

Usage Guidelines
This command lets you specify whether or not there is a backup power supply to the external 48V power source. If `internal` is selected, the internal power supply is brought up if the external 48V loses power. If `none` is selected, no other power supply is brought up if the external 48V loses power. In that case, the ports will not be able to provide power.

Example
The following command sets the internal power supply as the backup power supply to the external 48V power supply for slot 1:
```
config inline-power backup-source internal slot 1
```

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules.
configure inline-power budget

configure inline-power budget <watts> slot <slot_number>

Description
Configures the amount of power available for inline-power on the slot.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>watts</td>
<td>An integer specifying wattage in the range of 1 to 450 W.</td>
</tr>
<tr>
<td>slot_number</td>
<td>Specifies the slot being configured for power.</td>
</tr>
</tbody>
</table>

Default
15.4 W

Usage Guidelines
Before issuing this command, disable the slot using the disable inline-power slots <slot_id> command. The device is allowed to draw about 10% more power than the configured amount before power is shut off to the device.

Example
The following example configures slot 1 at 10 watts.

disable inline-power slot 1
configure inline-power budget 10 slot 1

History
This command was first available in ExtremeWare 7.3e

Platform Availability
This command is available only on the Summit 300-48 switches.
configure inline-power detection

configure inline-power detection [auto | discovery-test-only] ports <portlist>

Description
Sets the power detection mechanism on the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Forces automatic power discovery operations and specifies that power will be supplied to detected power devices (PDs) for the specified ports.</td>
</tr>
<tr>
<td>discovery-test-only</td>
<td>Forces power discovery operations and specifies that power will not be supplied to detected PDs for the specified ports.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:* 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

Default
Auto

Usage Guidelines
This command controls the power detection mechanism on the specified ports. Test mode forces power discovery operations; however, power is not supplied to detected PDs.

Example
The following command forces automatic power discovery operations and specifies that power will be supplied to detected PDs for ports 4 – 6 on slot 3:

```
configure inline-power detection auto ports 3:4-3:6
```

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
configure inline-power disconnect-precedence

configure inline-power disconnect-precedence [lowest-priority | deny-port]

Description
Controls the disconnect function of power management.

NOTE
This command is available only on the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lowest-priority</td>
<td>Specifies that the port with the lowest priority is to be shut down when the next port connects.</td>
</tr>
<tr>
<td>deny-port</td>
<td>Specifies that the next port is denied power, regardless of priority.</td>
</tr>
</tbody>
</table>

Default
Deny-port

Usage Guidelines
The PoE controller disconnects one of the ports to prevent an overload on the power supply. The disconnect function occurs when the power drain exceeds the available power budget because of a rise in power consumption after power is allocated to the ports.

Example
The following example configures the disconnect precedence to disconnect the lowest priority port when the next port attempts to connect:

configure inline-power disconnect-precedence lowest-priority

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available only on the Summit 300-48 switch.
configure inline-power display-string
configure inline-power label ports

For the Alpine series PoE modules:

    configure inline-power display-string <string> ports <portlist>

For the Summit 300-48 switch:

    configure inline-power label <string> ports <portlist>

Description

Lets you create your own label for a specified power port.

NOTE

This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>string</th>
<th>Specifies a name up to 13 characters long to identify the specified power port(s).</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:<em>, 1:5, 1:6-1:8, 2:</em>, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default

No label

Usage Guidelines

Use the `show inline-power configuration port <portlist>` command, as shown in the following example, to display inline power configuration information, including the display string (if any) for each port. The display string is shown under the “Label” column:

    show inline-power configuration port 1:1-1:7

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Config</th>
<th>Detect</th>
<th>Rsvd Pwr</th>
<th>Oper Lmt</th>
<th>Viol Prec</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
<td>max-class-operator</td>
</tr>
<tr>
<td>1:2</td>
<td>enabled</td>
<td>auto</td>
<td>10.0</td>
<td>15.4</td>
<td>advertised-limit</td>
<td>test_port2</td>
</tr>
<tr>
<td>1:3</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
<td>max-class-operator</td>
</tr>
<tr>
<td>1:4</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
<td>max-class-operator</td>
</tr>
<tr>
<td>1:5</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
<td>max-class-operator</td>
</tr>
<tr>
<td>1:6</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
<td>max-class-operator</td>
</tr>
<tr>
<td>1:7</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td></td>
<td>max-class-operator</td>
</tr>
</tbody>
</table>

Example

On an Alpine switch, the following command assigns the name alpha-test_1 to port 1 on slot 4:

    config inline-power display-string alpha-test_1 ports 4:1
On a Summit 300 switch, the following command assigns the name alpha-test_1 to port 1 on slot 1:
configure inline-power label alpha-test_1 ports 1:1

**History**
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
configure inline-power operator-limit ports

configure inline-power operator-limit <milliwatts> ports <portlist>

Description
Sets the maximum power on the specified ports to either the default value or the specified watts.

Syntax Description

<table>
<thead>
<tr>
<th>milliwatts</th>
<th>An integer specifying milliwatts in the range of 3000 – 20000 mW. On the Summit 300-24 or 400-24p, an integer specifying milliwatts in the range of 3000 – 15400 mW.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:<em>, 1:5, 1:6-1:8, 2:</em>, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
15400 mW

Usage Guidelines
The Summit 300-24 or 400-24p switch has an operator limit range of 300 to 15400 milliwatts. The Summit 300-48 and Alpine switches have an operator limit range of 300 to 20000 milliwatts.

The standard 802.3af protocol permits a powered device to be classified into one of 5 classes, each of which determines the maximal power draw to the power sourcing equipment (PSE). Extreme PSEs, in the default configuration, use the classification-to-power draw in performing power management and budgeting.

Classification is optional, and many powered devices do not support it. Therefore, under normal conditions, the Extreme PSE budgets for the maximum permitted power (15.4 watts), even though the maximum device draw may be less. This may cause fewer devices to be powered, since the power budget is prematurely exhausted. There is a wide variation in power consumption levels between 802.3af classes (~8 watts). In such cases, the power level limit (operator-limit) can be set on a per port basis. If this is done, the operator limit, rather than the discovered class limit will be used for power budgeting. It is also necessary for the violation-precedence to be set to operator-limit.

Regardless of how the port power limit is derived (through automatic classification or operator limit), the port power limit is used to determine whether the overall system limit has been exceeded. On the Summit 300-48 switch, after the overall system limit is reached, additional PoE ports are powered based on the system violation-precedence setting and port power priority. The Summit 300-24 and 400-24p switches have sufficient power to support 15.4 watts on all 24 ports.

The power port limit is also used during system operation to limit the power supplied to each PoE port. If a powered device attempts to draw more power than has been budgeted, the chassis will remove power from that port to prevent system overload or device damage.

This command sets the limit on the specified ports to either the default value or the specified watts. The range is 3000-20000 mW. The default value is 15400 mW minimum. This command is used in
conjunction with the violation precedence and has no effect if either none or advertised-class is selected for violation precedence using the following command:

```
configure inline-power violation-precedence [advertised-class | operator-limit | max-class-operator | none] ports <portlist>
```

**Example**

The following command sets the limit to 10000 mW on ports 3 – 6 of slot 5:

```
config inline-power operator-limit 10000 ports 5:3-5:6
```

**History**

This command was first available in ExtremeWare 7.2.

This command was added to the Summit "e" series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available on Alpine FM32-Pi PoE Modules, the Summit 300 series switches, and the Summit 400-24p switch.
configure inline-power power-supply

configure inline-power power-supply [redundant | load-sharing]

Description
This command selects the power supply operating mode.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>redundant</td>
<td>Specifies redundant power supply mode.</td>
</tr>
<tr>
<td>load-sharing</td>
<td>Specifies load-sharing mode.</td>
</tr>
</tbody>
</table>

Default
Redundant mode

Usage Guidelines
The PoE subsystem on the Summit 300-48 switch supports dual power supplies for either redundant or load-sharing modes. Redundant mode is the default and provides hitless PoE should one of the two power supplies fail, be removed, or powered off. Load-sharing mode allows both power supplies to provide power to the PoE system, providing greater PoE power capacity. For load-sharing operation, the amount of power provided to the PoE system is the sum of the power supplied by the power supplies. With load-sharing, all PoE devices may experience a power hit if a power supply fails.

Example
The following command configures a Summit 300-48 switch for redundant power supply mode:

```bash
configure inline-power power-supply redundant
```

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available only on the Summit 300-48 switch.
configure inline-power priority

configure inline-power priority [low | high | critical] ports <portlist>

Description
Configures the port priority.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>low</td>
<td>Specifies that the port is to have low priority, which is the default value. Ports with this priority level are given power only after all critical and high priority ports have power.</td>
</tr>
<tr>
<td>high</td>
<td>Specifies that the port is to have high priority. Ports with this priority level are given power only after all critical ports have power.</td>
</tr>
<tr>
<td>critical</td>
<td>Specifies that the port is to have critical priority. Ports with this priority receive power first.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 1:1, 1:2, 1:3-1:5.</td>
</tr>
</tbody>
</table>

Default
Low priority

Usage Guidelines
Power is allocated to ports by their designated priority. Power allocation is first provided to the higher priority ports.

Example
The following example sets port 5 as a critical power port:

```
configure inline-power priority critical ports 5
```

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available only on the Summit 300-48 switch.
configure inline-power reserved budget

configure inline-power reserved budget <milliwatts> ports <portlist>

Description
Sets the reserved power on the specified ports to either the default value or the specified watts.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>milliwatts</td>
<td>An integer specifying milliwatts at zero (0) or in the range of 3000 – 20000 mW.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
0 mW

Usage Guidelines
This command sets the reserved power on the specified ports to either the default value or the specified watts. The reserved power range is 0 or 3000-20000 mW. The default reserved power range value is 0 mW. Total power reserved may be up to but not greater than the total power for the module. If all the power available to the module is reserved, the common power pool is empty.

Example
The following command sets the reserved power for all the ports on slot 4 to 15000 mW:
config inline-power reserved budget 15000 ports 4:*

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
configure inline-power type

```
configure inline-power type [phone | webcam | wireless | other] ports <portlist>
```

**Description**

Sets the type of powered device (PD) connected to the specified ports.

**NOTE**

*This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>phone</td>
<td>Specifies the PD connected to the specified port as a phone.</td>
</tr>
<tr>
<td>webcam</td>
<td>Specifies the PD connected to the specified port as a webcam.</td>
</tr>
<tr>
<td>wireless</td>
<td>Specifies the PD connected to the specified port as a wireless device.</td>
</tr>
<tr>
<td>other</td>
<td>Specifies the PD connected to the specified port as a power device other than a phone, a webcam, or a wireless device.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command sets the type of powered device connected to the specified ports. This is a management-controlled entity because there is no support for dynamically determining the powered device type.

Use the `detail port` argument in the `show inline-power info [port <portlist] | detail port <portlist>` command to display the inline-power type for a selected port.

**Examples**

The following command specifies the type of powered device connected to port 3 on slot 4 as a wireless device on an Alpine switch:

```
configure inline-power type wireless ports 4:3
```

The following command specifies the type of powered device connected to port 3 as a wireless device on a Summit 300-48 switch:

```
configure inline-power type wireless ports 1:3
```

**History**

This command was first available in ExtremeWare 7.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
Platform Availability

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
configure inline-power usage-threshold

configure inline-power usage-threshold <threshold>

Description
Sets the inline power usage alarm threshold.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>threshold</td>
<td>Integer in the range 1 – 99 expressed as a percentage for derating of available power to measured power. The default value is 70 on the Summit 300-48 switch, the Summit 400-24p switch, or the Alpine series I/O modules. The default value is 90 on the Summit 300-24 switch.</td>
</tr>
</tbody>
</table>

Default
Alpine series FM-32Pi PoE Module: 70
Summit 300-24 switch: 90
Summit 300-48 switch: 70
Summit 400-24p switch: 70

Usage Guidelines
This command sets the threshold for initiation of an alarm if the measured power exceeds the threshold.

On the Alpine FM-32Pi PoE Module and the Summit 300-48 switch, the alarm threshold is shared between the system-level utilization and the allocated power budget per slot. If either measurement exceeds the threshold level, an alarm will be initiated.

On the Summit 400-24p switch, the usage threshold is not shared with the system usage; rather, it is power used by the PDs only.

Example
The following command sets the inline power usage alarm threshold at 75%:
configure inline-power usage-threshold 75

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit "e" series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
configure inline-power violation-precedence ports

configure inline-power violation-precedence [advertised-class | operator-limit | max-class-operator | none] ports <portlist>

Description
Sets the violation precedence for the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>advertised-class</td>
<td>Removes or denies power if an IEEE 802.3af-compliant power device (PD) consumes power beyond its advertised class limit.</td>
</tr>
<tr>
<td>operator-limit</td>
<td>Removes or denies power if the PD consumes power beyond the configured operator limit.</td>
</tr>
<tr>
<td>max-class-operator</td>
<td>Removes or denies power if the PD consumes power beyond the detected class limit or the operator limit, whichever is greater. Max-class-operator is the default value, which allows operation of 802.3af compliant PDs.</td>
</tr>
<tr>
<td>none</td>
<td>Removes or denies power if the PD exceeds the maximum limit of 20 watts.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default
max-class-operator

Usage Guidelines
This command sets the violation precedence for the specified ports. Power will be removed or denied to PDs connected to the selected ports if the PD consumes more power than the entered limit. The default value is max-class-operator, which removes or denies power if the PD consumes power beyond the greater value of the detected class limit or the configured operator limit, whichever is greater. The operator limit is configured with the following command:

`configure inline-power operator-limit <milliwatts> ports <portlist>`

Example
The following command sets the violation precedence for port 3 on slot 5 to the configured operator limit:

`configure inline-power violation-precedence operator-limit ports 5:3`

History
This command was first available in ExtremeWare 7.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
Platform Availability

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
disable inline-power

disable inline-power

Description
Shuts down power currently provided on all ports on all slots.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description
This command has no arguments or variables.

Default
Enable

Usage Guidelines
You can control whether inline power is provided to the system by using the disable inline-power command and the enable inline-power command. Using the disable inline-power command shuts down power currently provided on all ports on all slots. By default, inline power provided to the system is enabled.

Example
The following command shuts down power currently provided on all ports on all slots:

disable inline-power

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
disable inline-power legacy

disable inline-power legacy

Description
Disables legacy (802.3af compliant) devices from being detected by the PoE subsystem.

NOTE
This command is available only for the Summit 300-24 and 400-24p switches.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
The Summit 300-24 or 400-24p switch can power devices that are compliant with the IEEE 802.3af Power over Ethernet standard. The `enable inline-power legacy` command allows powering of PoE devices built before the standard was approved.

If all the devices connected to the switch are 802.3af standards compliant, it is advisable to keep the default setting of disabled for legacy device support.

You can determine whether a device connected to the switch is standards compliant or not by using the `show inline-power info [port <portlist | detail port <portlist]` command. The detailed status line shows if the device is 802.3af standards compliant.

Sample output from the show inline-power info detail ports command follows:

Summit 300-24:3 # show inline-power info detail ports 5

PORT - 5

Configured Admin State: Enabled
  Inline Power State: delivering
  MIB Detect Status: delivering
  Label:
  Violation Precedence: max-class-operator
  Operator Limit: 15400 milliwatts
  Inline Type: other
    PD Class: class3
  Max Allowed Power: 15.400 W
  Measured Power: 6.90 W
  Line Voltage: 50.2 Volts
  Current: 117 mA
  Fault Status: None (D 0)
  Detailed Status: valid resistor detected, 802.3af-compliant PD was detected
Example
The following command disables 802.3af compliant devices:

disable inline-power legacy

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the Summit 300-24 and 400-24p switches only.
disable inline-power ports

For the Alpine series I/O modules:

    disable inline-power [ports all | <portlist>]

For the Summit 300 series switches:

    disable inline-power ports <portlist>]

Description
Disables power provided by all system ports or specified ports.

**NOTE**

This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ports all</td>
<td>Disables power on all system ports. Applies only to the Alpine I/O modules.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more ports or slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

Default

Enabled

Usage Guidelines

You can control whether inline power is provided by all system ports or specified ports by using the disable inline-power [ports all | <portlist>] command and the enable inline-power [ports all | <portlist>] commands. Using the disable inline-power [ports all | <portlist>] command shuts down power currently provided by all system ports or specified ports. The system defaults to enabling power on all 10/100 ports.

To power any port, the following conditions must exist:

- The system must be enabled for power.
- The slot must be enabled for power.
- The ports must be enabled for power.

Disabling a port providing power to a powered device (PD) immediately removes power to the PD.

Example

The following command shuts down power currently provided by port 2 on slot 3:

```
disable inline-power 3:2
```

History

This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
disable inline-power slots

For the Alpine FM-32Pi PoE Module:
   disable inline-power slots <slot_id>

For the Summit 300 series switches:
   disable inline-power slot <slot_id>

Description

Disables power provided to the specified slot.

NOTE

This command is available only on the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| slot_id | Specifies the slot for which power will be disabled. |

Default

Enable

Usage Guidelines

You can control whether inline power is provided to a specific slot by using the disable inline-power slots <slot_id> command and the enable inline-power slots <slot_id> command. Using the disable inline-power slots <slot_id> command shuts down power currently provided to the selected slot. The system defaults to enabling power on all slots.

To power any port, the following conditions must exist:

- The system must be enabled for power.
- The slot must be enabled for power.
- The ports must be enabled for power.

Disabling a slot providing power to a powered device (PD) through one of its powered ports immediately removes power to the PD.

Example

The following command shuts down power currently provided by slot 2:
   disable inline-power slots 3

History

This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
Platform Availability

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
download firmware slot

download firmware slot <slot_number>

Description
Downloads firmware to the micro controller if the firmware needs to be upgraded.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module.

Syntax Description

| slot_number | Specifies the slot for which firmware will be downloaded to the micro controller. |

Default
None

Usage Guidelines
This command downloads firmware to the micro controller if needed. A version of PoE firmware is built into ExtremeWare just in case there is some corruption in the current firmware. A clean copy can be retrieved. ExtremeWare will log a message in syslog prompting for a firmware upgrade. This command is used to download the firmware. This command is available only if the board is present in the slot. This same command will be used for any other products that have firmware built into ExtremeWare.

Example
The following command downloads firmware to the micro controller for the board in slot 2:

download firmware slot 2

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules.
enable inline-power

Description
Enables power currently provided on all ports on all slots, except for the ports that are explicitly disabled by the disable inline-power ports command.

Syntax Description
This command has no arguments or variables.

Default
Enabled

Usage Guidelines
You can control whether inline power is provided to the system by using the disable inline-power command and the enable inline-power command. Using the enable inline-power command makes power available on all ports on all slots. Using the disable inline-power command shuts down power currently provided on all ports on all slots. By default, inline power provided to the system is enabled. To shut down power to a specific port, use the disable inline-power ports command.

Example
The following command enables power currently provided on all ports on all slots:

```
enable inline-power
```

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
enable inline-power legacy

enable inline-power legacy

**Description**

Enables legacy (802.3af compliant) devices to be detected by the PoE subsystem.

**NOTE**

*This command is available only for the Summit 300-24 and 400-24p switches.*

**Syntax Description**

This command has no arguments or variables.

**Default**

Disabled

**Usage Guidelines**

The Summit 300-24 or 400-24p switch can power devices that are compliant to the IEEE 802.3af Power over Ethernet standard. The `enable inline-power legacy` command allows PoE devices built before the standard was approved to be powered.

If all the devices connected to the switch are 802.3af standards compliant, it is advised to keep the default setting of disabled for legacy device support.

You can determine whether a device connected to the switch is standards compliant or not by using the `show inline-power info [port <portlist] | detail port <portlist>` command. The detailed status line shows if the device is 802.3af standards compliant.

Sample output from the show inline-power info detail ports command follows:

```
Summit 300-24:3 # show inline-power info detail ports 5
PORT - 5
Configured Admin State: Enabled
Inline Power State: delivering
MIB Detect Status: delivering
Label: 
Violation Precedence: max-class-operator
Operator Limit: 15400 milliwatts
Inline Type: other
PD Class: class3
Max Allowed Power: 15.400 W
Measured Power: 6.90 W
Line Voltage: 50.2 Volts
Current: 117 mA
Fault Status: None (D 0)
Detailed Status: valid resistor detected, 802.3af-compliant PD was detected
```

To disable legacy devices, use the `disable inline-power legacy` command.
Example
The following command enables 802.3af compliant devices:

```
enable inline-power legacy
```

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available only on the Summit 300-24 and 400-24p switch.es
enable inline-power ports

For the Alpine series I/O modules:
   enable inline-power [ports all | <portlist>]

For the Summit 300-48 switch:
   enable inline-power ports <portlist>

Description

Enables power provided by all system ports or specified ports.

NOTE

This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ports all</td>
<td>Enables power on all system ports. Applies only to Alpine series I/O modules.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports on which power will be enabled. May be in the form 2:*, 2:5, 2:6-2:8.</td>
</tr>
</tbody>
</table>

Default

Enable

Usage Guidelines

You can control whether inline power is provided by all system ports or specified ports by using the `disable inline-power [ports all | <portlist>]` command and the `enable inline-power [ports all | <portlist>]` command. Using the `enable inline-power [ports all | <portlist>]` command makes power available to all system ports or specified ports. Using the `disable inline-power [ports all | <portlist>]` command shuts down power currently provided by all system ports or specified ports. The system defaults to enabling power on all 10/100 ports.

To power any port, the following conditions must exist:

- The system must be enabled for power.
- The slot must be enabled for power.
- The ports must be enabled for power.

Disabling a port providing power to a powered device (PD) immediately removes power to the PD.

Example

The following command enables power currently provided by port 2 on slot 3:

```
enable inline-power 3:2
```
History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
enable inline-power slots

For the Alpine series I/O modules:
    enable inline-power slots <slot_id>
For the Summit 300-48 switch:
    enable inline-power slot <slot_id>

Description
Enables power provided to the specified slot.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| slot_id | Specifies the slot for which power will be enabled. |

Default
Enabled

Usage Guidelines
You can control whether inline power is provided to a specific slot by using the disable inline-power slots <slot_id> command and the enable inline-power slots <slot_id> command. Using the enable inline-power slots <slot_id> command makes power available to the selected slot. Using the disable inline-power slots <slot_id> command shuts down power currently provided to the selected slot. The system defaults to enabling power on all slots.

To power any port, the following conditions must exist:
- The system must be enabled for power.
- The slot must be enabled for power.
- The ports must be enabled for power.

Disabling a slot providing power to a powered device (PD) through one of its powered ports immediately removes power to the PD.

Example
The following command makes power available to slot 2:
    enable inline-power slots 2

History
This command was first available in ExtremeWare 7.2.
This command was first available in ExtremeWare 7.3e.
Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
reset inline-power ports

reset inline-power ports <portlist>

Description
Power cycles the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| portlist | Specifies one or more slots and ports for which power is to be reset. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8. |

Default
N/A

Usage Guidelines
This command power cycles the specified ports. Ports are immediately de-powered and re-powered, maintaining current power allocations.

Example
The following command resets power for port 4:
reset inline-power ports 4

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
reset inline-power slot

reset inline-power slot <slot number>

Description
Resets the specified slot.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description

| slot | Specifies that the PoE system is to use a specific slot. |

Default
N/A

Usage Guidelines
This command resets the specified slots. Slots are immediately de-powered and re-powered, maintaining current power allocations.

Example
The following command resets power for slot 1:

```
reset inline-power slot 1
```

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the Summit 300-48 only.
show inline-power

Description
Displays inline power status information for the system.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
The output indicates the following inline power status information for the system:

- System maximum inline power—The nominal power available, in watts.
- Configured System Power Usage—The configured power usage threshold for the system, shown in watts and as a percentage of available power.

The output indicates the following inline power status information for each slot:

- Main PSU Status—The operational status of the main power supply unit. The status conditions are:
  - ON: Power is being provided to the PoE controller.
  - OFF: Power is not being provided to the PoE controller.
  - FAULT: An error has occurred.
- Backup PSU Status—The condition of the backup power device, indicated by the following information:
  - State: Present, Not Present, Fault
  - Status: ACTIVATED, DEACTIVATED

Valid State/Status combinations are:

- Present, ACTIVATED
- Present, DEACTIVATED
- Not Present
- Fault

- Firmware Status—The condition of the firmware, indicated by one the following states:
  - Initializing—Firmware is still coming up.
  - Operational—Firmware is up and running.
  - Download failure—Firmware failed to download properly.
— Needs calibrating—Firmware downloaded properly or is up and running, but values stored in EEPROM are invalid. The unit should be returned to Extreme Networks Service for recalibration.
— Image not found—No firmware image found.
— Version mismatch—Firmware version does not match what the system expects for this particular ExtremeWare release.
— Invalid—Firmware was corrupted. Repeat the firmware download.

Example

The following command displays inline power status for the system:

```
show inline-power
```

Following is sample output from this command:

```
Inline Power System Information
System maximum inline-power: 32 watts
Power Usage: 70% (22 watts)
```

<table>
<thead>
<tr>
<th>Slot</th>
<th>Main PSU Status</th>
<th>Backup PSU Status</th>
<th>Firmware Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>OFF</td>
<td>Present, ACTIVATED</td>
<td>Operational</td>
</tr>
</tbody>
</table>

History

This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
show inline-power configuration port

    show inline-power configuration port <portlist>

Description
Displays inline power configuration information for the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| portlist | Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8. |

Default
N/A

Usage Guidelines
The output displays the following inline power configuration information for the specified ports:

- **Config**—Indicates whether the port is enabled to provide power:
  - Enabled: The port is available to provide power.
  - Disabled: The port is not available to provide power.
- **Detect**—Indicates the detect level:
  - Auto: The port will power up if there is enough available power.
  - Test: The port will not power up. Indicates a test mode to determine whether the port can be discovered.
- **Rsvd Pwr**—Displays the amount of configured reserved power in watts.
- **Oper Lmt**—Displays the configured operator limit in watts. The operator limit is used only with violation precedence.
- **Viol Prec**—Displays the violation precedence settings:
  - ADVERTISED-LIMIT: Removes or denies power if an IEEE 802.3af-compliant powered device (PD) consumes power beyond its advertised class limit.
  - OPERATOR-LIMIT: Removes or denies power if the PD consumes power beyond the configured operator limit.
  - MAX-CLASS-OPERATOR: Removes or denies power if the PD consumes power beyond the maximum of the detected class limit or the operator limit.
  - NONE: Removes or denies power if the PD consumes power in excess of the regulatory maximum allowable wattage.
- **Label**—Displays a text string, up to 13 characters in length, associated with the port.
Example

The following command displays inline power configuration information for ports 1-7 in slot 1:

```
show inline-power configuration port 1:1-1:7
```

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>Config</th>
<th>Detect</th>
<th>Rsvd Pwr</th>
<th>Oper Lmt</th>
<th>Viol Prec</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td>max-class-operator</td>
<td></td>
</tr>
<tr>
<td>1:2</td>
<td>enabled</td>
<td>auto</td>
<td>10.0</td>
<td>15.4</td>
<td>advertised-limit test_port2</td>
<td></td>
</tr>
<tr>
<td>1:3</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td>max-class-operator</td>
<td></td>
</tr>
<tr>
<td>1:4</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td>max-class-operator</td>
<td></td>
</tr>
<tr>
<td>1:5</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td>max-class-operator</td>
<td></td>
</tr>
<tr>
<td>1:6</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td>max-class-operator test_port6</td>
<td></td>
</tr>
<tr>
<td>1:7</td>
<td>enabled</td>
<td>auto</td>
<td>0.0</td>
<td>15.4</td>
<td>max-class-operator</td>
<td></td>
</tr>
</tbody>
</table>

History

This command was first available in ExtremeWare 7.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
show inline-power configuration slot

    show inline-power configuration slot <slotlist>

Description
Displays inline power configuration information for the specified slots.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| slotlist | Specifies one or more slots. |

Default
N/A

Usage Guidelines
The output displays the following inline power configuration information for the specified slots:

- **Status**—Indicates power status:
  - Enabled: The slot is available to provide power.
  - Disabled: The slot is not available to provide power.
- **Cfg PSU Backup**—Indicates the current setting of power source precedence:
  - Internal
  - None
- **PSU Active**—Indicates the power source currently supplying power:
  - Internal
  - External
- **Usage Threshold**—Displays the configured alarm threshold as a percentage.
- **Connection Order**—Displays the list of ports (1 – 32) by current connection order. (Maximum for the Alpine module is 32 ports.)

Example
The following command displays inline power configuration information for slot 1:
    show inline-power configuration slot 1

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Status</th>
<th>Cfg PSU Backup</th>
<th>PSU Active</th>
<th>Usage Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Enabled</td>
<td>Internal</td>
<td>Internal</td>
<td>70%</td>
</tr>
</tbody>
</table>
**History**
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
show inline-power info
show inline-power info port

For the Alpine series I/O modules:
  show inline-power info [port <portlist | detail port <portlist]
For the Summit 300-48 switch:
  show inline-power info [detail] port <portlist]

Description
Displays inline power information for the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Generates a detailed report.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
You can use this command to generate a summary report or a detailed report.

Summary output displays the following inline power information for the specified ports:

- State—Displays the port power state:
  - Disabled
  - Searching
  - Discovered
  - Delivering
  - Faulted
  - Disconnected
  - Other
  - Denied
- Class—Displays the class type:
  - “-----”: disabled or searching
  - “class0”: class 0 device
— “class1”: class 1 device
— “class2”: class 2 device
— “class3”: class 3 device
— “class4”: class 4 device

• Connect History—Displays the connection order of the port from the connection history (if one exists):
  — 0: No connection history exists or the port is not in the history list.
  — 1 – 32: There is a connection history and the port is in the history list.

• Volts—Displays the measured voltage. A value from 0 – 2V is valid for ports that are in a searching or discovered state.

• Curr—Displays the measure current in milli Amps (mA).

• Res—Displays the measured resistance in kilo Ohms (Kohms). A value greater than 100 Kohms indicates an empty port.

• Power—Displays the measured power in watts.

• Fault—Displays the fault value:
  — 0: No fault
  — 1: Over voltage
  — 2: Over voltage spike
  — 3: Peak over current
  — 4: Overload
  — 8: Discovery resistance failed
  — 9: Class violation
  — 10: Disconnect
  — 11: Discovery resistance, A2D fail
  — 12: Classify, A2D fail
  — 13: Sample A2D fail
  — 14: Device fault, A2D fail

The detail command lists all inline power information for the selected ports. Detail output displays the following information:

• Configured Admin State
• Inline Power State
• MIB Detect Status
• Label
• Violation Precedence
• Operator Limit
• Detection
• Reserved Power
• Inline Type
• Connect Order
• PD Class
• Max Allowed Power
• Measured Power
• Line Voltage
• Discovered Resistance
• Discovered Capacitance
• Current
• Fault Status

**Example**

The following command displays summary inline power information for port 1:

```
show inline info port 1:
```

Following is sample output from this command:

```
Port State  Class  Connect  Volts  Curr  Res  Power  Fault  History
   (mA)   (Kohms)   (Watts)
--- ----- ------- ------ ------ ------ ------- ------ --------
 1:1 searching ----- 0 0.0 0 0.0 0.00 0
```

The following command displays detail inline power information for port 1:

```
show inline info detail port 1:1
```

Following is sample output from this command:

```
Configured Admin State: Enabled
Inline Power State: searching
MIB Detect SStatus: searching
    Label: 
Violation Precedence: max-class-operator
    Operator Limit: 15400 milliwatts
    Detection: auto
    Reserved Power: 0 milliwatts
    Inline Type: other
    Connect Order: none
    PD Class:
    Max Allowed Power: 0.0 W
    Measured Power: 0.0 W
    Line Voltage: 0.0 Volts
    Discovered Resistance: 0.0K ohms
    Discovered Capacitance: 0 uF
    Current: 0 mA
    Fault Status: None
```

**History**

This command was first available in ExtremeWare 7.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
**Platform Availability**

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
show inline-power slot

  show inline-power slot <slotlist>

Description
Displays inline power information for the specified slots.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

<table>
<thead>
<tr>
<th>slotlist</th>
<th>Specifies one or more slots.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
The output displays the following inline power information for the specified slots:

• Common Power:
  — Configured: Displays in watts the configured amount of common power available. This amount is equal to the total amount of configured power minus the amount of configured reserved power.
  — Allocated: Displays in watts the amount of common power allocated.

• Reserved Power:
  — Configured: Displays in watts the amount of power configured as reserved.
  — Allocated: Displays in watts the amount of reserved power utilized.

• Measured Usage—Displays measured power in watts.

Example
The following command displays inline power information for slot 1:
show inline-power slot 1

Following is sample output from this command for the Alpine switches:

<table>
<thead>
<tr>
<th>Slot</th>
<th>Common Power</th>
<th>Reserved Power</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Configured</td>
<td>Configured</td>
</tr>
<tr>
<td>1</td>
<td>22000mW</td>
<td>10000mW</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.
Platform Availability

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
show inline-power stats ports

    show inline-power stats ports <portlist>

Description
Displays inline power statistics for the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| portlist | Specifies one or more slots and ports. May be in the form 1:1, 1:2, 1:3-1:5 2:* , 2:5, 2:6-2:8. |

Default
N/A

Usage Guidelines
The output displays the following inline power statistics for the specified ports:

- **State**—Displays the inline power state:
  - Disabled
  - Searching
  - Discovered
  - Delivering
  - Faulted
  - Disconnected
  - Other
  - Denied

- **Class**—Displays the class type:
  - “-----”: disabled or searching
  - “class0”: class 0 device
  - “class1”: class 1 device
  - “class2”: class 2 device
  - “class3”: class 3 device
  - “class4”: class 4 device

- **Absent**—Displays the number of times the port was disconnected.
- **InvSig**—Displays the number of times the port had an invalid signature.
- **Denied**—Displays the number of times the port was denied.
- **Over-current**—Displays the number of times the port entered an over-current state.
• Short—Displays the number of times the port entered under-current state.

Example
The following command displays inline power configuration information for ports 1-8 in slot 1:

```
show inline-power stats ports 1:1-1:8
```

Following is sample output from this command:

<table>
<thead>
<tr>
<th>Port</th>
<th>State</th>
<th>Class</th>
<th>Absent</th>
<th>InvSig</th>
<th>Denied</th>
<th>OverCurrent</th>
<th>Short</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:2</td>
<td>delivering</td>
<td>class0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:3</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:4</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:5</td>
<td>searching</td>
<td>------</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:6</td>
<td>delivering</td>
<td>class3</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:7</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>1:8</td>
<td>searching</td>
<td>------</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
show inline-power stats slot

    show inline-power stats slot <slotlist>

Description
Displays inline power statistics for the specified slots.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

    slotlist  Specifies one or more slots.

Default
N/A

Usage Guidelines
Use this command to produce a report that shows how many ports are faulted, powered, and waiting for power for the selected slots.

Example
The following command displays inline power statistics information for slot 1:
show inline-power stats slot 1

Following is sample output from this command:
PoE firmware status: Operational
PoE firmware revision: 1.6
Connection Order: 3 15
Total ports powered: 1
Total ports waiting for power: 0
Total ports faulted: 0
Total ports disabled: 1

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
unconfigure inline-power backup-source slot

unconfigure inline-power backup-source slot <slot_number>

Description
Resets the backup power source to its default for the specified slot. Does not take effect until the power is cycled on the slot.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot_number</td>
<td>Specifies the slot for which the backup power source will be reset to its default.</td>
</tr>
</tbody>
</table>

Default
Internal

Usage Guidelines
This command resets the backup power source that was configured with the following command:

```
command inline-power backup-source [internal | none] slot <slot_number>
```

Resetting the backup power source to its default for the specified slot does not take effect until the power is cycled on the slot.

Example
The following command resets the backup power source to its default for slot 1:

```
unconfig inline-power backup-source slot 1
```

History
This command was first available in ExtremeWare 7.2.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules.
unconfigure inline-power detection ports

unconfigure inline-power detection ports <portlist>

Description
Resets the power detection scheme to the default for the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| portlist  | Specifies one or more slots and ports. May be in the form 2:*, 2:5, 2:6-2:8. |

Default
N/A

Usage Guidelines
This command resets the power detection scheme that was configured with the following command:

configure inline-power detection [auto | discovery-test-only] ports <portlist>

Example
The following command resets the power detection scheme to its default for port 1 on slot 1:

unconfig inline-power detection ports 1:1

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
unconfigure inline-power disconnect-precedence

Description
Returns the disconnect-precedence to the default value.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description
This command has no arguments or variables.

Default
Deny-port

Usage Guidelines
The PoE controller disconnects one of the ports to prevent an overload on the power supply. The
disconnect function occurs when the power drain exceeds the available power budget because of a rise
in power consumption after power is allocated to the ports.

Example
The following example configures the disconnect precedence to disconnect the next port regardless of
priority:

unconfigure inline-power disconnect-precedence

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on the Summit 300-48 only.
**unconfigure inline-power operator-limit ports**

```
unconfigure inline-power operator-limit ports <portlist>
```

**Description**

Resets the operator limit back to the default for the specified ports.

**NOTE**

*This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.*

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8.</td>
</tr>
</tbody>
</table>

**Default**

The default operator limit is 15400 mW.

**Usage Guidelines**

This command resets the operator limit that was configured with the following command:

```
configure inline-power operator-limit <milliwatts> ports <portlist>
```

The Summit 300-24 or 400-24p switch has an operator limit range of 300 to 15400 milliwatts. The Summit 300-48 switch has an operator limit range of 300 to 20000 milliwatts.

**Example**

The following command resets the operator limit to its default for port 2 on slot 1:

```
unconfig inline-power operator-limit ports 1:2
```

**History**

This command was first available in ExtremeWare 7.2.

This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

**Platform Availability**

This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
unconfigure inline-power power-supply

unconfigure inline-power power-supply

Description
Sets the power supply mode to the default setting of redundant mode.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description
This command has no arguments or variables.

Usage Guidelines
The Summit 300-48 PoE subsystem supports dual power supplies for either redundant or load-sharing modes. Redundant mode is the default and provides hitless PoE should one of the two power supplies fail, be removed, or powered off. Load-sharing mode allows both power supplies to provide power to the PoE system, providing greater PoE power capacity. For load-sharing operation, the amount of power provided to the PoE system is the sum of the power supplied by the power supplies.

Example
The following command returns a Summit 300-48 switch to redundant power supply mode:

unconfigure inline-power power-supply

History
This command was first available in ExtremeWare 7.3e

Platform Availability
This command is available on the Summit 300-48 switch only.
unconfigure inline-power priority ports

unconfigure inline-power priority ports <portlist>

Description
Resets one or more ports to the default value of low priority.

NOTE
This command is available only for the Summit 300-48 switch.

Syntax Description
| portlist | Specifies one or more slots and ports. May be in the form 1:1,1:2, 1:3-1:5. |

Default
Low priority

Usage Guidelines
Power is allocated to ports by their designated priority. Power allocation is first provided to the higher priority ports.

Example
The following example resets port 1:5 to low priority:
unconfigure inline-power priority ports 1:5

History
This command was first available in ExtremeWare 7.3e.

Platform Availability
This command is available on Summit 300-48 only.
unconfigure inline-power reserved-budget ports

unconfigure inline-power reserved-budget ports <portlist>

Description
Resets the reserved budget back to the default value.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| portlist | Specifies one or more slots and ports. On a modular switch, can be a list of slots and ports. On a stand-alone switch, can be one or more port numbers. May be in the form 1, 2, 3-5, 1:*, 1:5, 1:6-1:8. |

Default
The default reserved budget value is 0 mW.

Usage Guidelines
This command resets to default the reserved power budget that was configured with one of the following commands:

configure inline-power reserved budget <milliwatts> ports <portlist>

Example
The following command resets the reserved power budget to its default for port 3 on slot 1:

unconfig inline-power reserved-budget ports 1:3

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
unconfigure inline-power usage-threshold

    unconfigure inline-power usage-threshold

Description
Resets the inline power usage threshold to the default value.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description
This command has no arguments or variables.

Default
The default value for the inline power usage threshold is 70 percent.

Usage Guidelines
This command resets to default the inline power usage threshold that was configured with the following command:

configure inline-power usage-threshold

Example
The following command resets the inline power usage threshold to its default value:

unconfig inline-power usage-threshold

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
unconfigure inline-power violation-precedence ports

unconfigure inline-power violation-precedence ports <portlist>

Description
Resets violation precedence to the default value for the specified ports.

NOTE
This command is available only for the Alpine FM-32Pi PoE Module and the Summit 300-48 switch.

Syntax Description

| portlist | Specifies one or more slots and ports. May be in the form 2:, 2:5, 2:6-2:8. |

Default
The default violation precedence value is max-class-operator.

Usage Guidelines
This command resets the violation precedence that was configured with the following command:

configure inline-power violation-precedence [advertised-class | operator-limit | max-class-operator | none] ports <portlist>

Example
The following command resets the violation precedence to its default value for port 3 on slot 1:

unconfig inline-power violation-precedence ports 1:3

History
This command was first available in ExtremeWare 7.2.
This command was added to the Summit “e” series of switches in ExtremeWare 7.3e.

Platform Availability
This command is available only on Alpine FM32-Pi PoE Modules and the Summit 300-48 switch.
This chapter describes the commands developed to support the Link Layer Discovery Protocol (LLDP) feature.

The Link Layer Discovery Protocol (LLDP) is a Layer 2 protocol (IEEE standard 802.1ab) that is used to determine the port capabilities of devices such as repeaters, bridges, access points, routers, and wireless stations. The ExtremeWare 7.5 support for LLDP enables devices to advertise their capabilities and media specific configuration information, and to learn the same information from the devices connected to it. The information is represented in Type Length Value (TLV) format for each data item. The 802.1ab specification provides detailed TLV information.
configure lldp ports management-address

configure lldp ports [all | <portlist>] [advertise | no-advertise] management-address

**Description**
Configures LLDP ports to advertise or not advertise management address information to its neighbors.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

**Default**
The default is not to advertise.

**Usage Guidelines**
N/A.

**Example**
The following command advertises address information for port 1:5.

```
configure lldp ports 1:5 advertise management-address
```

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on all Extreme switches.
configure lldp ports port-description

configure lldp ports [all | <portlist>] [advertise | no-advertise] port-description

Description
Configures LLDP ports to advertise or not advertise port description information to its neighbors.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*; i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

Default
The default is not to advertise.

Usage Guidelines
N/A.

Example
The following command configures port 1:7 to not advertise the port description information to neighbors.

configure lldp ports 1:7 no-advertise port-description

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp ports system-capabilities

configure lldp ports [all | <portlist>] [advertise | no-advertise] system-capabilities

Description
Configures LLDP ports to advertise or not to advertise its system capabilities to its neighbors.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

Default
The default is not to advertise.

Usage Guidelines
N/A.

Example
The following command configures all ports to advertise system capability information to neighbors.

configure lldp ports all advertise system-capabilities

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
**configure lldp ports system-description**

configure lldp ports [all | <portlist>] [advertise | no-advertise] system-description

**Description**
Configures LLDP ports to advertise or not to advertise its system description to its neighbors.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

**Default**
The default is not to advertise.

**Usage Guidelines**
N/A.

**Example**
The following command configures port 1:4 through port 1:8 to not advertise the system description information to neighbors.

configure lldp ports 1:4 - 1:8 no-advertise system-description

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on all Extreme switches.
configure lldp ports system-name

configure lldp ports [all | <portlist>] [advertise | no-advertise] system-name

**Description**
Configures LLDP ports to advertise or not to advertise its system name to its neighbors.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

**Default**
The default is not to advertise.

**Usage Guidelines**
N/A.

**Example**
The following command configures port 1:6 to advertise the system name to neighbors.

```bash
configure lldp ports 1:4 - 1:8 no-advertise system-name
```

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on all Extreme switches.
configure lldp ports vendor-specific dot1 port-protocol-vlan-ID

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot1 port-protocol-vlan-ID [<cr> | vlan [all | <vlan name>]]

Description
Configures LLDP ports to advertise or not advertise port VLAN information to its neighbors. Since this is a vendor specific option, there may not be support for this from the neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*; i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
<tr>
<td>all</td>
<td>Applies to all VLANs.</td>
</tr>
<tr>
<td>vlan name</td>
<td>Applies to the specified VLANs.</td>
</tr>
</tbody>
</table>

Default
The default is not to advertise.

Usage Guidelines
N/A.

Example
The following command configures all ports to advertise port VLAN information to neighbors.
```
configure lldp ports all advertise vendor-specific dot1 port-protocol-vlan-id
```

The following command configures port 1:5 to advertise information about VLAN vlannew to neighbors.
```
configure lldp ports 1:5 advertise vendor-specific dot1 port-protocol-vlan-id vlan vlannew
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp ports vendor-specific dot1 port-vlan-ID

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot1 port-vlan-ID

Description
Configures LLDP ports to advertise or not advertise port vlan ID information to its neighbors. This allows a VLAN bridge port to advertise the port VLAN identifier that will be associated with untagged or priority-tagged frames. Since this is a vendor specific option, there may not be support for this from the neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

Default
The default is not to advertise.

Usage Guidelines
N/A.

Example
The following command configures all ports to advertise port vlan ID information to neighbors.

configure lldp ports all advertise vendor-specific dot1 port-vlan-ID

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp ports vendor-specific dot1 protocol-identity

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot1 protocol-identity

Description

Configures LLDP ports to advertise or not advertise protocol identity information to its neighbors. This allows an 802 LAN station to advertise the particular protocols that are accessible through the port. Since this is a vendor specific option, there may not be support for this from the neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i*, t:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

Default

The default is not to advertise.

Usage Guidelines

N/A.

Example

The following command configures all ports to not advertise protocol-identity information to neighbors.

configure lldp ports all no-advertise vendor-specific dot1 protocol-identity

History

This command was first available in ExtremeWare 7.4.

Platform Availability

This command is available on all Extreme switches.
configure lldp ports vendor-specific dot1 vlan-name

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot1 vlan-name

**Description**

Configures LLDP ports to advertise or not advertise VLAN name information to its neighbors. This allows an IEEE 802.1Q-compatible 802 LAN station to advertise the assigned name of any VLAN with which it is configured. Since this is a vendor specific option, there may not be support for this from the neighbor.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

**Default**

The default is not to advertise.

**Usage Guidelines**

N/A.

**Example**

The following command configures all ports to not advertise VLAN name information to neighbors.

configure lldp ports all no-advertise vendor-specific dot1 vlan-name

**History**

This command was first available in ExtremeWare 7.4.

**Platform Availability**

This command is available on all Extreme switches.
configure lldp ports vendor-specific dot3 link-aggregation

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot3 link-aggregation

**Description**

Configures LLDP ports to advertise or not advertise link aggregation capabilities to its neighbors. Since this is a vendor specific option, there may not be support for this from the neighbor.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:* , i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

**Default**

The default is not to advertise.

**Usage Guidelines**

N/A.

**Example**

The following command configures port 1:12 to not advertise link aggregation capabilities to neighbors.

```
configure lldp ports 1:12 no-advertise vendor-specific dot3 link-aggregation
```

**History**

This command was first available in ExtremeWare 7.4.

**Platform Availability**

This command is available on all Extreme switches.
configure lldp ports vendor-specific dot3 mac-phy

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot3 mac-phy

Description
Configures LLDP ports to advertise or not advertise MAC and physical layer capabilities to its neighbors. The capabilities include duplex and bit-rate. Since this is a vendor specific option, there may not be support for this from the neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

Default
The default is not to advertise.

Usage Guidelines
N/A.

Example
The following command configures all ports to advertise MAC/PHY capabilities to neighbors.

```
configure lldp ports all advertise vendor-specific dot3 mac-phy
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp ports vendor-specific dot3 max-framesize

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot3 max-framesize

**Description**
Configures LLDP ports to advertise or not advertise its maximum frame size to its neighbors. Since this is a vendor specific option, there may not be support for this from the neighbor.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*; i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

**Default**
The default is not to advertise.

**Usage Guidelines**
N/A.

**Example**
The following command configures ports 1:12 - 1:13 to advertise the maximum frame size to neighbors.

configure lldp ports 1:12 - 1:13 no-advertise vendor-specific dot3 max-framesize

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on all Extreme switches.
configure lldp ports vendor-specific dot3 power-via-mdi

configure lldp ports [all | <portlist>] [advertise | no-advertise] vendor-specific dot3 power-via-mdi

Description
Configures LLDP ports to advertise or not advertise MDI (Power Over Ethernet) capabilities to its neighbors. This is a vendor specific option; therefore, there may not be support for this capability from the neighbor.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>advertise</td>
<td>Specifies that information is to be sent to neighbors.</td>
</tr>
<tr>
<td>no-advertise</td>
<td>Specifies that information is not to be sent to neighbors.</td>
</tr>
</tbody>
</table>

Default
The default is not to advertise.

Usage Guidelines
N/A.

Example
The following command configures all ports to advertise MDI capabilities to neighbors.

configure lldp ports all advertise vendor-specific dot3 power-via-mdi

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp reinitialize-delay

    configure lldp reinitialize-delay <seconds>

Description
Configures the delay that applies to a re-initialization attempt after LLDP ports were disabled or the link went down.

Syntax Description

| seconds | Specifies the delay that applies to the re-initialization attempt. The range is 1 - 10 seconds. |

Default
The default is 2 seconds.

Usage Guidelines
N/A.

Example
The following command configures a re-initialization delay of 10 seconds after LLDP ports were disabled or the link is lost.

    configure lldp reinitialize-delay 10

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp snmp-notification-interval

    configure lldp snmp-notification-interval <seconds>

Description
Configures the allowed interval at which Simple Network Management Protocol (SNMP) notifications can be sent. If multiple neighbor information changes occur after the sent notification, no additional notifications are sent.

Syntax Description

| seconds | Specifies the interval at which lldp notifications are sent. The range is 5 - 3600 seconds. |

Default
The default is 5 seconds.

Usage Guidelines
N/A.

Example
The following command configures an interval of 60 seconds for SNMP notifications.

    configure lldp snmp-notification-interval 60

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp transmit-delay

configure lldp transmit-delay { auto | <seconds>}

Description
Configures the delay time between successive frame transmissions initiated by a value change or status change in any of the LLDP local systems Management Information Base (MIB). The auto option uses the formula, (0.25 * transmit-interval), to calculate the number of seconds.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>auto</td>
<td>Uses the formula, (0.25 * transmit-interval), to calculate the seconds. The range is 1 - 8192.</td>
</tr>
<tr>
<td>seconds</td>
<td>Specifies the interval at which lldp notifications are sent. The range is 5 - 3600.</td>
</tr>
</tbody>
</table>

Default
The default is 2 seconds.

Usage Guidelines
N/A.

Example
The following command configures the automatic delay between LLDP frame transmissions.

```
configure lldp transmit-delay auto
```

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp transmit-hold

    configure lldp transmit-hold <value>

Description
Calculates the actual time-to-live (TTL) value used in the LLDP PDU packets. The formula is
transmit-interval * transmit-hold; by default this value is 30*4=120 seconds.

Syntax Description

| value | Specifies the TTL value to transmit. The range is 2 to 10. |

Default
The default is 4.

Usage Guidelines
N/A.

Example
The following command configures a transmit-hold value of 5 for the LLDP PDU packets.

configure lldp transmit-hold 5

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
configure lldp transmit-interval

    configure lldp transmit-interval <seconds>

Description
Configures the periodic transmit interval for LLDP protocol data units (PDUs).

Syntax Description

| seconds | Specifies the time duration between LLDP transmissions. The range is 5 - 32768. |

Default
The default is 30 seconds.

Usage Guidelines
N/A.

Example
The following command configures a transmit interval of 20 seconds for LLDP PDUs.
configure lldp transmit-interval 20

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
disable lldp ports

disable lldp ports [all | <portlist>] {transmit-only | receive-only}

Description
Disables LLDP transmit mode, receive mode or transmit and receive mode on the specified port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>transmit only</td>
<td>Specifies that only the transmit mode is disabled.</td>
</tr>
<tr>
<td>receive only</td>
<td>Specifies that only the receive mode is disabled. If neither the transmit-only nor receive-only option is specified, then both transmit and receive are disabled.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
N/A.

Example
The following example disables receive mode on ports 1:2 - 1:6.

disable lldp ports 1:2-1:6 receive only

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
disable snmp traps lldp port

disable snmp traps lldp port  [all | <portlist>]

Description
Disables the sending of LLDP-specific SNMP traps on the specified port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>all</th>
<th>Applies to all ports on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
</tbody>
</table>

Default
By default, sending of SNMP traps is disabled.

Usage Guidelines
N/A.

Example
The following example disables sending of LLDP SNMP traps on all switch ports.
disable snmp traps lldp port all

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
enable lldp ports

   enable lldp ports [all | <portlist>] {transmit-only | receive-only}

**Description**

Enables LLDP transmit mode, receive mode or transmit and receive mode on the specified port or ports. If transmit or receive option is not specified, both transmit and receive are enabled.

**Syntax Description**

<table>
<thead>
<tr>
<th>all</th>
<th>Applies to all ports on the switch.</th>
</tr>
</thead>
<tbody>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>transmit only</td>
<td>Specifies that only the transmit mode is enabled.</td>
</tr>
<tr>
<td>receive only</td>
<td>Specifies that only the receive mode is enabled. If neither the transmit-only nor receive-only option is not specified, then both transmit and receive are enabled.</td>
</tr>
</tbody>
</table>

**Default**

By default, LLDP is disabled on all ports.

**Usage Guidelines**

N/A.

**Example**

The following example enables LLDP transmit and receive mode on port 1:4.

```
enable lldp ports 1:4 all
```

**History**

This command was first available in ExtremeWare 7.4.

**Platform Availability**

This command is available on all Extreme switches.
enable snmp traps lldp port

enable snmp traps lldp port  [all | <portlist>]

**Description**
Enables the transmission of LLDP SNMP trap notifications.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*; i:n, or i:n-i-m.</td>
</tr>
</tbody>
</table>

**Default**
By default notification sending is disabled.

**Usage Guidelines**
N/A.

**Example**
The following command enables LLDP SNMP traps for all ports.

```
enable snmp traps lldp port all
```

**History**
This command was first available in ExtremeWare 7.4.

**Platform Availability**
This command is available on all Extreme switches.
show lldp

    show lldp

Description
Displays LLDP configuration information for all ports.

Syntax Description
N/A.

Default
N/A.

Usage Guidelines
N/A.

Example
The following example displays LLDP configuration information for the switch.

    # show lldp

LLDP Configuration
Advertised Interval : 30 seconds
    Hold Value : 4
    Transmit Delay : 2 seconds
Notification Interval : 5 seconds
    Re-init Delay : 2 seconds

<table>
<thead>
<tr>
<th>Port</th>
<th>Tx State</th>
<th>Rx State</th>
<th>SNMP Notification</th>
<th>Optional enabled transmit TLVs</th>
<th>LLDP</th>
<th>802.1</th>
<th>802.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>5:18</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:19</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:20</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:21</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:22</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:23</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td>PNDCM</td>
<td>NPp-</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:24</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td>-NDM</td>
<td>NPp-</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:25</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:26</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:27</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:28</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:29</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:30</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:31</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>5:32</td>
<td>ENABLED</td>
<td>ENABLED</td>
<td>DISABLED</td>
<td></td>
<td>-----</td>
<td>-----</td>
<td>-----</td>
</tr>
</tbody>
</table>
show lldp

U->page up  D->page down ESC->exit

Flags:  (P) Port Description,  (N) System Name,  (D) System Description
        (C) System Capabilities,  (M) Mgmt Addr

802.1 Flags:  (P) Port VLAN ID,  (p) Port & Porocotol VLAN ID,  (N) VLAN Name
            (I) Protocol Identity

802.3 Flags:  (M) MAC/PHY Configuration/Status,  (P) Power via MDI
            (L) Link Aggregation,  (F) Frame Size

History

This command was first available in ExtremeWare 7.4.

Platform Availability

This command is available on all Extreme switches.
show lldp neighbor

show lldp neighbor

Description
Displays LLDP neighbor information for all ports.

Syntax Description
N/A.

Default
N/A.

Usage Guidelines
N/A.

Example
The following example shows neighbor information for port 5:24, which is the only port enabled for LLDP. Ports must be enabled for LLDP in order to show this information.

# show lldp neighbor

LLDP port 5:24 Total neighbors = 1
Neighbor:
Chassis ID (subtype 4): 00:04:96:1F:A4:06
Port ID (subtype 5): 23
TTL: 120 seconds
Port Description:
System Name: SummitX450-24t
System Description:
System Capabilities Supported:
  Router
  Bridge
System Capabilities Enabled:
  Bridge
Management Address: 10.210.51.3
  Interface subtype: ifIndex
  Interface Number: 1000006

Extended TLV Info 802.3 OUI (hex value) = 00-12-0f
-MAC PHY Configuration & Status
  -Auto-negotiation Support & Status: Supported, enabled
  -Advertised capability bits (hex value): 6c01
    10baseT
    10baseTFD
    100baseTX
show lldp neighbor

- 100baseTXFD
- 1000baseTFD
  - Operational MAU Type : 16
  - Power Via MDI
    - MDI : Not supported
  - Link Aggregation
    - Status : capable, not in aggregation
    - Port ID: 0
  - Maximum Frame Size
    - Frame Size: 1522

Extended TLV Info 802.1
- Port VLAN ID
  - ID: 1
- Port & Protocol VLAN ID
  - Capability & Status: capable, disabled
  - Reference number : 0
- VLAN Name
  - ID & Name: 1, Default

=====================================================================

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
show lldp port statistics

show lldp port [all | <portlist>] {detailed} statistics

Description

Displays statistical counters related to the specified port or ports. The following counters are presented with the standard command (taken from the 802.1ab MIB definition):

- Last table change time: Last time an entry in the LLDP database was added/changed or deleted.
- Number of table inserts: The number of times the complete set of information advertised by a particular neighbor has been inserted into tables.
- Number of table deletes: The number of times the complete set of information advertised by a particular neighbor has been deleted from tables.
- Number of table drops: The number of times the complete set of information advertised by a particular neighbor could not be stored in memory because of insufficient resources.
- Number of table age outs: The number of times the complete set of information advertised by a particular neighbor has been deleted from tables because the information timeliness interval has expired.
- Tx Total: The number of LLDP frames transmitted by this switch on the indicated port.
- Rx Total: The number of valid LLDP frames received by this switch on the indicated port, while this LLDP agent is enabled.
- Rx Discarded: The number of LLDP frames received by this switch on the indicated port, and then discarded for any reason.
- RX Errors: The number of invalid LLDP frames received by this switch on the indicated port, while this LLDP agent is enabled.
- TLVs Discarded: The number of LLDP TLVs discarded for any reason by this switch on the indicated port.
- TLVs Unrecognized: The number of LLDP TLVs received on the given port that are not recognized by the switch.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>detailed</td>
<td>Shows detailed information.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

N/A.
Example

The following example lists statistical counters for all ports on the switch.

```
# show lldp port all statistics

Last table change time   : Fri Dec 17 10:42:33 2004
Number of Table Inserts  : 3
Number of Table Deletes  : 0
Number of Table Drops    : 0
Number of Table Age Outs : 0

<table>
<thead>
<tr>
<th>Port</th>
<th>Tx Total</th>
<th>Rx Total</th>
<th>Rx Discarded</th>
<th>Rx Errors</th>
<th>TLVs Discarded</th>
<th>TLVs Unrecogn.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:1</td>
<td>189</td>
<td>5654</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>2:2</td>
<td>188</td>
<td>565</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
```

History

This command was first available in ExtremeWare 7.4.

Platform Availability

This command is available on all Extreme switches.
show lldp ports

show lldp ports [all | <portlist>] {detailed}

Description
Displays LLDP configuration information for the specified port or ports. The detailed keyword is used
to show the configured VLANs on the port and the enabled VLAN specific TLVs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
</tr>
<tr>
<td>portlist</td>
</tr>
<tr>
<td>detailed</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
N/A.

Example
The following example displays LLDP configuration information for port 5:23.

```
# show lldp ports 5:23
LLDP Configuration
Advertised Interval : 30 seconds
  Hold Value : 4
  Transmit Delay : 2 seconds
Notification Interval : 5 seconds
  Re-init Delay : 2 seconds
Port     Tx     Rx     SNMP     Optional enabled transmit TLVs
         State  State  Notification LLDP    802.1    802.3
======================================================================================
5:23     ENABLED ENABLED DISABLED  PNDCM    NPp-      ----
```

Flags: (P) Port Description, (N) System Name, (D) System Description
       (C) System Capabilities, (M) Mgmt Addr

802.1 Flags: (P) Port VLAN ID, (p) Port & Porocotol VLAN ID, (N) VLAN Name
802.3 Flags: (M) MAC/PHY Configuration/Status, (P) Power via MDI
(L) Link Aggregation, (F) Frame Size

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
show lldp ports neighbor

show lldp ports [all | <portlist>] neighbor {detailed}

Description
Displays the information related to the LLDP neighbors detected on the specified port or ports.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i*, i:n, or i:n-i-m.</td>
</tr>
<tr>
<td>detailed</td>
<td>Shows information on the configured VLANs on the port.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
N/A.

Example
The following example displays LLDP neighbor information for switch port 5:24, which has been enabled for LLDP.

# show lldp ports 5:24 neighbors

LLDP port 5:24 Total neighbors = 1
Neighbor:
Chassis ID (subtype 4): 00:04:96:1F:A4:06
Port ID (subtype 5): 23
TTL : 120 seconds
Port Description :
System Name : SummitX450-24t
System Description : ExtremeWare XOS version 11.2.0.9 v1120b9 by release-manager on Thu Feb 24 13:04:06 PST 2005
System Capabilities Supported:
    Router
    Bridge
System Capabilities Enabled:
    Bridge
Management Address : 10.210.51.3
    Interface subtype: ifIndex
    Interface Number : 1000006

Extended TLV Info 802.3 OUI (hex value) = 00-12-0f
-MAC PHY Configuration & Status
    -Auto-negotiation Support & Status : Supported, enabled
    -Advertised capability bits (hex value): 6c01
show lldp ports neighbor

10baseT
10baseTFD
100baseTX
100baseTXFD
1000baseTFD
-Operational MAU Type: 16
-Power Via MDI
-MDI: Not supported
-Link Aggregation
-Status: capable, not in aggregation
-Port ID: 0
-Maximum Frame Size
-Frame Size: 1522

Extended TLV Info 802.1
OUI (hex value) = 00-80-c2
-Port VLAN ID
-ID: 1
-Port & Protocol VLAN ID
-Capability & Status: capable, disabled
-Reference number: 0
-VLAN Name
-ID & Name: 1, Default
=====================================================================
unconfigure lldp

unconfigure lldp

Description
Restores all system-wide LLDP configuration values to factory defaults.

Syntax Description
N/A.

Default
N/A.

Usage Guidelines
N/A.

Example
The following command restores system-wide factory defaults.
unconfigure lldp

History
This command was first available in ExtremeWare 7.4.

Platform Availability
This command is available on all Extreme switches.
unconfigure lldp port

unconfigure lldp port [all | <portlist>]

**Description**

Restores all LLDP factory default values for the specified port or ports.

**Syntax Description**

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Applies to all ports on the switch.</td>
</tr>
<tr>
<td>portlist</td>
<td>Specifies a list of switch ports in the form i:*, i:n, or i:n-i-m.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

N/A.

**Example**

The following command restores LLDP factory default values for ports 1:4 - 1:8.

unconfigure lldp port 1:4 - 1:8

**History**

This command was first available in ExtremeWare 7.4.

**Platform Availability**

This command is available on all Extreme switches.
H-VPLS (Hierarchical Virtual Private LAN Services) defines an architectural bridging model for interconnecting multiple Ethernet LAN segments over a service provider MPLS network. Unlike VPLS, which requires a full mesh of Virtual Circuits (VCs), H-VPLS specifies a hierarchical architecture to extend spoke VCs to the service provider's network edge. The H-VPLS bridging model is based on standard 802.1D bridging concepts. By implementing standard bridging technology, a protocol agnostic L2 VPN architecture can be implemented independent of the underlying MPLS IP metro core.
clear mpls vpls counters

clear mpls vpls counters

Description
Resets all VPLS counters and statistics.

Syntax Description
N/A.

Default
N/A.

Usage Guidelines
This command resets all VPLS counters and statistics.

Example
N/A.

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls add vpls

configure mpls add vpls <vpls_name> vpn <vpnid> {from <local_endpoint_ipaddress> | <local_endpoint_vlan>}

Description
Configures a VPLS with the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>vpn</td>
<td>Specifies a vpn ID.</td>
</tr>
<tr>
<td>local_endpoint_ipaddress</td>
<td>Defines the local_endpoint_ipaddress from which VC-LSPs are established for the VPLS vpls_name.</td>
</tr>
<tr>
<td>local_endpoint_vlan</td>
<td>Specifies a vlan instead of the local_endpoint_ipaddress.</td>
</tr>
</tbody>
</table>

Default
edge-service-mode - vlan
local_endpoint_ipaddress - configured OSPF/ISIS Router ID.

Usage Guidelines

This command configures a VPLS with the specified vpls_name. Each VPLS represents a separate VSI. The vpls_name parameter is a character string that is to be used to identify the VPLS within the switch. The vpls_name string must begin with an alphabetic character, and may contain up to 31 additional alphanumeric characters. Each VPLS is a member of a single vpn and each vpn may have only one associated VPLS per switch. Externally to the switch, the vpn is identified by the vpnid. The vpnid is any non-zero 32-bit value and has network-wide significance.

The optional from keyword defines the local_endpoint_ipaddress from which VC-LSPs are established for the VPLS vpls_name. Since the local endpoint must first establish an LDP session to the targeted LDP peer (VPLS peer) prior to exchanging vpn parameters, the VPLS peer must be capable of accepting LDP Hello messages. By default, the local_endpoint_ipaddress is the configured OSPF/ISIS Router ID. The from keyword must be specified when VPLS peers are configured in conjunction with ESRP. The local_endpoint_ipaddress should be configured to match the local VPLS egress VLAN interface IP address (see Layer-2 Transport on page 3 for discussion on how to use ESRP to provide redundancy). This allows VC-LSPs to properly fail over to the slave switch when both the master and the slave switch are configured with the same local_endpoint_ipaddress. Optionally, the local_endpoint_vlan may be specified in place of the local_endpoint_ipaddress. There is no functional difference between these two configuration parameters. If the local_endpoint_vlan parameter is specified, the local endpoint IP address used for the VPLS is the IP interface address of the specified local_endpoint_vlan.

Example

None
History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls delete

configure mpls delete vpls [<vpls_name> | all]

Description
Deletes the VPLS with the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VPLS.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command deletes the VPLS with the specified vpls_name. All VC-LSPs established to VPLS peers are terminated. The all keyword may be used to indicate that all VPLS instances are to be deleted.

Example
config mpls delete vpls myvpls

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls edge-service-mode

  configure mpls slot <slot> edge-service-mode [vlan | port]

Description
Configures MPLS Layer 2 edge service mode for MPLS H-VPLS port mode.

Syntax Description

<table>
<thead>
<tr>
<th>slot</th>
<th>Specifies a switch slot.</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan</td>
<td>Specifies a vlan ID.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a switch port in the specified slot.</td>
</tr>
</tbody>
</table>

Default

edge-service-mode - vlan

Usage Guidelines

This command configures the MPLS Layer 2 edge service mode for all ports associated with the module in the specified slot. The keyword edge-service-mode is used to specify how customer interfaces are identified. The keyword vlan configures the module in the specified slot so that customer traffic is identified by the received packet's 802.1q tag. The keyword port configures the module in the specified slot so that customer traffic is identified based on the port that the packet was received. Port mode configured ports are implicitly defined as customer facing Layer 2 service ports. Thus, MPLS cannot be enabled on these ports. The default edge-service-mode is vlan.

Ports configured in different modes cannot send traffic between them without the use of the MPLS module. That is, traffic received on a port that is configured in vlan mode cannot switch traffic directly to a port on a module that is configured in port mode, and vice versa. Thus, ports configured in different modes cannot be members of the same VLAN or VPLS. VPLS ingress traffic can be received on a port that is in port mode and label switched out a port that is configured in vlan mode. Traffic received on ports in port mode is also switched directly to local egress ports that are members of the same VPLS. Configured VLANs for ports in vlan mode cannot conflict with core (or provider) network interior VLANs configured within the same switch.

Changing the edge-service-mode will disrupt traffic for all ports on the module in the specified slot.

Example

The following command configures the edge service mode for slot 1, vlan ID 10:

```
config mpls slot 1 edge-service-mode 10
```

History

This command was first available in an ExtremeWare 7.3.0.

Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls ldp acl

configure mpls ldp acl [enabled | disabled]

Description
Enables or disables an MPLS LDP Access Control List (ACL).

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Enables MPLS LDP ACL such that all required authentication procedures are</td>
</tr>
<tr>
<td></td>
<td>enforced.</td>
</tr>
<tr>
<td>disabled</td>
<td>Disables MPLS LDP ACL.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command enables or disables an MPLS LDP Access Control List (ACL). The enabled keyword specifies that the ACL be enabled. When enabled, all required authentication procedures are enforced. LDP ACLs cannot be enabled unless at least one LDP ACL peer has been configured. The disabled keyword specifies that the ACL be disabled. No authentication procedures are enforced. LDP ACLs must be disabled before all LDP ACL peers can be deleted. Changing the ACL enabled configuration may result in the termination of sessions or services with peers that cannot be validated. The LDP ACL status is displayed using the show mpls command.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls ldp acl add peer

configure mpls ldp acl add [peer <ipaddress> | <host_name>]

Description
Adds an LDP peer to the ACL.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Identifies the peer from which targeted and non-targeted LDP sessions are accepted.</td>
</tr>
<tr>
<td>host_name</td>
<td>Identifies the peer. Must be able to be resolved to an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command adds an LDP peer to the ACL. The acl keyword is used to configure an LDP peer that is allowed to establish LDP peer session with this LSR. Up to 256 peers may be configured. The ipaddress parameter identifies the peer from which targeted and non-targeted LDP sessions are accepted. If the peer is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address. LDP Hellos from IP addresses that are not included in the acl list are ignored.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls ldp acl delete peer

configure mpls ldp acl delete peer [<ipaddress> | <host_name> | all]

Description
Deletes a configured LDP peer from the ACL.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Identifies the peer for deletion.</td>
</tr>
<tr>
<td>host_name</td>
<td>Identifies the peer. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all LDP peers are deleted from the ACL.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command deletes a configured LDP peer from the ACL. The `ipaddress` and `host_name` parameter identify the peer to be deleted from the ACL. When the keyword all is specified, all configured LDP peers are removed.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls vpls add

    configure mpls vpls <vpls_name> add [vlan <vlan_name> | ports <port-list>]

Description
Configures service for VPLS.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS interface within the switch.</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Logically binds the VLAN to the specified vpl.</td>
</tr>
<tr>
<td>port-list</td>
<td>Specifies a list of ports.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command configures a local Ethernet VPLS interface for the specified vpls_name. The VPLS interface may be a VLAN or a physical port. Specifying the vlan_name logically binds the VLAN to the specified vpl. Only one VLAN may be configured per VPLS. Specifying a port-list logically binds one or more physical ports to the specified vpl. Only ports configured for edge-service-mode port can be directly added to a vpl (see Configure MPLS Edge Service Mode on page 3 for additional information). Edge-service-mode vlan ports must be added to a VLAN and the VLAN assigned to a vpl, since the VLAN ID (and not the port) is the service identifier. If multiple ports are added or there are multiple ports configured for vlan_name, VPLS traffic local to the switch is forwarded within the switch. Simultaneous support for both vlan and ports for a single vpl is not supported.

When a vlan interface has been configured for a VPLS, the VLAN is added to the VPLS as specified by the vpls_name. The VLAN ID is locally significant to each VPLS. Thus, each VLAN VPLS interface within the H-VPLS network, may have a different VLAN ID. This greatly simplifies VLAN ID coordination between metro network access points. Traffic may be switched locally between VLAN ports if more than one port is configured for the VLAN.

When a port interface has been configured for a VPLS, the port-list is automatically added to a unique VMAN ID. The VMAN ID assigned, is the highest unallocated VLAN ID. The VMAN allocated for the VLAN ID has the same name as the configured VPLS instance (i.e., vpls_name). Any additional local switch ports added to the VPLS are implicitly added to the VMAN. The VMAN ID uniquely maps to a vpls_name and thus identifies the ports that have been added to the Port VPLS interface. Because the VMAN ID must uniquely identify the port, the port cannot be added to any other local VLAN.

Example

    config mpls vpls myvpls add [vlan <vlan_name> | ports <port-list>]
    config mpls vpls myvpls add myvlan
    config mpls vpls myvpls add ports 1:5

History
This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls vpls add peer

configure mpls vpls <vpls_name> add peer [<ipaddress> | <host_name>]
    [core-to-core | spoke-to-core (primary | secondary) | core-to-spoke {vpls |
    tls {vcid <vcid>} | tps {vcid <vcid>}}] {lsp <lsp_name>}

Description

Configures a VPLS peer for the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>core-to-core</td>
<td>Specifies the VPLS peer relationship which represents a member of a fully meshed VPLS core peer group.</td>
</tr>
<tr>
<td>spoke-to-core</td>
<td>Specifies the spoke connectivity from a spoke node to a core node.</td>
</tr>
<tr>
<td>core-to-spoke</td>
<td>Specifies the spoke connectivity from the core node to the spoke node.</td>
</tr>
<tr>
<td>vcid</td>
<td>Specifies an option for VC-LSP between the core and spoke.</td>
</tr>
<tr>
<td>tps</td>
<td>Specifies an option for VC-LSP between the core and spoke.</td>
</tr>
<tr>
<td>ldp_name</td>
<td>Specifies an option for VC-LSP between the core and spoke.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

This command configures a VPLS peer for the specified vpls_name. Up to 32 peers may be configured for each VPLS. Peers may belong to multiple VPLS instances. The ipaddress parameter identifies the peer node that is the endpoint of the VC-LSP. The ipaddress should be configured with a 32-bit prefix on the peer node. When the peer node is also an Extreme switch, then either OSPF/ISIS must also be enabled on the VLAN that the ipaddress is assigned, or the peer switch must be configured to distribute direct routes into the OSPF/ISIS domain. Note that the export command should be used when the tunnel LSP needs to cross OSPF area boundaries or when ESRP is enabled on the VLAN that the ipaddress is assigned. If the VPLS peer is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address.

Per node, each peer relationship for each VPLS must be configured. The peer relationships are defined as either a core-to-core, core-to-spoke, or spoke-to-core. This relationship implicitly defines the packet flooding behavior for the VC-LSP set up to the configured peer.

A VPLS peer relationship defined as core-to-core indicates that the peer is a member of a fully meshed VPLS core peer group. Flood traffic received from a core node by the core node is forwarded to spoke nodes only.

A VPLS peer relationship defined as spoke-to-core specifies the spoke connectivity from a spoke node to a core node. Flood traffic received by a spoke node from a core node is forwarded to the local egress interface. The spoke-to-core keyword may optionally be qualified with the redundant configuration mode. The core node is either the primary or secondary VPLS peer. One primary core
node and up to two secondary core nodes may be added to \texttt{vpls}\_\texttt{name}. The configured core node defaults to primary when no primary core node has been configured and defaults to secondary if a primary core node has previously been configured for \texttt{vpls}\_\texttt{name}. Configuration of the primary core node is not required. All configured primary and secondary core nodes for the \texttt{vpls}\_\texttt{name} must be configured with a different endpoint IP address. Adding a secondary core node designates the node as a hot-standby redundant H-VPLS core node. A backup VC-LSP is established but is not used. Packets received on the backup VC-LSP are discarded. In the event that a VC-LSP cannot be established or the active VC-LSP fails, the VC-LSP to one of the secondary core nodes becomes the active VC-LSP. When a fail-over occurs, all secondary core nodes have equal preference; the first one available is chosen. If at any time the VC-LSP to the primary core node is re-established, the switch immediately terminates the VC-LSP to the secondary core node and begins using the VC-LSP to the primary core node. The VC-LSP to the secondary core node is re-established and returns to hot-standby state. Dropping the VC-LSP to the secondary core node forces the core node to flush its MAC FDB relative to the terminated VC-LSP and to propagate this information throughout the H-VPLS network. If the VC-LSP to the secondary core node fails while in-use, the VC-LSP to the remaining configured secondary core node becomes the active VC-LSP. The VC-LSP to the secondary core node remains the active VC-LSP unless the primary VC-LSP is re-established.

A VPLS peer relationship defined as \texttt{core-to-spoke} specifies the spoke connectivity from the core node to the spoke node. Flood traffic received from a spoke node by the core node is forwarded to all core-node and spoke-node peers. The \texttt{core-to-spoke} may be optionally qualified with the VC-LSP signaling mode. The VC-LSP between the core and spoke may be signaled as \texttt{vpls}, \texttt{tls}, or \texttt{tps}. VC-LSPs established to a tls configured spoke are signaled using the martini-draft VLAN FEC. Martini tls VC-LSPs carry traffic for a single VLAN. Thus, tls core-to-spoke VC-LSPs are incompatible with local egress VPLS port interfaces (i.e., tls VC-LSPs and local egress ports can not be configured for the same vpls). VC-LSPs established to an tps configured spoke are signaled using the martini-draft Ethernet FEC. Martini tps VC-LSPs carry traffic for a set of ports (i.e., port-list). Thus, tps core-to-spoke VC-LSPs are incompatible with local egress VPLS VLAN interfaces (i.e., tps VC-LSPs and a local egress VLAN can not be configured for the same vpls). The vcid of the martini VC-LSP can be optionally specified for either tls or tps. If the vcid is not specified, the configured VPLS VPN ID is used to signal the vcid. VC-LSPs established to a vpls configured spoke are signaled using the VPLS FEC. The spoke node must use the VC-LSP signaling method configured on the core node or the VC-LSP will not be established. If the VC-LSP signaling mode is not specified when the core-to-spoke keyword is specified, vpls signaling is selected by default. VPLS spoke nodes support additional features that are not defined in the martini-drafts. These features are automatically enabled when vpls is signaled and are disabled when tls or tps is signaled. These features include support for MAC Address Withdraw TLV, VPLS OAM packets, and purging looping packets based on the VC-FEC TTL.

Packets are never forwarded onto a VC-LSP from which the packet was received.

Optionally, the peer VC-LSP connection can be configured to use a specific RSVP-TE LSP. The lsp keyword specifies which LSP to use. The LSP must have previously been configured. If the lsp is configured and the LSP specified by \texttt{lsp}\_\texttt{name} terminates, VPN connectivity to the VPLS peer also terminates. (To protect the LSP, backup paths can be configured to provide alternate paths to the peer ipaddress. See Add a Path to a Traffic Engineered LSP on page 3.) If the lsp keyword is omitted, the VC-LSP will use the best-routed path LSP to the peer ipaddress. If the best-routed path LSP fails, the next best routed path LSP will be used. In this case, failing over to the next best-routed path LSP will most likely require a route topology convergence.

\textbf{Example}

\texttt{None}
History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls delete vpls

configure mpls delete vpls [<vpls_name> | all]

**Description**

Deletes the VPLS with the specified vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>vpls_name</th>
<th>Identifies the VPLS within the switch (character string)</th>
</tr>
</thead>
<tbody>
<tr>
<td>all</td>
<td>Marks all VPLS for deletion.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command deletes the VPLS with the specified vpls_name. All VC-LSPs established to VPLS peers are terminated. The all keyword may be used to indicate that all VPLS instances are to be deleted.

**Example**

config mpls delete vpls myvpls

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls health-check add mplsing

configure mpls health-check add mplsing [<ipaddress> | prefix <ipaddress/masklength> | <host_name> | lsp <lsp_name>](interval-time <seconds>) (trap-send-holdtime <seconds>)

Description

Configures an MPLS tunnel LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Option for specifying the forwarding equivalence class (FEC).</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Option for specifying the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Option for specifying the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Configures the tunnel LSP health-check</td>
</tr>
<tr>
<td>interval-time</td>
<td>Determines the rate at which ping packets are sent.</td>
</tr>
<tr>
<td>trap-send-holdtime</td>
<td>Specifies the interval after interval-time when service connectivity is</td>
</tr>
<tr>
<td></td>
<td>considered down if there is no echo response.</td>
</tr>
</tbody>
</table>

Default

interval-time range - 60 seconds

trap-send-holdtime range - 10 seconds

Usage Guidelines

This command configures a MPLS tunnel LSP service connectivity health-check. The health-check command can be used to configure recurring tunnel LSP connectivity checks. If the configured tunnel LSP connectivity is lost, a trap is sent to alert management stations of a possible service failure and an error message is logged. Connectivity is verified by sending an MPLS ping packet. Up to 256 mplsing health-checks can be configured.

Ping packets are sent at the rate specified by the interval-time. If an echo response is not received within trap-send-holdtime seconds after the interval-time ping was sent, service connectivity is considered down and an error message is logged and a trap message may be sent. The valid interval-time range is 10 to 600 seconds with a default value of 60 seconds. The valid trap-send-holdtime range is 3 to 30 seconds with a default value of 10 seconds and must be less than the interval-time. Ping packets may be dropped due to spurious network conditions. In order to minimize service disconnect “false alerts”, when an echo request has not been received within trap-send-holdtime/3 seconds, echo requests are sent in rapid succession at a rate of one per second. This operation continues until an echo response is received or the trap-send-holdtime expires. If an echo response is received before the trap-send-holdtime expires, the rapid sending of echo requests is immediately stopped and the service is deemed connected.

Specifying the LSP FEC configures the tunnel LSP health-check. The FEC can be specified using the ipaddress, ipaddress/masklength or host_name parameter. If the FEC is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address. The resolved host name IP address is assumed to be a /32 prefix. If there is more than one outgoing LSP that matches the FEC, only one is used. For RSVP-TE LSPs, the FEC is implied from the LSP configuration. Thus, the lsp keyword may be used to configure an tunnel LSP health-check for lsp_name.
Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls health-check delete mplsping

configure mpls health-check delete mplsping [<ipaddress> | prefix <ipaddress/masklength> | <host_name> | lsp <lsp_name> | all]

Description
Deletes an MPLS tunnel LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Option for specifying the forwarding equivalence class (FEC).</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Option for specifying the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Option for specifying the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Deletes the tunnel LSP health-check</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all mplsping health-checks.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The command deletes a MPLS tunnel LSP service connectivity health-check. Deleting a LSP health-check, as specified by the ipaddress or host_name parameter or the prefix or lsp keyword, terminates and deletes the configured mplsping. If the all keyword is specified, all mplsping health-checks are deleted.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls health-check add vplsping

    configure mpls health-check add vplsping <vpls_name> [peer <ipaddress> | mac-address <macaddress>] {interval-time <seconds>} {trap-send-holdtime <seconds>}

Description

Configures a VPLS VC-LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>vpls_name</th>
<th>Identifies the VPLS within the switch (character string)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>interval-time</td>
<td>Determines the rate at which ping packets are sent.</td>
</tr>
<tr>
<td>trap-send-holdtime</td>
<td>Specifies the interval after interval-time when service connectivity is considered down if there is no echo response.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

This command configures a VPLS VC-LSP service connectivity health-check. The healthcheck command can be used to configure recurring VC-LSP connectivity checks. If VC-LSP connectivity is lost, a trap is sent to alert management stations of a possible service failure and an error message is logged. Connectivity is verified by sending a VPLS ping packet. Up to 256 vplsping health-checks may be configured.

Ping packets are sent at the rate specified by the interval-time. If an echo response is not received within trap-send-holdtime seconds after the interval-time ping was sent, service connectivity is considered down and an error message is logged and a trap message may be sent. The valid interval-time range is 10 to 600 seconds with a default value of 60 seconds. The valid trap-send-holdtime range is 3 to 30 seconds with a default value of 10 seconds and must be less than the interval-time. Ping packets may be dropped due to spurious network conditions. In order to minimize service disconnect “false alerts”, when an echo request has not been received within trap-send-holdtime/3 seconds, echo requests are sent in rapid succession at a rate of one per second. This operation continues until an echo response is received or the trap-send-holdtime expires. If an echo response is received before the trap-send-holdtime expires, the rapid sending of echo requests is immediately stopped and the service is deemed connected.

Specifying the VPLS node address configures the VPLS health-check to a VPLS node. The VPLS node can be specified using the peer or mac-address keyword. When the peer’s ipaddress is specified, the IP address is used to look up the corresponding VPLS node’s MAC address. If the MAC address has not been learned, the health-check keyword will fail with a “No MAC address learned for IP address” error. The mac-address keyword specifies the target VPLS node or a customer MAC address. The macaddress parameter must be a unicast MAC address and is specified as a colon separated list of six bytes in hex format.
Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls health-check delete vplsping

configure mpls health-check delete vplsping <vpls_name> [peer <ipaddress> | mac-address <macaddress> | all]

**Description**
Deletes a VPLS VC-LSP service connectivity health-check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all vplsping health-checks for the specified vpls_name.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
The command deletes a VPLS VC-LSP service connectivity health-check. Deleting a VC-LSP health-check, as specified by the `peer` or `mac-address` keyword, terminates and deletes the configured vplsping. If the `all` keyword is specified, all vplsping health-checks for the specified `vpls_name` are deleted.

**Example**
None

**History**
This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure mpls health-check delete vplsping

configure mpls health-check delete vplsping <vpls_name> [peer <ipaddress> | mac-address <macaddress> | all]

Description
Deletes a VPLS VC-LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all vplsping health-checks for the specified vpls_name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The command deletes a VPLS VC-LSP service connectivity health-check. Deleting a VC-LSP health-check, as specified by the peer or mac-address keyword, terminates and deletes the configured vplsping. If the all keyword is specified, all vplsping health-checks for the specified vpls_name are deleted.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te add profile

configure mpls rsvp-te add profile <profile_name> {bandwidth <bps>} {setup-priority <priority>} {hold-priority <priority>} {retry-timeout <seconds>} {hop-count <number>} {ping-interval <seconds>} {metric [<metric] | igp-tracking} {record [enabled | disabled]} {mtu <number>}

Description
None

Syntax Description

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Identifies the profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>bps</td>
<td>bits per second</td>
</tr>
<tr>
<td>priority</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>number</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td></td>
</tr>
<tr>
<td>mtu</td>
<td>Specifies the MTU value transport payload packet (customer packet).</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The mtu keyword optionally specifies the MTU value transport payload packet (customer packet). The mtu value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same mtu value. If the mtu values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS mtu is set to 1500. The configurable mtu range is 1492 through 9216. Changing the mtu setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS MTU setting is greater than the MPLS MTU setting for the VC-LSP interface. The vplsping command may be used to verify end-to-end path connectivity for specific payload packet sizes.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te profile

configure mpls rsvp-te profile <profile_name> {bandwidth <bps>} {setup-priority <priority>} {hold-priority <priority>} {retry-timeout <seconds>} {hop-count <number>} {ping-interval <seconds>} {metric [<metric> | igp-tracking]} {record [enabled | disabled]} {mtu <number>}

Description
None

Syntax Description

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Identifies the profile</th>
</tr>
</thead>
<tbody>
<tr>
<td>bps</td>
<td>bits per second</td>
</tr>
<tr>
<td>priority</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>number</td>
<td></td>
</tr>
<tr>
<td>seconds</td>
<td></td>
</tr>
<tr>
<td>metric</td>
<td></td>
</tr>
<tr>
<td>mtu</td>
<td></td>
</tr>
</tbody>
</table>

Specifies the MTU value transport payload packet (customer packet).

Default
N/A.

Usage Guidelines
The mtu keyword optionally specifies the MTU value transport payload packet (customer packet). The mtu value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same mtu value. If the mtu values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS mtu is set to 1500. The configurable mtu range is 1492 through 9216. Changing the mtu setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS MTU setting is greater than the MPLS MTU setting for the VC-LSP interface. The vplsping command may be used to verify end-to-end path connectivity for specific payload packet sizes.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls tls-tunnel lsp

configure mpls tls-tunnel <tunnel_name> [add | delete] lsp <lsp_name>

Description
Deletes a VPLS VC-LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel_name</td>
<td>Refers to the TLS tunnel.</td>
</tr>
<tr>
<td>add</td>
<td>Allows addition of up to 4 RSVP-TE LSPs to the TLS tunnel.</td>
</tr>
<tr>
<td>delete</td>
<td>Removes the specified LSP.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the LSP.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command configures additional LSPs for a TLS tunnel. The add keyword may be used to add up to four RSVP-TE LSPs to the TLS tunnel specified by tunnel_name. TLS traffic across the TLS tunnel is aggregated across all configured LSPs. LSP traffic aggregation is described in Equal-cost Multipath LSP Support on page 3. The delete keyword will remove the LSP specified by the lsp_name parameter from the VC-LSP aggregation list. If all the LSPs are deleted, the VC-LSP will attempt to use the best-routed path LSP, if one exists. If no LSPs exist to the TLS tunnel endpoint, TLS tunnel connectivity to the endpoint IP address is lost.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
**configure mpls vpls**

```
configure mpls vpls <vpls_name> {vman-id <vman_id>} {mtu <number>}
```

**Description**

Configures transmit parameters for packets received on the local VPLS interface as specified by `vpls_name`.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>vpls_name</code></td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td><code>vman-id</code></td>
<td>Specifies the VLAN ID used internally in the switch to identify the vpls port list configured for <code>vpls_name</code>.</td>
</tr>
<tr>
<td><code>number</code></td>
<td>Specifies the MTU value of the VPLS transport payload packet.</td>
</tr>
</tbody>
</table>

**Default**

Priority - 0

ttl_value - 4

number (MTU) - 1500

**Usage Guidelines**

This command optionally configures transmit parameters for packets received on the local VPLS interface as specified by `vpls_name`.

By default, the `vman_id` is automatically chosen when the vpls is configured, but may be changed by specifying the `vman-id` keyword. The `vman-id` parameter specifies the VLAN ID used internally in the switch to identify the vpls port list configured for `vpls_name`. Valid values are 1 through 4096. The specified `vman-id` cannot conflict with any other configured VLAN ID.

The `mtu` keyword optionally specifies the MTU value of the VPLS transport payload packet (customer packet). The `mtu` value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same `mtu` value. If the `mtu` values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS `mtu` is set to 1500. The configurable `mtu` range is 1492 through 9216. Changing the `mtu` setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS MTU setting is greater than the MPLS MTU setting for the VC-LSP interface.

The `vplsping` command may be used to verify end-to-end path connectivity for specific payload packet sizes (see VPLS Ping Command on page 3).

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls vpls add

configure mpls vpls <vpls_name> add [vlan <vlan_name> | ports <port-list>]

Description
Configures transmit parameters for packets received on the local VPLS interface as specified by vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Specifies the name of the VLAN to which the command applies.</td>
</tr>
<tr>
<td>port-list</td>
<td>Specifies the ports to which the command applies.</td>
</tr>
</tbody>
</table>

Default
Priority - 0
ttl_value - 4
number (MTU) - 1500

Usage Guidelines
This command optionally configures transmit parameters for packets received on the local VPLS interface as specified by vpls_name.

By default, the vman_id is automatically chosen when the vpls is configured, but may be changed by specifying the vman-id keyword. The vman-id parameter specifies the VLAN ID used internally in the switch to identify the vpls port list configured for vpls_name. Valid values are 1 through 4096. The specified vman-id cannot conflict with any other configured VLAN ID.

The mtu keyword optionally specifies the MTU value of the VPLS transport payload packet (customer packet). The mtu value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same mtu value. If the mtu values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS mtu is set to 1500. The configurable mtu range is 1492 through 9216. Changing the mtu setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS MTU setting is greater than the MPLS MTU setting for the VC-LSP interface. The vplsping command may be used to verify end-to-end path connectivity for specific payload packet sizes (see VPLS Ping Command on page 3).

Example
None

History
This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch only.
**configure mpls vpls add peer**

```
configure mpls vpls <vpls_name> add peer [<ipaddress> | <host_name>] [core-to-core | spoke-to-core {primary | secondary} | core-to-spoke {vpls | tls {vcid <vcid>} {dot1q ethertype <hex_number>}}] {lsp <lsp_name>}
```

**Description**

Adds a VPLS peer with the specified vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string). Up to 32 peers can be configured for each VPLS.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Should be configured with a 32-bit prefix on the peer node.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>core-to-core</td>
<td>Indicates that the peer is a member of a fully meshed VPLS core peer group.</td>
</tr>
<tr>
<td>core-to-spoke</td>
<td>Specifies the spoke connectivity from the core node to the spoke node.</td>
</tr>
<tr>
<td>spoke-to-core</td>
<td>Specifies the spoke connectivity from a spoke node to a core node.</td>
</tr>
<tr>
<td>hex_number</td>
<td>Specifies the ethertype used on the customer traffic sent across the VC-LSP.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Configures the peer VC-LSP connection to use a specific RSVP-TE LSP.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command configures a VPLS peer for the specified vpls_name. Up to 32 peers may be configured for each VPLS. Peers may belong to multiple VPLS instances. The ipaddress parameter identifies the peer node that is the endpoint of the VC-LSP. The ipaddress should be configured with a 32-bit prefix on the peer node. When the peer node is also an Extreme switch, then either OSPF/ISIS must also be enabled on the VLAN that the ipaddress is assigned, or the peer switch must be configured to distribute direct routes into the OSPF/ISIS domain. Note that the export command should be used when the tunnel LSP needs to cross OSPF area boundaries or when ESRP is enabled on the VLAN that the ipaddress is assigned. If the VPLS peer is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address.

Per node, each peer relationship for each VPLS must be configured. The peer relationships are defined as either a core-to-core, core-to-spoke, or spoke-to-core. This relationship implicitly defines the packet flooding behavior for the VC-LSP set up to the configured peer.

A VPLS peer relationship defined as core-to-core indicates that the peer is a member of a fully meshed VPLS core peer group. Flood traffic received from a core node by the core node is forwarded to spoke nodes only.

A VPLS peer relationship defined as spoke-to-core specifies the spoke connectivity from a spoke node to a core node. Flood traffic received by a spoke node from a core node is forwarded to the local egress interface. The spoke-to-core keyword may optionally be qualified with the redundant configuration mode. The core node is either the primary or secondary VPLS peer. One primary core node and up to two secondary core nodes may be added to vpls_name. The configured core node defaults to primary when no primary core node has been configured and defaults to secondary if a primary core node has
configure mpls vpls add peer

previously been configured for vpls_name. Configuration of the primary core node is not required. All configured primary and secondary core nodes for the vpls_name must be configured with a different endpoint IP address. Adding a secondary core node designates the node as a hot-standby redundant H-VPLS core node. A backup VC-LSP is established but is not used. Packets received on the backup VC-LSP are discarded. In the event that a VC-LSP cannot be established or the active VC-LSP fails, the VC-LSP to one of the secondary core nodes becomes the active VC-LSP. When a fail-over occurs, all secondary core nodes have equal preference; the first one available is chosen. If at any time the VC-LSP to the primary core node is re-established, the switch immediately terminates the VC-LSP to the secondary core node and begins using the VC-LSP to the primary core node. The VC-LSP to the secondary core node is re-established and returns to hot-standby state. Dropping the VC-LSP to the secondary core node forces the core node to flush its MAC FDB relative to the terminated VC-LSP and to propagate this information throughout the H-VPLS network. If the VC-LSP to the secondary core node fails while in-use, the VC-LSP to the remaining configured secondary core node becomes the active VC-LSP. The VC-LSP to the secondary core node remains the active VC-LSP unless the primary VC-LSP is re-established.

A VPLS peer relationship defined as core-to-spoke specifies the spoke connectivity from the core node to the spoke node. Flood traffic received from a spoke node by the core node is forwarded to all core-node and spoke-node peers. The core-to-spoke may be optionally qualified with the VC-LSP signaling mode. The VC-LSP between the core and spoke may be signaled as vpls or tls. VC-LSPs established to a tls configured spoke are signaled using the martini-draft VLAN FEC. Martini tls VC-LSPs carry traffic for a single VLAN. Thus, tls core-to-spoke VC-LSPs are incompatible with local egress VPLS port interfaces (i.e., tls VC-LSPs and local egress ports can not be configured for the same vpls). The vcid of the martini VC-LSP can be optionally specified as tls. If the vcid is not specified, the configured VPLS VPN ID is used to signal the vcid. VC-LSPs established to a vpls configured spoke are signaled using the VPLS FEC. The spoke node must use the VC-LSP signaling method configured on the core node or the VC-LSP will not be established. If the VC-LSP signaling mode is not specified when the core-to-spoke keyword is specified, vpls signaling is selected by default. VPLS spoke nodes support additional features that are not defined in the martini-drafts. These features are automatically enabled when vpls is signaled and are disabled when tls is signaled. These features include support for MAC Address Withdraw TLV, VPLS OAM packets, and purging looping packets based on the VC-FEC TTL.

The optional dot1q keyword may be used to specify the ethertype used on the customer traffic sent across the VC-LSP. By default, the configured switch ethertype is used. If configured, the ethertype in the outer 802.1q field of the customer packet is overwritten using the configured per VC-LSP ethertype. The ethertype value is ignored on receipt.

Packets are never forwarded onto a VC-LSP from which the packet was received.

Optionally, the peer VC-LSP connection can be configured to use a specific RSVP-TE LSP. The lsp keyword specifies which LSP to use. The LSP must have previously been configured. If the lsp is configured and the LSP specified by lsp_name terminates, VPN connectivity to the VPLS peer also terminates. (To protect the LSP, backup paths can be configured to provide alternate paths to the peer ipaddress. See Add a Path to a Traffic Engineered LSP on page 92.) If the lsp keyword is omitted, the VC-LSP will use the best-routed path LSP to the peer ipaddress. If the best-routed path LSP fails, the next best routed path LSP will be used. In this case, failing over to the next best-routed path LSP will most likely require a route topology convergence.

Example

None

History

This command was first available in an ExtremeWare 7.3.0.
**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls vpls delete

configure mpls vpls <vpls_name> delete [vlan <vlan_name> | ports <port-list> | all]

**Description**

Deletes a VPLS peer from the specified vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>vcid</td>
<td>Qualifies a specific core-to-spoke Martini VC-LSP.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all VPLS peers.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command deletes a VPLS peer from the specified vpls_name. When the VPLS peer is deleted, VPN connectivity to the VPLS peer is terminated. The optional `vcid` keyword may be specified to fully qualify a specific core-to-spoke Martini VC-LSP. The all keyword may be used to indicate that all VPLS peers be deleted.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls vpls delete peer

    configure mpls vpls <vpls_name> delete peer [<ipaddress> (vcid <vcid>) | <host_name> (vcid <vcid>) | all]

**Description**

Deletes a VPLS peer from the specified vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>vcid</td>
<td>Qualifies a specific core-to-spoke Martini VC-LSP.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all VPLS peers.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command deletes a VPLS peer from the specified vpls_name. When the VPLS peer is deleted, VPN connectivity to the VPLS peer is terminated. The optional vcid keyword may be specified to fully qualify a specific core-to-spoke Martini VC-LSP. The all keyword may be used to indicate that all VPLS peers be deleted.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls vpls peer

configure mpls vpls <vpls_name> peer [<ipaddress> | <host_name>] [add | delete] [lsp <lsp_name>]

Description
Configures additional LSPs to a VPLS peer.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>add</td>
<td>Permits addition of up to four RSVP-TE LSPs to the VPLS peer.</td>
</tr>
<tr>
<td>delete</td>
<td>Removes the LSP specified by the lsp_name parameter from the VC-LSP aggregation list.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Removes the specified lsp.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command configures additional LSPs to a VPLS peer. The add keyword may be used to add up to four RSVP-TE LSPs to the VPLS peer. Traffic to the VPLS peer is aggregated across all configured LSPs. LSP traffic aggregation is described in Equal-cost Multipath LSP Support on page 3. The delete keyword will remove the LSP specified by the lsp_name parameter from the VC-LSP aggregation list. If all the LSPs are deleted, the VC-LSP will attempt to use the best-routed path LSP, if one exists. If no LSPs exist to the VPLS peer, VPN connectivity to the VPLS peer is lost.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
mplsping

mplsping {continuous} {{<ipaddress> | prefix <ipaddress/masklength> | <host_name>}} {next-hop {{<ipaddress> | <host_name>}}} | lsp <lsp_name> | {from <ipaddress>} {exp <exp_value>} {ping-address <ipaddress>} {start-size <size} {end-size <size}} {reply-mode [ip | mpls]}

Description
Sends an MPLS ping packet to a FEC over an LSP.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Determines the tunnel LSP on which the MPLS echo request.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the source IP address in the MPLS echo request.</td>
</tr>
<tr>
<td>exp_value</td>
<td>Specifies the experimental bits in the MPLS shim header of the MPLS echo request.</td>
</tr>
<tr>
<td>start_size</td>
<td>Specifies the number of bytes to include as payload data in the MPLS ping packet.</td>
</tr>
<tr>
<td>end_size</td>
<td>Determines whether size of the packet will increment by one byte for each new MPLS echo request sent.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the tunnel LSP on which to send the MPLS echo request.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the return path for the MPLS echo response. Routes back to the sender via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Specifies the return path for the MPLS echo response. Switches the echo reply back to the sender via an IPv4 packet over an LSP.</td>
</tr>
</tbody>
</table>

Default
exp_value - 0
dot1p_value - 0

Usage Guidelines
This command sends an MPLS ping packet to a FEC over an LSP. The mplsping command can be used to verify data plane connectivity across an LSP. This is useful, since not all failures can be detected using the MPLS control plane. The FEC can be specified using the ipaddress, ipaddress/masklength or host_name parameter. If the FEC is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address. The resolved host name IP address is assumed to be a /32 prefix. If there is more than one outgoing LSP that matches the FEC, the MPLS echo request will be sent on each LSP in round-robin fashion. For RSVP-TE LSPs, the FEC is implied from the LSP configuration. The lsp keyword may be used to specify the tunnel LSP on which to send the MPLS echo request. The tunnel LSP on which the MPLS echo request is sent is specified by the lsp_name parameter. The TTL value in the MPLS Echo Request is set to 255.
The `from` keyword is used to specify the source IP address used in the MPLS echo request. This is the IP address used by the target LSR will use to send the MPLS echo reply. If not specified, the OSPF/ISIS router ID is used.

The optional `exp` keyword is used to specify the Experimental bits in the MPLS shim header of the MPLS echo request. Valid `exp` parameter values are 0 through 7. The default value is 0.

The optional `dot1p` keyword is used to specify the 802.1p bits in the MPLS echo request. Valid `dot1p` parameter values are 0 through 7. The default value is 0.

The optional `continuous` keyword specifies that MPLS ping packets be sent continuously. Pressing any key can interrupt the operation.

The optional `size` keyword specifies the number of bytes to include as payload data in the MPLS ping packet. If no `size` parameter is specified, the size of the payload data is eight bytes. The minimum valid `size` value is one. The maximum `size` value is variable, depending on the type of MPLS ping packet sent, but the total size of the MPLS ping packet cannot exceed the configured jumbo packet size, if jumbo frames are enabled, or 1518 if jumbo frames are disabled. If the `size` parameter is specified, the size of the packet will increment by one byte for each new MPLS echo request sent. The next MPLS echo request is not sent until the MPLS echo response for the previous packet is received. This is useful for detecting interface MTU mismatch configurations between LSRs. The switch ceases sending MPLS echo requests when the specified `size` value is reached, the MPLS ping is user interrupted, or a MPLS echo response is not received after four successive retries.

The optional `reply-mode` keyword is used to specify the return path for the MPLS echo response. When the `ip` option is specified, the MPLS echo reply is routed back to the sender via an IPv4 packet with the IP Router Alert option. When the `mpls` option is specified, the MPLS echo reply is switched back to the sender via an IPv4 packet over an LSP. If there is no return LSP available, the MPLS echo reply is not sent. This option is useful for determining if there is a failure along the return LSP. If the `reply-mode` is not specified, the `mpls` reply mode is used.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
mplstrace

mplstrace [[<ipaddress> | prefix <ipaddress/masklength> | <hostname>] (next-hop [<ipaddress> | <host_name>]})] | lsp <lsp_name>] {from <ipaddress>} {reply-mode [ip | mpls]} {ttl <max_ttl_value>} {ping-address <ipaddress>} {detail}

Description
Traces the path an LSP takes for the specified FEC.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the source IP address in the MPLS echo request.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the tunnel LSP on which to send the MPLS echo request.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the return path for the MPLS echo response. Routes back to the</td>
</tr>
<tr>
<td></td>
<td>sender via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Specifies the return path for the MPLS echo response. Switches the echo</td>
</tr>
<tr>
<td></td>
<td>reply back to the sender via an IPv4 packet over an LSP.</td>
</tr>
<tr>
<td>max_ttl_value</td>
<td>Specifies the maximum TTL value in the MPLS echo request packet.</td>
</tr>
</tbody>
</table>

Default

max_ttl_value - 30.

Usage Guidelines
This command traces the path an LSP takes for the specified FEC. The mplstrace command works by repeatedly sending a MPLS echo request. The TTL value is incremented for each successive MPLS echo request sent. The sending LSR waits 5 seconds before sending the next MPLS echo request. This operation continues until either the egress LSR for the FEC is reached, the maximum TTL value is reached, or the operation is interrupted. For each response received, the following information is displayed on the console: IP address of the replying LSR, return code, and an indication of a MPLS echo reply timeout if no response was received.

The FEC can be specified using the ipaddress, ipaddress/masklength or hostname parameter. If the FEC is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address. The resolved host name IP address is assumed to be a /32 prefix. The lsp keyword may be used to specify the LSP to trace. The selected LSP is specified by the lsp_name parameter.

The from keyword is used to specify the source IP address used in the MPLS echo request. This is the IP address used by the target LSR will use to send the MPLS echo reply. If not specified, the OSPF/ISIS router ID is used.

The optional reply-mode keyword is used to specify the return path for the MPLS echo response. When the ip option is specified, the MPLS echo reply is routed back to the sender via an IPv4 packet with the IP Router Alert option. When the mpls option is specified, the MPLS echo reply is switched back to the sender via an IPv4 packet over an LSP. If the reply-mode is not specified, the mpls reply mode is used.
The **ttl** keyword optionally specifies the maximum TTL value in the MPLS echo request packet. The TTL value is decremented along the path at each LSR. When the TTL value reaches zero, the packet is not forwarded but is redirected to the control plane for additional processing. When the TTL value specified by the `max_ttl_value` parameter is exceeded, the `mplstrace` command ends. The valid `max_ttl_value` range is one to 30 with a default value of 30.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
show fdb vpls

    show fdb vpls {<vpls_name>} {peer [<ipaddress> | <host_name>]}"

Description
Displays FDB information learned for VPLS.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Displays FDB information only for the specified vpls.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the peer.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer. Must be able to be resolved to an IP address.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays FDB information learned for VPLS. MAC addresses learned on both the egress VLAN (if applicable) and VC-LSPs are displayed. Information displayed includes the MAC address, VPLS name, egress VLAN (if applicable), VC-LSP peer, Age, and Port List. Optionally specifying the vpls_name displays FDB information for the specified vpls only. If a VPLS peer qualifies the command, only FDB information learned from the specified peer is displayed. The peer is specified using the ipaddress or host_name parameter.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls health-check mpls{ing}

show mpls health-check mpls{ing} {detail | <ipaddress> | prefix <ipaddress/masklength> | <host_name> | lsp <lsp_name>}

**Description**
Displays the configuration and status for MPLS tunnel LSP health-checks.

**Syntax Description**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays the health-check information in comprehensive detail format.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Display specific mpls{ing} information for the specified address.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Display specific mpls{ing} information for the specified address.</td>
</tr>
<tr>
<td>host_name</td>
<td>Display specific mpls{ing} information for the specified host. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the LSP to trace.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
This command displays the configuration and status for MPLS tunnel LSP health-checks. If no optional keywords are specified, information is displayed in tabular format for all configured MPLS tunnel LSP health-checks. Health-check information displayed includes the type of health-check, current status, and relevant configuration parameters. If the optional detail keyword is specified, the health-check information is displayed in a comprehensive detail format. The detail format includes total state transition count from up to down and down to up, time of last failure, total up time, and total down time, and error code (if applicable). Optionally, an ipaddress, ipaddress/masklength, host_name, or lsp_name parameter can be specified to display specific mpls{ing} information. This information is always displayed in the detailed format.

**Example**
None

**History**
This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
show mpls health-check vplsping

    show mpls health-check vplsping {detail | <vpls_name> {peer <ipaddress> | mac-address <macaddress>}} {detail}

Description
Displays the configuration and status for VPLS health-checks.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Displays only health-checks associated with the specified vpl.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays the health-check information in comprehensive detail format.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Restricts the vplsping information as specified.</td>
</tr>
<tr>
<td>macaddress</td>
<td>Restricts the vplsping information as specified.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays the configuration and status for VPLS health-checks. If no optional keywords are specified, information is displayed in tabular format for all configured VPLS health-checks. Optionally, if the vpls_name parameter is specified, only the health-checks associated with the specified vpl are displayed. Health-check information displayed includes the type of health-check, current status, and relevant configuration parameters. If the optional detail keyword is specified, the health-check information is displayed in a comprehensive detail format. The detail format includes total state transition count from up to down and down to up, time of last failure, total up time, and total down time, and error code (if applicable). The optional peer and mac-address keywords may be specified to further restrict the vplsping information displayed for the vpls_name. Information displayed for a specific ipaddress or macaddress is always displayed in the detailed format.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls ldp acl

    show mpls ldp acl {<ipaddress> | <host_name>}

Description
Displays the list of configured LDP ACL entries.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for a specific LDP ACL.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the host name for a specific LDP ACL.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays the list of configured LDP ACL entries. Optionally, a specific LDP ACL can be displayed by specifying the ipaddress or host_name for the configured ACL.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls vpls

    show mpls vpls {summary | detail | <vpls_name> {detail | | peer
    [<ipaddress> | <host_name>] | peer [<ipaddress> | <host_name>] {detail}}

Description
Displays VPLS configuration and status information.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays summary counts.</td>
</tr>
<tr>
<td>vpls_name</td>
<td>Displays information for the specified vpls.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays additional information in comprehensive detail format.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
<tr>
<td>host_name</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
<tr>
<td>detail (peer)</td>
<td>Specifies all VPLS.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays VPLS configuration and status information. The show mpls vpls command (without specifying any optional parameters) displays all currently configured VPLS instances for the switch. Information displayed includes the VPLS name, IP addresses of peers, peer mode, VC-LSP state, and local egress VLAN or ports. If the vpls_name is specified, information is displayed for the specified vpls. If the optional detail keyword is specified, additional information is displayed in comprehensive detail format. The detail format additionally displays transmit and receive packet and byte counts. Optionally, specifying the peer keyword qualified by the ipaddress or host_name, displays VPLS information for the specified peer in detailed format. If the peer keyword is specified and is unqualified by a vpls_name, all VPLS instances that the peer is a member of are displayed. The summary keyword displays a set of summary counts. The counts include the number of VPLS instances, configured VPLS peers, active VPLS peers, targeted LDP sessions, VC-LSPs, and errors.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls vpls nodes

    show mpls vpls {summary | detail | <vpls_name> {detail | | peer
    [<ipaddress> | <host_name>]} | peer [<ipaddress> | <host_name>] {detail}}

Description
Displays information about all the nodes in the H-VPLS network.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Specifies the VPLS nodes that are members of the VPN.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
<tr>
<td>host_name</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

This command displays information about all the nodes in the H-VPLS network. When the optional vpls_name is specified, only VPLS nodes that are members of the VPN as specified by vpls_name are displayed. If vpls_name is omitted, information pertaining to all VPLS nodes is displayed. Information displayed includes IP address of each node, MAC address of each node, VPN ID, and immediate or remote node indication.

Example

None

History

This command was first available in an ExtremeWare 7.3.0.

Platform Availability

This command is available on the BlackDiamond switch only.
vplsping

vplsping {continuous} <vpls_name> [{<ipaddress> | mac-address <macaddress>}] {next-hop [{<ipaddress> | <host_name>}] {from <source_macaddress>}} {ping-address <ipaddress>} {start-size <size} {end-size <size}} {reply-mode [ip | mpls | vpls]}

Description

Sends VPLS ping packets to another VPLS node or to a specific destination MAC address.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the address to look up the corresponding VPLS node's MAC address.</td>
</tr>
<tr>
<td>macaddress</td>
<td>Specifies the MAC address that is being pinged.</td>
</tr>
<tr>
<td>source-macaddress</td>
<td>Specifies the source MAC address used for the VPLS echo request.</td>
</tr>
<tr>
<td>start_size</td>
<td>Specifies the number of bytes to include as payload data in the VPLS ping packet.</td>
</tr>
<tr>
<td>end_size</td>
<td>Determines if the size of the packet will increment by one byte for each new VPLS echo request sent.</td>
</tr>
<tr>
<td>ip</td>
<td>Determines whether the VPLS echo reply is routed back to the sender, specified in the L2 VPN Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Determines if the VPLS echo reply is routed back to the sender over an MPLS LSP.</td>
</tr>
<tr>
<td>vpls</td>
<td>Determines if the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

This command sends a VPLS ping packet to another VPLS node. The vplsping command can be used to verify data plane connectivity between any two VPLS nodes. This is useful, since not all failures can be detected using the MPLS or VPLS control plane. The VPLS ping is a modified MPLS ping sent in-band over a VC-LSP for a specific MAC address. The target MAC address of the VPLS echo request may represent a VPLS node's MAC address or a customer MAC address. VPLS nodes forward the VPLS echo request using their local MAC FDB. If the VPLS ping reaches a VPLS egress node, a VPLS echo reply is sent based on a local FDB lookup. VPLS ping packets are never forwarded out local VPLS egress interfaces. The TTL value in the VPLS echo request is set to 255.

The VPLS node can be specified using the ipaddress parameter. When the ipaddress parameter is specified, the IP address is used to look up the corresponding VPLS node's MAC address. If the MAC address has not been learned, the vplsping command will fail with a “No MAC address learned for IP address” error. The mac-address keyword specifies the MAC address that is being pinged. The mac-address may represent the MAC address of a VPLS node or a customer MAC address. The macaddress parameter must be a unicast MAC address and is specified as a colon separated list of six
bytes in hex format. The specified or learned MAC address is copied into the destination MAC address field of the VPLS echo request and is included in the L2-VPN Prefix Target FEC TLV. By default, the switch's MAC address is used for the source MAC address of the VPLS echo request. The from keyword optionally specifies the source MAC address used for the VPLS echo request. This option allows the VPLS echo request to be sent as if it originated from a customer's source MAC address. If link aggregation is supported along the path to the destination MAC address, this insures that the VPLS ping verifies connectivity through the VPLS network for the exact same path that the customer's traffic would travel.

The optional continuous keyword specifies that VPLS ping packets be sent continuously. The operation can be interrupted by pressing any key.

The optional size keyword specifies the number of bytes to include as payload data in the VPLS ping packet. If no start_size parameter is specified, the size of the payload data is eight bytes. The minimum valid start_size value is one. The maximum start_size value is variable, depending on the type of VPLS ping packet sent, but the total size of the VPLS ping packet cannot exceed the configured jumbo packet size, if jumbo frames are enabled, or 1518 if jumbo frames are disabled. If the end_size parameter is specified, the size of the packet will increment by one byte for each new VPLS echo request sent. The next VPLS echo request is not sent until the VPLS echo response for the previous packet is received. This is useful for detecting interface MTU mismatch configurations between VPLS nodes. The node ceases sending VPLS echo requests when the specified end_size value is reached, the VPLS ping is interrupted, or a VPLS echo response is not received after four successive retries.

The optional reply-mode keyword is used to specify the return path for the VPLS echo response. When the ip option is specified, the VPLS echo reply is routed back to the sender, specified in the L2 VPN Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option. If the mpls option is specified, the VPLS echo reply is routed back to the sender over an MPLS LSP. If no LSP is available, the VPLS echo reply is not sent. When the vpls option is specified, the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet. This option is useful for determining if there is a failure along the return VPLS VC-LSP path. If the reply-mode is not specified, the vpls reply mode is used.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
vplstrace

vplstrace <vpls_name> {<ipaddress> | mac-address <macaddress>}{next-hop [<ipaddress> | <host_name>] {ping-address <ipaddress>}} {reply-mode {ip | mpls | vpls}} {ttl <max_ttl_value>} {detail}

Description
Traces the path a packet takes to another VPLS node, or to a specific destination MAC address.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Determines whether the IP address is used to look up the corresponding VPLS node's MAC address.</td>
</tr>
<tr>
<td>macaddress</td>
<td>Specifies the MAC address being pinged.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the source IP address in the MPLS echo request.</td>
</tr>
<tr>
<td>ip</td>
<td>Routes back to the sender as specified in the L2 VPN Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Routes back to the sender over an MPLS LSP.</td>
</tr>
<tr>
<td>vpls</td>
<td>Determines if the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet.</td>
</tr>
<tr>
<td>max_ttl_value</td>
<td>Specifies the maximum TTL value in the VPLS echo request packet.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command traces the path a packet with a specific destination MAC address takes through the H-VPLS network for vpls_name. The vplstrace command works by sending a VPLS Ping or VPLS echo request (i.e., MPLS echo request for a VC-FEC in-band over the H-VPLS network). The TTL value in the VC-FEC label is initially set to 1. The TTL value is incremented for each successive VPLS echo request sent. The sending node waits 5 seconds before sending the next VPLS echo request. This operation continues until the egress VPLS node for the L2 VPN Prefix VC-FEC is reached, the maximum TTL value is reached, or the operation is interrupted. For each response received, the following information is displayed on the console: MAC address of the replying H-VPLS node, IP address of node (if known), return code, and an indication of a VPLS echo reply timeout if no response was received.

The VPLS node can be specified using the ipaddress parameter. When the ipaddress parameter is specified, the IP address is used to look up the corresponding VPLS node's MAC address. If the MAC address has not been learned, the vplstrace command will fail with a “No MAC address learned for IP address” error. The mac-address keyword specifies the MAC address that is being pinged. The mac-address may represent the MAC address of a VPLS node or a customer MAC address. The mac-address parameter must be a unicast MAC address and is specified as a colon separated list of six bytes in hex format. The specified or learned MAC address is copied into the destination MAC address field of the VPLS echo request and is included in the L2-VPN Prefix Target FEC TLV.

The optional reply-mode keyword is used to specify the return path for the VPLS echo response. When the ip option is specified, the VPLS echo reply is routed back to the sender, specified in the L2 VPN.
Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option. If the mpls option is specified, the VPLS echo reply is routed back to the sender over an MPLS LSP. If no LSP is available, the VPLS echo reply is not sent. When the vpls option is specified, the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet. This option is useful for determining if there is a failure along the return VPLS VC-LSP path. If the reply-mode is not specified, the vpls reply mode is used.

The ttl keyword optionally specifies the maximum TTL value in the VPLS echo request packet. The TTL value in the VC-FEC label is decremented along the path at each VPLS node. When the TTL value in the VC-FEC label reaches zero, the packet not forwarded but is redirected to the control plane for additional processing. When the TTL value specified by the max_ttl_value parameter is exceeded, the vplstrace command ends. The valid max_ttl_value range is one to 30 with a default value of 4.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
The MultiProtocol Label Switching (MPLS) module is a self-contained module for the BlackDiamond switch. Unlike other BlackDiamond modules, there are no external network interfaces on the MPLS module. Instead, the MPLS module provides advanced IP services for the other input/output (I/O) modules installed in the chassis. The MPLS module contains a powerful set of packet processing resources that operate in a one-armed fashion: receiving frames from the switch fabric, processing the frames, and transmitting the frames back into the switch fabric.

MPLS encompasses a growing set of protocols defined by the IETF. True to its name, MPLS is based on a label-switching forwarding algorithm. ATM and Frame Relay are examples of other protocols that use label-switching forwarding algorithms.

Conceptually, label switching is straightforward. A label is a relatively short, fixed-length identifier that is used to forward packets received from a given link. The label value is locally significant to a particular link and is assigned by the receiving entity.

Because labels are relatively short (for example, 20 bits in a MPLS shim header), the label of a received packet can be used as an index into a linear array containing the forwarding database. Forwarding database entries indicate the outgoing port and any label(s) to be applied to forwarded frames. Thus, forwarding may consist of a simple lookup and replacement of the incoming label with the appropriate outgoing label (otherwise known as label swapping).

The MPLS module includes the following features:

- **MultiProtocol label switching (MPLS)**—MultiProtocol Label Switching (MPLS) is a forwarding algorithm that uses short, fixed-length labels to make next-hop forwarding decisions for each packet in a stream.

- **IP unicast forwarding (longest prefix match)**—IP unicast packets are forwarded in the hardware using the longest prefix match algorithm. IP unicast forwarding is required to switch packets at ingress or upon egressing an MPLS network domain.

- **Destination-sensitive accounting**—Counts of IP packets and bytes are maintained based on the IP routes used to forward packets. Destination-sensitive accounting gives you the flexibility to bill your customers at predetermined and different rates. The rates are based on the customers’ IP unicast packet destinations.

  The accounting feature categorizes IP unicast packets using two parameters, input VLAN ID and accounting bin number. The VLAN ID is used to identify from which customer the packet is received. The accounting bin number is associated with the route used to forward the packet. External billing application servers can correlate the accounting bin number to a specific billing rate.
This chapter documents the MPLS command set. Some commands are new for the MPLS module; other commands have been enhanced to support the MPLS module.
clear mpls vpls counters

clear mpls vpls counters

Description
Resets all VPLS counters and statistics.

Syntax Description
N/A.

Default
N/A.

Usage Guidelines
This command resets all VPLS counters and statistics.

Example
This example resets all VPLS counters and statistics:
clear mpls vpls counters

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls

configure mpls [ldp | targeted-ldp] [hello | keep-alive] <hold_time> <interval_time>

Description
Configures LDP session timers.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldp</td>
<td>Specifies an LDP session.</td>
</tr>
<tr>
<td>targeted-ldp</td>
<td>Specifies a targeted LDP session.</td>
</tr>
<tr>
<td>hello &lt;hold_time&gt; &lt;interval_time&gt;</td>
<td>The amount of time (in seconds) that a hello message received from a neighboring LSR remains valid. If a hello message is not received from a particular neighboring LSR within the specified hello &lt;hold_time&gt;, the hello-adjacency is not maintained with that neighboring LSR. The range is 6 to 65,534.</td>
</tr>
<tr>
<td>keep-alive &lt;hold_time&gt; &lt;interval_time&gt;</td>
<td>The time (in seconds) during which an LDP message must be received for the LDP session with a particular peer LSR to be maintained. If an LDP PDU is not received within the specified session keep-alive &lt;hold_time&gt; &lt;interval_time&gt;, the corresponding LDP session is torn down. The &lt;hold_time&gt; range is 6 to 65,534. The &lt;interval_time&gt; range is 1 to 21844.</td>
</tr>
</tbody>
</table>

Default

ldp hello <hold_time> – 15 seconds

targeted-ldp hello <hold_time> – 45 seconds

ldp hello <interval_time> – 5 seconds

targeted-ldp hello <interval_time> – 15 seconds

ldp keep-alive <hold_time> – 40 seconds

targeted-ldp keep-alive <hold_time> – 60 seconds

ldp keep-alive <interval_time> – 13 seconds

targeted-ldp keep-alive <interval_time> – 20 seconds

Usage Guidelines

LDP session timers are separately configurable for LDP and targeted LDP sessions. The hello <hold_time> <interval_time> parameter specifies the amount of time (in seconds) that a hello message received from a neighboring LSR remains valid. If a hello message is not received from a particular neighboring LSR within the specified hello <hold_time>, the hello-adjacency is not maintained with that neighboring LSR.

The session keep-alive <hold_time> <interval_time> parameter specifies the time (in seconds) during which an LDP message must be received for the LDP session with a particular peer LSR to be
maintained. If an LDP PDU is not received within the specified session keep-alive <interval_time>,
the corresponding LDP session is torn down.

The minimum and maximum values for both the hello <hold_time> <interval_time> and
keep-alive <hold_time> <interval_time> are 6 and 65,534, respectively.

This command can only be executed when MPLS is disabled.

Example
The following command configures LDP session hello hold time to 30 seconds and the interval time to 5
seconds:
```
configure mpls ldp hello 30 5
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on
v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls add vpls

    config mpls add vpls <vpls_name> vpn <vpnid> {from
    <local_endpoint_ipaddress> | <local_endpoint_vlan>}

Description
Configures a VPLS with the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>vpnid</td>
<td>Specifies a vpn ID.</td>
</tr>
<tr>
<td>local_endpoint_ipaddress</td>
<td>Defines the local_endpoint_ipaddress from which VC-LSPs are established for</td>
</tr>
<tr>
<td></td>
<td>the VPLS vpls_name.</td>
</tr>
<tr>
<td>local_endpoint_vlan</td>
<td>Specifies a vlan instead of the local_endpoint_ipaddress.</td>
</tr>
</tbody>
</table>

Default
edge-service-mode - vlan
local_endpoint_ipaddress - configured OSPF/ISIS Router ID.

Usage Guidelines
This command configures a VPLS with the specified vpls_name. Each VPLS represents a separate VSI. The vpls_name parameter is a character string that is to be used to identify the VPLS within the switch. The vpls_name string must begin with an alphabetic character, and may contain up to 31 additional alphanumeric characters. Each VPLS is a member of a single vpn and each vpn may have only one associated VPLS per switch. Externally to the switch, the vpn is identified by the vpnid. The vpnid is any non-zero 32-bit value and has network-wide significance.

The optional from keyword defines the local_endpoint_ipaddress from which VC-LSPs are established for the VPLS vpls_name. Since the local endpoint must first establish an LDP session to the targeted LDP peer (VPLS peer) prior to exchanging vpn parameters, the VPLS peer must be capable of accepting LDP Hello messages. By default, the local_endpoint_ipaddress is the configured OSPF/ISIS Router ID. The from keyword must be specified when VPLS peers are configured in conjunction with ESRP. The local_endpoint_ipaddress should be configured to match the local VPLS egress VLAN interface IP address (see Layer-2 Transport on page 3 for discussion on how to use ESRP to provide redundancy). This allows VC-LSPs to properly fail over to the slave switch when both the master and the slave switch are configured with the same local_endpoint_ipaddress. Optionally, the local_endpoint_vlan may be specified in place of the local_endpoint_ipaddress. There is no functional difference between these two configuration parameters. If the local_endpoint_vlan parameter is specified, the local endpoint IP address used for the VPLS is the IP interface address of the specified local_endpoint_vlan.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch.
configure mpls add tls-tunnel

```
config mpls add tls-tunnel <tunnel_name> <ipaddress> <local_vlan_name>
[tls-labels <ingress_label> <egress_label> |
vcid <vcid> [{<groupid>}] {from <local_endpoint_ipaddress>})
```

**Description**

Adds a TLS tunnel.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel_name</td>
<td>Specifies a name used to identify the TLS tunnel within the switch.</td>
</tr>
<tr>
<td>lsp &lt;lsp_name&gt;</td>
<td>Identifies the peer LSR that is the tunnel endpoint. The DNS client must be</td>
</tr>
<tr>
<td>&lt;ipaddress&gt;</td>
<td>configured to use the &lt;lsp_name&gt;.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies a VLAN name that identifies the layer 2 traffic that is to be</td>
</tr>
<tr>
<td>local_vlan_name</td>
<td>transported.</td>
</tr>
<tr>
<td>tls-labels &lt;ingress_label&gt;</td>
<td>Identifies the innermost labels of the tunnel stack.</td>
</tr>
<tr>
<td>&lt;egress_label&gt;</td>
<td>vcid</td>
</tr>
<tr>
<td></td>
<td>Identifies the virtual circuit identifier. The vcid value is a non-zero, 32-bit number.</td>
</tr>
<tr>
<td>groupid</td>
<td>Identifies the logical VCID group number. The groupid is a 32-bit number. All TLS tunnels that are members of the same TLS group ID can be withdrawn simultaneously by specifying the groupid.</td>
</tr>
<tr>
<td>from &lt;local_endpoint_ipaddress&gt;</td>
<td>Identifies the local endpoint of the TLS tunnel.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command adds a Transparent LAN Services (TLS) tunnel. There are two types of TLS tunnels that can be configured: dynamic TLS tunnels, as defined by the martini-draft, and static TLS tunnels. A dynamic TLS tunnel is configured by specifying a vcid and optionally the groupid that uniquely define the tunnel at both tunnel endpoints. A static TLS tunnel is configured by statically defining the ingress/egress tls-labels at each tunnel peer. Both TLS tunnel types may be configured on a switch simultaneously.

The tunnel_name, ipaddress, and local_vlan_name parameters must be specified for either type of TLS tunnel. The tunnel_name parameter is a character string that is to be used to identify the TLS tunnel within the switch. The tunnel_name string must begin with an alphabetic character, and may contain up to 31 additional alphanumeric characters. The TLS tunnel is used to transport layer-2 traffic across a MPLS network. The layer-2 traffic is transported across a MPLS LSP using a two-level label stack. The ipaddress parameter identifies the peer LSR that is the endpoint of the tunnel. This ipaddress should be configured with a 32-bit prefix on the peer LSR. When the peer LSR is also an Extreme switch, then either OSPF must also be enabled on the VLAN that the ipaddress is assigned to (using the configure ospf add vlan command on the peer switch), or the peer switch must be configured to distribute direct routes into the OSPF domain (via the enable ospf export direct command). Note that the export command should be used when the tunnel LSP needs to cross OSPF area boundaries or when ESRP is
enabled on the VLAN that the ipaddress is assigned. The local_vlan_name parameter identifies the layer-2 traffic that is to be transported. All of the local traffic that the switch receives for this VLAN is transported across the tunnel.

When configuring static TLS tunnels, the tls-labels parameters specify the innermost labels of the tunnel label stack. The egress_label is inserted into the MPLS header of layer-2 frames forwarded onto the tunnel LSP by this switch, and must be meaningful to the peer TLS node. All traffic received from the tunnel LSP that contains the ingress_label is forwarded to the local VLAN identified by the local_vlan_name parameter. The tls-labels parameters are specified using hexadecimal notation. The value of the ingress_label parameter must be unique within the switch (i.e., the same ingress_label value cannot be used for two different tunnels). The valid range of the ingress label parameter is [8C000–8FFFF]. The valid range of the egress_label parameter is [00010–FFFFF] (note that if the peer LSR is also an Extreme switch, then the egress_label must be in the range [8C000–8FFFF]). Since LSPs are unidirectional in nature, coordinated configuration is required at both tunnel endpoint switches. The egress_label at one tunnel endpoint switch must match the ingress_label at the other tunnel endpoint switch, and vice versa.

When configuring dynamic TLS tunnels, the defined vcid parameters are encoded in a new martini-draft FEC-TLV and advertised in an LDP Label Mapping Message to the targeted LDP peer. Included in the Label Mapping Message is the advertised egress TLS tunnel label that is encoded in the Label TLV. The advertising LER automatically allocates the egress TLS tunnel label from the set of unused labels in the TLS LER Label Partition [8C000-8FFFF]. When the Label Mapping Message is received by the egress TLS tunnel peer, the egress TLS tunnel peer cross references the vcid parameters advertised in the martini-draft FEC-TLV with its own locally defined TLS tunnel vcid parameter values. If a vcid and groupid match is found, the TLS tunnel is bound to the local_vlan_name by correlating the advertised egress TLS tunnel label with the local VLAN ID. Once the TLS tunnel label and the local VLAN ID are dynamically bound, all traffic received from the tunnel LSP that contains the egress TLS tunnel label is forwarded to the local VLAN identified by the local_vlan_name parameter. The optional from command defines the local_endpoint_ipaddress from which the dynamic TLS tunnel is established. Since dynamic TLS tunnels must first establish an LDP session to the targeted LDP peer (TLS endpoint) prior to exchanging tunnel vcid parameters, the TLS endpoint switch must be capable of accepting LDP Hello messages for the configured TLS tunnel's targeted ipaddress. By default, the local_endpoint_ipaddress is the configured OSPF Router ID. The from parameter must be specified when dynamic TLS tunnels are used in conjunction with ESRP. The local_endpoint_ipaddress should be configured to match the local tunnel endpoint VLAN interface IP address (see Layer-2 Transport on page 43 for discussion on how to use ESRP to provide TLS redundancy). This allows dynamic TLS tunnels to properly fail over to the slave switch when both the master and the slave switch are configured with the same local_endpoint_ipaddress. The vcid is a non-zero 32-bit ID that defines the tunnel connection and the groupid is a 32-bit value that defines a dynamic TLS tunnel connection group. The groupid may be used to simultaneously delete all dynamic TLS tunnels in a group. If the groupid is not specified, its value defaults to zero.

When ingress traffic is forwarded to the local VLAN, the VLAN ID is set to the VLAN ID of the local VLAN, without regard to the VLAN ID in the MAC header of the frame received from the tunnel LSP. Thus, there is no requirement that all sites of an extended VLAN be configured to use the same VLAN ID, which can simplify network management in some situations.

**Example**

The following command creates a TLS tunnel to 11.0.4.11 for traffic originating from VLAN unc:

```
configure mpls add tls-tunnel rt40 11.0.4.11 unc tls-labels 8f001 8f004
```

To add a static labeled TLS tunnel, use the following command:

```
configure mpls add tls-tunnel <tunnel_name> [lsp <lsp_name> | <ipaddress> | <host_name>] <local_vlan_name> tls-labels <ingress_label> <egress_label>
```
To add a dynamic labeled TLS tunnel (martini-draft compliant), use the following command:

```
configure mpls add tls-tunnel <tunnel_name> [lsp <lsp_name> | <ipaddress> | <host_name>] <local_vlan_name> vcid <vcid> <groupid>
```

The `<tunnel_name>` parameter is a character string that is to be used to identify the TLS tunnel within the switch. It must begin with an alphabetic character and can contain up to 31 additional alphanumeric characters.

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls add vlan

configure mpls add vlan [<vlan name> | all] {ldp | rsvp-te}

**Description**

Enables LDP or RSVP-TE for one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>ldp</td>
<td>Enables LDP.</td>
</tr>
<tr>
<td>rsvp-te</td>
<td>Enables RSVP-TE.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

MPLS must be enabled on all VLANs that transmit or receive MPLS-encapsulated frames. Using the `configure mpls add vlan` command causes the LDP neighbor discovery process to begin on the specified VLAN.

**NOTE**

The specified VLAN must be configured with an IP address and must have IP forwarding enabled. IGMP snooping must also be enabled on the switch.

If all VLANs are selected, MPLS is enabled on all VLANs that have an IP address and IP forwarding enabled.

If you have enabled MPLS on an OSPF interface that is used to reach a particular destination, make sure that you enable MPLS on all additional OSPF interfaces that can reach that same destination (for example, enable MPLS on all VLANs that are connected to the backbone network).

**Example**

The following command enables RSVP-TE on vlan1:

```
configure mpls add vlan vlan1 rsvp-te
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls delete

    config mpls delete vpls [<vpls_name> | all]

Description
Deletes the VPLS with the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VPLS.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes the VPLS with the specified vpls_name. All VC-LSPs established to VPLS peers are terminated. The all keyword may be used to indicate that all VPLS instances are to be deleted.

Example
config mpls delete vpls myvpls

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch.
configure mpls delete tls-tunnel

configure mpls delete tls-tunnel [<tunnel_name> | group <groupid> | all]

Description
Deletes one or all TLS tunnels.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel_name</td>
<td>Specifies a TLS tunnel name.</td>
</tr>
<tr>
<td>group &lt;groupid&gt;</td>
<td>Specifies a group identifier</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all TLS tunnels.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes the TLS tunnel with the specified tunnel name. Specify the <groupid> if you want to delete all TLS tunnels belonging to a specific group. Specify the <groupid> if you want to delete all TLS tunnels belonging to a specific group. Use the all keyword to delete all TLS tunnels.

Example
The following command deletes the TLS tunnel rt40:

configure mpls delete tls-tunnel rt40

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls delete vlan

configure mpls delete vlan [<vlan name> | all] {ldp | rsvp-te}

Description
Disables LDP or RSVP-TE on one or all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>ldp</td>
<td>Disables LDP.</td>
</tr>
<tr>
<td>rsvp-te</td>
<td>Disables RSVP-TE.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Disables LDP or RSVP-TE on one or all VLANs. If not specified, both are disabled for the specified VLAN.

Example
The following command disables RSVP-TE on vlan1:

```
configure mpls delete vlan vlan1 rsvp-te
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls delete vpls

    config mpls delete vpls [<vpls_name> | all]

Description
Deletes the VPLS with the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>all</td>
<td>Marks all VPLS for deletion.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes the VPLS with the specified vpls_name. All VC-LSPs established to VPLS peers are terminated. The all keyword may be used to indicate that all VPLS instances are to be deleted.

Example
config mpls delete vpls myvpls

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls edge-service-mode

    config mpls slot <slot> edge-service-mode [vlan | port]

Description
Configures MPLS Layer 2 edge service mode for MPLS H-VPLS port mode.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>slot</td>
<td>Specifies a switch slot.</td>
</tr>
<tr>
<td>vlan</td>
<td>Specifies a vlan ID.</td>
</tr>
<tr>
<td>port</td>
<td>Specifies a switch port in the specified slot.</td>
</tr>
</tbody>
</table>

Default

edge-service-mode - vlan

Usage Guidelines

This command configures the MPLS Layer 2 edge service mode for all ports associated with the module in the specified slot. The keyword edge-service-mode is used to specify how customer interfaces are identified. The keyword vlan configures the module in the specified slot so that customer traffic is identified by the received packet's 802.1q tag. The keyword port configures the module in the specified slot so that customer traffic is identified based on the port that the packet was received. Port mode configured ports are implicitly defined as customer facing Layer 2 service ports. Thus, MPLS cannot be enabled on these ports. The default edge-service-mode is vlan.

Ports configured in different modes cannot send traffic between them without the use of the MPLS module. That is, traffic received on a port that is configured in vlan mode cannot switch traffic directly to a port on a module that is configured in port mode, and vice versa. Thus, ports configured in different modes cannot be members of the same VLAN or VPLS. VPLS ingress traffic can be received on a port that is in port mode and label switched out a port that is configured in vlan mode. Traffic received on ports in port mode is also switched directly to local egress ports that are members of the same VPLS. Configured VLANs for ports in vlan mode cannot conflict with core (or provider) network interior VLANs configured within the same switch.

Changing the edge-service-mode will disrupt traffic for all ports on the module in the specified slot.

Example

The following command configures the edge service mode for slot 1, vlan ID 10:

    config mpls slot 1 edge-service-mode 10

History

This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls health-check add mplsping

```bash
config mpls health-check add mplsping [ipaddress | prefix
<ipaddress/masklength> | <host_name> | lsp <lsp_name>]){interval-time
<seconds>} {trap-send-holdtime <seconds>}
```

**Description**

Configures an MPLS tunnel LSP service connectivity health-check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Option for specifying the forwarding equivalence class (FEC).</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Option for specifying the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Option for specifying the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Configures the tunnel LSP health-check</td>
</tr>
<tr>
<td>interval-time</td>
<td>Determines the rate at which ping packets are sent.</td>
</tr>
<tr>
<td>trap-send-holdtime</td>
<td>Specifies the interval after interval-time when service connectivity is considered down if there is no echo response.</td>
</tr>
</tbody>
</table>

**Default**

- interval-time range - 60 seconds
- trap-send-holdtime range - 10 seconds

**Usage Guidelines**

This command configures a MPLS tunnel LSP service connectivity health-check. The health-check command can be used to configure recurring tunnel LSP connectivity checks. If the configured tunnel LSP connectivity is lost, a trap is sent to alert management stations of a possible service failure and an error message is logged. Connectivity is verified by sending an MPLS ping packet. Up to 256 mplsping health-checks can be configured.

Ping packets are sent at the rate specified by the `interval-time`. If an echo response is not received within `trap-send-holdtime` seconds after the `interval-time` ping was sent, service connectivity is considered down and an error message is logged and a trap message may be sent. The valid `interval-time` range is 10 to 600 seconds with a default value of 60 seconds. The valid `trap-send-holdtime` range is 3 to 30 seconds with a default value of 10 seconds and must be less than the `interval-time`. Ping packets may be dropped due to spurious network conditions. In order to minimize service disconnect “false alerts”, when an echo request has not been received within `trap-send-holdtime/3` seconds, echo requests are sent in rapid succession at a rate of one per second. This operation continues until an echo response is received or the `trap-send-holdtime` expires. If an echo response is received before the `trap-send-holdtime` expires, the rapid sending of echo requests is immediately stopped and the service is deemed connected.

Specifying the LSP FEC configures the tunnel LSP health-check. The FEC can be specified using the `ipaddress`, `ipaddress/masklength` or `host_name` parameter. If the FEC is specified using the `host_name` parameter, the DNS client must be configured so that the `host_name` can first be resolved to an IP address. The resolved host name IP address is assumed to be a /32 prefix. If there is more than one outgoing LSP that matches the FEC, only one is used. For RSVP-TE LSPs, the FEC is implied from the LSP configuration. Thus, the `lsp` keyword may be used to configure an tunnel LSP health-check for `lsp_name`. 
**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls health-check delete mplsping

    config mpls health-check delete mplsping [<ipaddress> | <ipaddress/masklength> | <host_name> | lsp <lsp_name> | all]

Description
Deletes an MPLS tunnel LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Option for specifying the forwarding equivalence class (FEC).</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Option for specifying the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Option for specifying the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Deletes the tunnel LSP health-check</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all mplsping health-checks.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The command deletes a MPLS tunnel LSP service connectivity health-check. Deleting a LSP health-check, as specified by the ipaddress or host_name parameter or the prefix or lsp keyword, terminates and deletes the configured mplsping. If the all keyword is specified, all mplsping health-checks are deleted.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls health-check add vplsping

```
config mpls health-check add vplsping <vpls_name> [peer <ipaddress> | mac-address <macaddress>] {interval-time <seconds>} {trap-send-holdtime <seconds>}
```

**Description**

Configures a VPLS VC-LSP service connectivity health-check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>interval-time</td>
<td>Determines the rate at which ping packets are sent.</td>
</tr>
<tr>
<td>trap-send-holdtime</td>
<td>Specifies the interval after interval-time when service connectivity is considered down if there is no echo response.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command configures a VPLS VC-LSP service connectivity health-check. The healthcheck command can be used to configure recurring VC-LSP connectivity checks. If VC-LSP connectivity is lost, a trap is sent to alert management stations of a possible service failure and an error message is logged. Connectivity is verified by sending a VPLS ping packet. Up to 256 vplsping health-checks may be configured.

Ping packets are sent at the rate specified by the interval-time. If an echo response is not received within trap-send-holdtime seconds after the interval-time ping was sent, service connectivity is considered down and an error message is logged and a trap message may be sent. The valid interval-time range is 10 to 600 seconds with a default value of 60 seconds. The valid trap-send-holdtime range is 3 to 30 seconds with a default value of 10 seconds and must be less that the interval-time. Ping packets may be dropped due to spurious network conditions. In order to minimize service disconnect “false alerts”, when an echo request has not been received within trap-send-holdtime/3 seconds, echo requests are sent in rapid succession at a rate of one per second. This operation continues until an echo response is received or the trap-send-holdtime expires. If an echo response is received before the trap-send-holdtime expires, the rapid sending of echo requests is immediately stopped and the service is deemed connected.

Specifying the VPLS node address configures the VPLS health-check to a VPLS node. The VPLS node can be specified using the peer or mac-address keyword. When the peer's ipaddress is specified, the IP address is used to look up the corresponding VPLS node's MAC address. If the MAC address has not been learned, the health-check keyword will fail with a “No MAC address learned for IP address” error. The mac-address keyword specifies the target VPLS node or a customer MAC address. The macaddress parameter must be a unicast MAC address and is specified as a colon separated list of six bytes in hex format.
**Example**
None

**History**
This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure mpls health-check delete vplsping

    config mpls health-check delete vplsping <vpls_name> [peer <ipaddress> | mac-address <macaddress> | all]

**Description**

Deletes a VPLS VC-LSP service connectivity health-check.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all vplsping health-checks for the specified vpls_name.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

The command deletes a VPLS VC-LSP service connectivity health-check. Deleting a VC-LSP health-check, as specified by the peer or mac-address keyword, terminates and deletes the configured vplsping. If the all keyword is specified, all vplsping health-checks for the specified vpls_name are deleted.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls health-check delete vplsping

    config mpls health-check delete vplsping <vpls_name> [peer <ipaddress> | mac-address <macaddress> | all]

Description
Deletes a VPLS VC-LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>vpls_name</th>
<th>Identifies the VPLS within the switch (character string)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Option for specifying the health check.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all vplsping health-checks for the specified vpls_name.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
The command deletes a VPLS VC-LSP service connectivity health-check. Deleting a VC-LSP health-check, as specified by the peer or mac-address keyword, terminates and deletes the configured vplsping. If the all keyword is specified, all vplsping health-checks for the specified vpls_name are deleted.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls ldp acl

configure mpls ldp acl [enabled | disabled]

Description
Enables or disables an MPLS LDP Access Control List (ACL).

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>enabled</td>
<td>Enables MPLS LDP ACL such that all required authentication procedures are enforced.</td>
</tr>
<tr>
<td>disabled</td>
<td>Disables MPLS LDP ACL.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command enables or disables an MPLS LDP Access Control List (ACL). The enabled keyword specifies that the ACL be enabled. When enabled, all required authentication procedures are enforced. LDP ACLs cannot be enabled unless at least one LDP ACL peer has been configured. The disabled keyword specifies that the ACL be disabled. No authentication procedures are enforced. LDP ACLs must be disabled before all LDP ACL peers can be deleted. Changing the ACL enabled configuration may result in the termination of sessions or services with peers that cannot be validated. The LDP ACL status is displayed using the show mpls command.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
**configure mpls ldp acl add peer**

    config mpls ldp acl add [peer <ipaddress> | <host_name>]

**Description**

Adds an LDP peer to the ACL.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Identifies the peer from which targeted and non-targeted LDP sessions are accepted.</td>
</tr>
<tr>
<td>host_name</td>
<td>Identifies the peer. Must be able to be resolved to an IP address.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command adds an LDP peer to the ACL. The acl keyword is used to configure an LDP peer that is allowed to establish LDP peer session with this LSR. Up to 256 peers may be configured. The `ipaddress` parameter identifies the peer from which targeted and non-targeted LDP sessions are accepted. If the peer is specified using the `host_name` parameter, the DNS client must be configured so that the `host_name` can first be resolved to an IP address. LDP Hellos from IP addresses that are not included in the acl list are ignored.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only
configure mpls ldp acl delete peer

    config mpls ldp acl delete peer [<ipaddress> | <host_name> | all]

Description
Deletes a configured LDP peer from the ACL.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Identifies the peer for deletion.</td>
</tr>
<tr>
<td>host_name</td>
<td>Identifies the peer. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all LDP peers are deleted from the ACL.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes a configured LDP peer from the ACL. The ipaddress and host_name parameter identify the peer to be deleted from the ACL. When the keyword all is specified, all configured LDP peers are removed.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls ldp advertise

configure mpls ldp advertise [direct | rip | static] [all | none | route-map <route_map>]

**Description**

Configures a filter to be used by LDP when originating unsolicited label mapping advertisements to LDP neighbors.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>direct</td>
<td>Specifies that the advertisement filter is applied to the associated FECs with directly-attached routing interfaces.</td>
</tr>
<tr>
<td>rip</td>
<td>Specifies that the advertisement filter is applied to FECs associated with RIP routes exported by OSPF.</td>
</tr>
<tr>
<td>static</td>
<td>Specifies that the advertisement filter is applied to FECs associated with static routes.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that unsolicited label mapping advertisements are originated for all routes of the specified type.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no unsolicited label mapping advertisements are originated for the specified route type.</td>
</tr>
<tr>
<td>route-map</td>
<td>Specifies a route map is used to filter the origination of unsolicited label mapping advertisements for the specified route type.</td>
</tr>
</tbody>
</table>

**Default**

All—the default setting for the direct routing method.

None—the default setting for the RIP and static routing methods.

**Usage Guidelines**

Only the nlri-list route-map match operation keyword is supported for filtering origination of MPLS label advertisements.

You can configure how the advertisement filter is applied, as follows:

- **direct**—The advertisement filter is applied to the FECs associated with directly-attached routing interfaces.
- **rip**—The advertisement filter is applied to the FECs associated with RIP routes exported by OSPF.
- **static**—The advertisement filter is applied to the FECs associated with static routes.

You can configure the advertisement filter, as follows:

- **all**—All unsolicited label mappings are originated for all routes of the specified type (direct, RIP, or static). This is the default setting for direct routes.
- **none**—No unsolicited label mappings are originated for all routes of the specified type. This is the default setting for RIP and static routes.
• route-map <route_map>—The specified route map is used to permit or deny the origination of unsolicited label mappings for all routes of the specified type.

   The only supported route map match operation keyword is nlri-list. If selected, the access_profile parameter of the nlri-list keyword is compared to the FEC that is associated with each route.

   **NOTE**

   For more information on route maps, see the ExtremeWare Software Users Guide.

RIP routes are advertised with the Implicit NULL label and direct routes are advertised with an MPLS label, unless PHP is enabled.

Advertising labels for a large number of routes may increase the required number of labels that must be allocated by LSRs. Take care to ensure that the number of labels advertised by LERs does not overwhelm the label capacity of the LSRs.

**Example**

The following command configures a filter to be used by LDP when originating unsolicited label mapping advertisements for RIP routes:

```plaintext
configure mpls ldp advertise rip all
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls ldp advertise vlan

configure mpls ldp advertise [add | delete] vlan <vlan name>

Description
Configures LDP to originate an unsolicited label for the FECs associated with the directly attached routing interface of the specified VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>add</td>
<td>Originates an unsolicited label for the FECs associated with the directly attached routing interface of the specified VLAN</td>
</tr>
<tr>
<td>delete</td>
<td>Removes label origination of the direct route for the specified VLAN</td>
</tr>
<tr>
<td>vlan name</td>
<td>Specifies the name of the VLAN.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
Configures LDP to originate an unsolicited label for the FECs associated with the directly attached routing interface of the specified VLAN. The delete keyword removes label origination of the direct route for the specified VLAN. The LDP label origination configuration for directly attached routing interfaces can also be set using the configure mpls ldp advertise direct command.

Example
The following command configures LDP to advertise a label for the direct route configured for VLAN vlan1:

configure mpls advertise add vlan vlan1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls php

    configure mpls php [enabled | disabled]

Description
Enables and disables penultimate hop popping (PHP) at the egress LSR. When enabled, PHP is requested on all LSPs for which the switch is the egress LSR.

Syntax Description
This command has no arguments or variables.

Default
Disabled

Usage Guidelines
This command enables or disables whether PHP is requested by the egress LER.

When PHP is enabled, PHP is requested on all LSPs for which the switch is the egress LER.

PHP is requested by assigning the Implicit Null Label in an advertised mapping. PHP is always performed when requested by an egress LSR (for example, when the switch is acting as an intermediate LSR). The Implicit Null Label is always used in conjunction with routes exported by OSPF, regardless of the PHP configuration.

This command can only be executed when MPLS is disabled.

Example
The following command enables penultimate hop popping (PHP) at the egress LSR:
configure mpls php enabled

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls propagate-ip-ttl

configure mpls propagate-ip-ttl [enabled | disabled]

Description
Enables or disables the propagation of the IP time-to-live (TTL) field for routed IP packets. When propagation is enabled, each LSR is viewed as a router hop from an IP TTL perspective. When propagation is disabled, the LSP is viewed as a point-to-point link between the ingress LSR and the egress LSR.

Syntax Description
This command has no arguments or variables.

Default
N/A

Usage Guidelines
This command enables and disables the propagation of the IP TTL value for routed IP packets. The default setting is enabled.

NOTE
You must maintain identical propagate-ip-ttl settings on all LERs in the MPLS domain. Not doing so may cause packets to loop endlessly and not be purged from the network if a routing loop is inadvertently introduced.

When propagate-ip-ttl is disabled, the LSP is viewed as a point-to-point link between the ingress LSR and the egress LSR. Intermediate LSRs in the MPLS network are not viewed as router hops (from an IP TTL perspective). In this case, the IP TTL is decremented once by the ingress LSR and once by the egress LSR. When disabled, the MPLS TTL is set to 255 by the ingress LSR and is independent of the IP TTL.

When propagate-ip-ttl is enabled, each LSR is viewed as a router hop (from an IP TTL perspective). When a packet traverses an LSP, it emerges with the same TTL value that it would have had if it had traversed the same sequence of routers without being label-switched. When enabled, the MPLS TTL field is initially set to the IP TTL field at the ingress LSR, and the IP TTL field is set to the MPLS TTL by the egress LSR.

Example
The following command enables the propagation of the IP time-to-live (TTL) field for routed IP packets:

configure mpls propagate-ip-ttl enabled

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls qos-mapping

configure mpls qos-mapping [dot1p-to-exp | exp-to-dot1p] [all | <input_value>]/<output_value>

Description
Configures MPLS-specific QoS mappings.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dot1p-to-exp</td>
<td>Specifies that mappings are used in performing the ingress LSR function. The value in this priority field is set based on the QoS classification performed by the ingress I/O module.</td>
</tr>
<tr>
<td>exp-to-dot1p</td>
<td>Specifies that mappings are used when performing label swapping as an intermediate LSR and when performing the egress LSR function.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies to map all input values to the specified output value.</td>
</tr>
<tr>
<td>input_value</td>
<td>Specifies an input value.</td>
</tr>
<tr>
<td>output_value</td>
<td>Specifies an output value.</td>
</tr>
</tbody>
</table>

Default
Mapping tables are initialized such that an <input_value> of n is mapped to an <output_value> of n.

Usage Guidelines
The valid range of integers for the <input_value> and the <output_value> is 0 to 7. Two mappings are supported:
- dot1p-to-exp
- exp-to-dot1p

Dot1p-to-exp Mappings
The dot1p-to-exp mappings are used by the ingress LSR. When a non-MPLS ingress frame arrives at the MPLS module, the frame always contains an IEEE 802.1p priority field.

The value of the priority field is set based on the QoS classification performed by the ingress I/O module. The ingress I/O modules assign each packet to a hardware queue, based on the configured ExtremeWare QoS policies. There is a one-to-one mapping between the hardware queue and the 802.1p priority values that are inserted into frames forwarded to the MPLS module. For example, the 802.1p priority value is set to 0 for frames forwarded from hardware queue 0, set to 1 for frames forwarded from hardware queue 1, and so on.

The dot1p-to-exp table maps 802.1 priority values to MPLS EXP values. The table is completely flexible, such that any 802.1p priority <input_value> can be mapped to any EXP <output_value>. The EXP output_value is set in the MPLS header of the packet as it is forwarded to the MPLS network.
**Exp-to-dot1p Mappings**

The exp-to-dot1p mappings are used when the switch performs label swapping as an intermediate LSR and when the switch is the egress LSR. In both of these cases, the MPLS module receives an MPLS-encapsulated frame.

The EXP field in the frame is used as an <input_value> to the exp-to-dot1p table. The corresponding <output_value> is an 802.1p priority value. The 802.1p priority value is inserted into the frame before the frame is forwarded by the MPLS module.

The exp-to-dot1p table is completely flexible, such that any EXP <input_value> can be mapped to any 802.1p priority <output_value>.

The exp-to-dot1p table is also used by Packet over SONET (PoS) ports when classifying MPLS-encapsulated packets received from the SONET link. When a PoS port receives an MPLS-encapsulated packet from the SONET link, the packet is classified based on the EXP value in the MPLS shim header. The EXP value from the received frame is used as an index into the exp-to-dot1p mapping table to retrieve an 802.1p priority value. The frame is then assigned to a QoS profile, based on the retrieved 802.1p priority value. The mappings between 802.1p priority values and QoS profiles are configured using the following command:

```
configure dotip type
```

**Example**

The following command configures the dot1p-to-exp MPLS-specific QoS mappings:

```
configure mpls qos-mapping dot1p-to-exp 0/1
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls rsvp-te add lsp

configure mpls rsvp-te add lsp <lsp_name> path <path_name> {<profile_name>} {primary | secondary}

**Description**

Adds an RSVP-TE LSP.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lsp_name</td>
<td>Specifies the LSP name.</td>
</tr>
<tr>
<td>path_name</td>
<td>Specifies the path name</td>
</tr>
<tr>
<td>profile_name</td>
<td>Specifies the profile name.</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies the primary LSP.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies a secondary LSP.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

Both the `<lsp_name>` and `<path_name>` must be specified. The `<lsp_name>` parameter is a character string that is to be used to identify the LSP within the switch. The `<lsp_name>` string must begin with an alphabetic character and can contain up to 31 additional alphanumeric characters. The `<profile_name>` is optional. If omitted, the default profile is applied to the LSP. If no explicitly specified, the `<path_name>` defaults to the primary path. The LSP is immediately signaled as soon as it is configured. The maximum number of configurable LSPs is 1024.

**Example**

The following command adds a primary RSVP-TE LSP that takes the routed path named paththroughdenver:

```
configure mpls rsvp-te add lsp lsptonyc path paththroughdenver
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls rsvp-te add path

configure mpls rsvp-te add path <path_name> [<ipaddress> | <host_name>] {from <local_endpoint_vlan>}

Description
Adds a path to an RSVP-TE LSP.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path_name</td>
<td>Specifies the path name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address.</td>
</tr>
<tr>
<td>hostname</td>
<td>Specifies the hostname.</td>
</tr>
<tr>
<td>local_endpoint_value</td>
<td>Specifies the local endpoint from which the path is signaled.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

The <path_name> and <ipaddress> or <host_name> must be specified for the path. The <path_name> parameter is a character string that is to used to identify the path within the switch. The <path_name> string must begin with an alphabetic character, and may contain up to 31 additional alphanumeric characters. Each <path_name> represents a routed path to a single IP destination.

If the <host_name> is specified, the DNS client on the switch must be configured so that the <host_name> can first be resolved to an IP address. Alternate routed paths to the same IP destination may be configured by adding additional <path_names> and specifying the same <ipaddress> or <host_name> as the path endpoint.

The RSVP-TE path is not signaled until an LSP is added with the specified <path_name>. If no explicit route objects are configured, the path will follow the best-routed path to the configured <ipaddress> (or IP address obtained from DNS name resolution). Optionally, the from keyword can be used to specify the <local_endpoint_vlan> from which the path is signaled. The maximum number of configurable paths is 255.

Example
The following command adds a path to 76.42.10.1 called paththroughdenver:

configure mpls rsvp-te add path paththroughdenver 76.42.10.1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls rsvp-te add profile

configure mpls rsvp-te profile <profile_name> {bandwidth <bps>} {setup-priority <priority>} {hold-priority <priority>} {retry-timeout <seconds>} {hop-count <number>} {ping-interval <seconds>} {metric [<metric] | igp-tracking} {record [enabled | disabled]} {mtu <number>}

Description
Adds an RSVP-TE profile.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>profile_name</td>
<td>Specifies the profile name.</td>
</tr>
<tr>
<td>bandwidth</td>
<td>Specifies the reserved bandwidth for the LSP.</td>
</tr>
<tr>
<td>setup-priority</td>
<td>A value that is compared to the hold-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.</td>
</tr>
<tr>
<td>hold-priority</td>
<td>A value that is compared to the setup-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.</td>
</tr>
<tr>
<td>retry-timeout</td>
<td>Specifies the maximum number of seconds the switch allows for LSP setup.</td>
</tr>
<tr>
<td>ping-interval</td>
<td>Specifies how frequently an ICMP echo request is transmitted to the egress LSR IP address on the established LSP.</td>
</tr>
<tr>
<td>metric</td>
<td>Specifies a route metric used to determine if an established RSVP-TE LSP will actually be used to send data.</td>
</tr>
<tr>
<td>record</td>
<td>Specifies hop-by-hop path recording.</td>
</tr>
<tr>
<td>mtu</td>
<td>Specifies the MTU value transport payload packet (customer packet).</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
A profile is a set of attributes that are applied to the LSP when the LSP is configured using the configure mpls rsvp-te add lsp command. A default profile is provided which cannot be deleted, but can be applied to any configured LSP. The profile name for the default profile is default. The default profile parameter values are initially set to their respective default values. The maximum number of configurable profiles is 255 (one of which is reserved for the default profile).

The bandwidth parameter specifies the desired reserved bandwidth for the LSP. Any positive integer bps value is valid. Optionally, you can append the characters, k for kilobits, m for megabits, or g for gigabits, to the bps value to specify the unit of measure. If the k, m, or g, character is omitted, the unit of measure is assumed to be kilobits. The default bandwidth bps value is zero, which indicates that the QoS for the LSP is best effort. ExtremeWare does not support bandwidth reservation.

The setup-priority and hold-priority are optional parameters indicating the LSP priority. During path setup, if the requested bandwidth cannot be reserved through the LSR, the setup-priority parameter is compared to the hold-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established. Lower numerical values represent higher priorities. The setup-priority range is 0 to 7 and the default value is 7. The
configure mpls rsvp-te add profile

**hold-priority** range is also 0 to 7 and is set equal to the **setup-priority** by default. ExtremeWare does not support LSP preemption.

The **retry-timeout** keyword specifies the maximum number of seconds the switch allows for LSP setup. If the LSP cannot be established within **retry-timeout** seconds, the LSP is signaled again. The default value for **retry-timeout** is 30 seconds with a configurable range of 5 to 600 seconds. The **hop-count** parameter limits the number of LSRs the path can traverse, including the ingress and egress router. The default **hop-count** value is 255 with a configurable range of two to 255.

After an LSP has established, the egress LSR may be optionally pinged to determine end-to-end path connectivity. If a ping response is not received within \[2 \times \text{ping-interval} - 1\] seconds, the LSP is considered unavailable. The **ping-interval** keyword specifies how frequently an ICMP echo request is transmitted to the egress LSR IP address on the established LSP. The default **ping-interval** is zero, which indicates no end-to-end LSP health checking is performed. You can set the **ping-interval** value to any interval between 0 and 60 seconds.

The **route-metric** is used to determine if an established RSVP-TE LSP will actually be used to send data. Whenever the configured metric is less than, or equal, to the calculated IGP metric, the LSP is used for sending routed IP traffic. In this case, the LSP is also used to send TLS data when the TLS tunnel is configured by specifying the tunnel LSP endpoint IP address. Traffic is distributed across up to four equal-cost LSPs. The valid metric values range from 1 to 65535. Specifying the **igp-tracking** keyword forces the route metric to track the underlying IGP metrics. If no IGP metric exists for the LSP (for example, the LSP traverses a RIP network), the metric is ignored. Tracking IGP metrics is the default behavior.

The **record** keyword is used to enable hop-by-hop path recording. The enabled keyword causes the record route object (RRO) to be inserted into the path message. The RRO is returned in the reserve message and contains a list of IPv4 subobjects that describe the RSVP-TE path. Path recording by default is disabled. When disabled, no RRO is inserted into the path message.

The **mtu** keyword optionally specifies the MTU value transport payload packet (customer packet). The **mtu** value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same **mtu** value. If the **mtu** values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS **mtu** is set to 1500. The configurable **mtu** range is 1492 through 9216. Changing the **mtu** setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS **mtu** setting is greater than the MPLS **mtu** setting for the VC-LSP interface. The **vplsping** command may be used to verify end-to-end path connectivity for specific payload packet sizes.

**Example**

The following command adds a profile with the configured attributes:

- Reserved bandwidth signaled is 100 Mbps
- Tunnel LSP setup priority is 1
- Tunnel LSP hold priority is 0
- Route recording is enabled

```
configure mpls rsvp-te add profile customer1 bandwidth 100m setup-priority 1
hold-priority 0 record enabled
```
MPLS Commands—BlackDiamond Switch Only

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te delete lsp

configure mpls rsvp-te delete lsp [<lsp_name> | all]

Description
Deletes an RSVP-TE LSP.

Syntax Description

<table>
<thead>
<tr>
<th>isp_name</th>
<th>Specifies the name of the LSP.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
Deleting an LSP name disassociates all configured paths with this LSP and all configuration information for the LSP name is deleted. LSPs cannot be deleted if the specified <lsp_name> has been configured as the LSP for a TLS tunnel. If you specify the all keyword, all LSPs not associated with a TLS tunnel are deleted.

Example
The following command deletes all RSVP-TE LSPs:
configure mpls rsvp-te delete lsp all

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te delete path

    configure mpls rsvp-te delete path [<path_name> | all]

Description
Deletes an RSVP-TE path.

Syntax Description

<table>
<thead>
<tr>
<th>path_name</th>
<th>Specifies the name of the path.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
This command deletes a configured MPLS RSVP-TE routed path with the specified <path_name>. All associated configuration information for <path_name> is deleted. A path cannot be deleted as long as the <path_name> is associated with an LSP. If the all keyword is specified, all paths not associated with an LSP are deleted.

Example
The following command deletes all RSVP-TE paths:

    configure mpls rsvp-te delete path all

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te delete profile

configure mpls rsvp-te delete profile [<profile_name> | all]

Description
Deletes an RSVP-TE path profile.

Syntax Description

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Specifies the name of the profile.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
This command deletes a configured RSVP-TE profile with the specified profile name. The default profile cannot be deleted. If a profile is associated with a configured LSP, the profile cannot be deleted. If you specify the all keyword, all profiles not associated with an LSP are deleted (except for the default profile).

Example
The following command deletes all RSVP-TE path profiles:

configure mpls rsvp-te delete profile all

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te lsp add path

configure mpls rsvp-te lsp <lsp_name> add path <path_name> {<profile_name>} (secondary | primary)

**Description**

Adds a path to an RSVP-TE LSP.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lsp_name</td>
<td>Specifies the name of a configured LSP.</td>
</tr>
<tr>
<td>path_name</td>
<td>Specifies the path name.</td>
</tr>
<tr>
<td>profile_name</td>
<td>Specifies the profile name.</td>
</tr>
<tr>
<td>primary</td>
<td>Specifies the primary path.</td>
</tr>
<tr>
<td>secondary</td>
<td>Specifies a secondary path.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

The `<lsp_name>` must represent a configured LSP. Only one primary path and up to two secondary paths can be added per `<lsp_name>`. The `<path_name>` specified defaults to primary when no primary path has been configured for `<lsp_name>` and defaults to secondary if the primary path has been previously configured for `<lsp_name>`.

You do not need to configure the primary path for an LSP. Each `<path_name>` added to an `<lsp_name>` must be unique, but a `<path_name>` can be associated with multiple LSP names.

All configured primary and secondary paths for the `<lsp_name>` must have the same endpoint IP address. For example, three paths can be configured for the `<lsp_name>`, but all paths should represent different topological paths through the network to the same LSP endpoint.

Adding a secondary `<path_name>` designates a path as a hot-standby redundant path, used in the event that the primary or secondary path cannot be established or fails. Provided the `<path_name>` has not already been established, all `<path_name>`s are signaled as soon as they are associated with an `<lsp_name>`. If the primary `<path_name>` fails, is not configured, or cannot be established after the specified LSP retry-timeout, one of the configured secondary paths may become the active path for `<lsp_name>`. All of the secondary paths have equal preference; the first one available is chosen. If at any time the primary path is established, `<lsp_name>` immediately switches to using the primary path. If a secondary path fails while in use, the remaining configured secondary paths can become the active path for `<lsp_name>`.

**Example**

The following command adds a secondary path named paththroughdc for the specified LSP:

```
configure mpls rsvp-te lsp lsptonyc add path paththroughdc secondary
```
History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te delete path

    configure mpls rsvp-te delete path [<path_name> | all]

Description
Deletes an RSVP-TE path.

Syntax Description

<table>
<thead>
<tr>
<th>path_name</th>
<th>Specifies the name of the path.</th>
</tr>
</thead>
</table>

Default
N/A

Usage Guidelines
This command deletes a configured MPLS RSVP-TE routed path with the specified <path_name>. All associated configuration information for <path_name> is deleted. A path cannot be deleted as long as the <path_name> is associated with an LSP. If the all keyword is specified, all paths not associated with an LSP are deleted.

Example
The following command deletes all RSVP-TE paths.
configure mpls rsvp-te delete path all

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te add ero

configure mpls rsvp-te path <path_name> add ero [ipaddress <ipaddress/masklength> | <host_name>] {strict | loose} {order <number>}

Description
Adds an RSVP-TE explicit route.

Syntax Description

<table>
<thead>
<tr>
<th>Path Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path_name</td>
<td>Specifies the path name.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Specifies an LSR using either a /32 address, which may represent an LSR router ID, loopback address, or direct router interface, or an IP prefix, which represents a directly connected subnet.</td>
</tr>
<tr>
<td>strict</td>
<td>Specifies a strict subobject.</td>
</tr>
<tr>
<td>loose</td>
<td>Specifies a loose subobject.</td>
</tr>
<tr>
<td>order &lt;number&gt;</td>
<td>Specifies the LSR path order.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command adds an IP address to the explicit route object (ERO) for the specified path name. The RSVP-TE routed path may be described by a configured sequence of the LSRs and/or subnets traversed by the path. Each defined LSR or subnet represents an ERO subobject. Up to 64 subobjects can be added to each path name.

When specifying an LSR using the <host_name> parameter, the DNS client on the switch must be configured so that the <host_name> can first be resolved to an IP address. The ipaddress keyword identifies an LSR using either a /32 address, which may represent an LSR router ID, loopback address, or direct router interface, or an IP prefix, which represents a directly connected subnet. Each IP address or prefix is included in the ERO as an IPv4 subobject. Each specified subobject must be topologically adjacent to the next subobject, as listed in the ERO. If the subobject matches a direct router interface or a directly attached subnet, the switch verifies that the path message is received on the matching router interface. If the LSR specified matches the OSPF router ID or a configured loopback IP address, the router interface on which the packet is received is ignored.

If the IP address is specified as strict, the strict subobject must be topologically adjacent to the previous subobject as listed in the ERO. If the IP address is specified as loose, the loose subobject is not required to be topologically adjacent to the previous subobject as listed in the ERO. If omitted, the default subobject attribute is strict. Each IP address or prefix is included in the ERO as an IPv4 subobject.

If the subobject matches a direct router interface or a directly attached subnet, the switch verifies that the path message is received on the matching router interface. If the LSR specified matches the OSPF router-id of the immediate neighbor LSR.

1. The LSP next hop matches either the interface IP address or the OSPF router-id of the immediate neighbor LSR.
router ID or a configured loopback IP address, the router interface which the packet is received is ignored.

The LSR path order is optionally specified using the order keyword. The order number parameter is an integer value from 1 to 65535. IP prefixes with a lower number are sequenced before IP prefixes with a higher number. You can specify multiple paths and assign them an order number. The order number determines the path that the LSP follows. Thus, the LSP path follows the configured path of the IP prefix with the order value from low to high. If the order keyword is not specified, the number value for the LSR defaults to a value 100 higher than the current highest number value.

If the list of IP prefixes, added to the path, does not reflect an actual path through the network topology, the path message is returned with an error from a downstream LSR and the LSP is not established.

The order of a configured subobject cannot be changed. The ERO subobject must be deleted and re-added using a different order. If a subobject is added to or deleted from the ERO while the associated LSP is established, the path is torn down and is signaled again using the new ERO.

Duplicate ERO subobjects are not allowed. Defining an ERO for the path is optional. If you do not configure an ERO, the path is signaled along the best-routed path and the ERO is not included in the path message. When the last subobject in the ERO of the path message is reached and the egress IP node of the path has not been reached, the remaining path to the egress node is signaled along the best-routed path. Specification of an ERO could lead to undesirable routed paths, so you should be careful when terminating the ERO routed-path definition prior to the configured path egress node.

Example
The following command adds a strict ERO subobject of 192.18.32.5 to the specified path:

```
configure mpls rsvp-te path paththroughdenver add ero ipaddress 192.18.32.5
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te delete ero

configure mpls rsvp-te path <path_name> delete ero [all | ipaddress <ipaddress/masklength> | <host_name> | order <number>]

Description
Deletes an RSVP-TE explicit route.

Syntax Description

<table>
<thead>
<tr>
<th>path_name</th>
<th>Specifies the path name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress/masklength</td>
<td>Specifies an LSR using either a /32 address, which may represent an LSR router ID, loopback address, or direct router interface, or an IP prefix, which represents a directly connected subnet.</td>
</tr>
<tr>
<td>strict</td>
<td>Specifies a strict subobject.</td>
</tr>
<tr>
<td>loose</td>
<td>Specifies a loose subobject.</td>
</tr>
<tr>
<td>order &lt;number&gt;</td>
<td>Specifies the LSR path order.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines
This command deletes an LSR or subnet from the ERO for the specified path name. The LSR is specified using the ipaddress, <host_name>, or order parameter. If an LSR is deleted from an ERO while the associated LSP is established, the path is torn down and is signaled again using a new ERO. Use the all keyword to delete the entire ERO from the path name. When there is no configured ERO, the path is no longer required to take an explicit routed path. The path is then signaled along the best-routed path and no ERO is included in the path message.

Example
The following command deletes all configured ERO subobjects from the specified path:
configure mpls rsvp-te path paththroughdc delete ero all

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te profile

configure mpls rsvp-te profile <profile_name> {bandwidth <bps>} {setup-priority <priority>} {hold-priority <priority>} {retry-timeout <seconds>} {hop-count <number>} {ping-interval <seconds>} {metric [<metric> | igp-tracking]} {record [enabled | disabled]} {mtu <number>}

Description

Configures an existing RSVP-TE profile.

Syntax Description

<table>
<thead>
<tr>
<th>profile_name</th>
<th>Specifies the profile name.</th>
</tr>
</thead>
<tbody>
<tr>
<td>bandwidth</td>
<td>Specifies the reserved bandwidth for the LSP.</td>
</tr>
<tr>
<td>setup-priority</td>
<td>A value that is compared to the hold-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.</td>
</tr>
<tr>
<td>hold-priority</td>
<td>A value that is compared to the setup-priority of existing LSPs to determine if any of the existing LSPs need to be preempted to allow a higher priority LSP to be established.</td>
</tr>
<tr>
<td>retry-timeout</td>
<td>Specifies the maximum number of seconds the switch allows for LSP setup.</td>
</tr>
<tr>
<td>ping-interval</td>
<td>Specifies how frequently an ICMP echo request is transmitted to the egress LSR IP address on the established LSP.</td>
</tr>
<tr>
<td>metric</td>
<td>Specifies a route metric used to determine if an established RSVP-TE LSP will actually be used to send data.</td>
</tr>
<tr>
<td>record</td>
<td>Specifies hop-by-hop path recording.</td>
</tr>
<tr>
<td>mtu</td>
<td>Specifies the MTU value transport payload packet (customer packet).</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

This command configures RSVP-TE attributes for the specified profile. The <profile_name> must have been previously added. All of the LSP profile values are updated dynamically. For LSPs configured with this profile, the LSP parameters are updated automatically with the sending of the next refresh path message. If the metric is changed, all LSPs using this profile are rechecked against the calculated IGP metric. In some cases, the LSP may be torn down because of a profile configuration change. For example, if the bandwidth value is increased, the LSRs along the existing path may not be able to accommodate the additional reserved bandwidth. In this scenario, the LSP is torn down and signaled again.

The mtu keyword optionally specifies the MTU value transport payload packet (customer packet). The mtu value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same mtu value. If the mtu values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS mtu is set to 1500. The configurable mtu range is 1492 through 9216. Changing the mtu setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS MTU setting is greater than the MPLS MTU setting for the VC-LSP interface. The vplsping command may be used to verify end-to-end path connectivity for specific payload packet sizes.
Example
The following command configures the attributes for the specified profile:
```
configure mpls rsvp-te profile customer1 ping-interval 2
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls rsvp-te vlan

configure mpls rsvp-te vlan [<vlan name> | all] {hello-interval <seconds>} {refresh-time <seconds>} {summary-refresh-time <tenth-seconds>} {bundle-time <tenth-seconds>} {keep-multiplier <number>}

Description
Configures RSVP-TE protocol parameters

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies the VLAN name.</td>
</tr>
<tr>
<td>hello-interval</td>
<td>Specifies the RSVP hello packet transmission interval.</td>
</tr>
<tr>
<td>refresh-time</td>
<td>Specifies the interval for sending refresh path messages.</td>
</tr>
<tr>
<td>bundle-time</td>
<td>Specified the maximum amount of time a transmit buffer is held so that multiple RSVP messages can be bundled into a single PDU.</td>
</tr>
<tr>
<td>summary-refresh-time</td>
<td>Specifies the time interval for sending summary refresh RSVP messages.</td>
</tr>
</tbody>
</table>

Default
N/A

Usage Guidelines

This command configures the RSVP-TE protocol parameters for the specified VLAN. The RSVP-TE keyword all indicates that the configuration changes apply to all RSVP-TE enabled VLANs.

The hello-interval time specifies the RSVP hello packet transmission interval. The RSVP hello packet is used by the switch to detect when a RSVP-TE peer is no longer reachable. If an RSVP hello packet is not received from a peer with \( \text{hello-interval} \times \text{keep-multiplier} \) seconds, the peer is declared down and all RSVP sessions to and from that peer are torn down. The default hello-interval time is three seconds with a valid range from one to 60 seconds.

The refresh-time specifies the interval for sending refresh path messages. RSVP refresh messages provide “soft state” link-level keep-alive information for previously established paths and enables the switch to detect when an LSP is no longer active. RSVP sessions are torn down if an RSVP refresh message is not received from a neighbor within \([\text{keep-multiplier} + 0.5] \times 1.5 \times \text{refresh-time}\) seconds. The default refresh-time is 30 seconds and the default keep-multiplier value is three. The minimum and maximum refresh-time values are one and 36,000 seconds (or one hour) respectively. The minimum and maximum keep-multiplier values are one and 255 respectively.

The bundle-time, specified in tenths of a second, indicates the maximum amount of time a transmit buffer is held so that multiple RSVP messages can be bundled into a single PDU. The default bundle-time is zero, indicating that RSVP message bundling is not enabled. The bundle-time value may be set to any value between zero and 30 (or 3 seconds).

The summary-refresh-time, specified in tenths of a second, indicates the time interval for sending summary refresh RSVP messages. The summary-refresh-time must be less than the configured refresh-time. The default summary-refresh-time is zero, indicating that no summary refresh RSVP
messages are sent. The summary-refresh-time value may be set to any value between zero to 100 (or 10 seconds).

If configured, the bundled and summary refresh RSVP messages are only sent to RSVP-TE peers supporting RSVP refresh reduction.

Example
The following command configures the rsvp-te interface parameters for VLAN vlan1.

```
configure mpls rsvp-te vlan vlan1 hello-interval 2 refresh-time 5
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls tls-tunnel lsp

    config mpls tls-tunnel <tunnel_name> [add | delete] lsp <lsp_name>

Description

Deletes a VPLS VC-LSP service connectivity health-check.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tunnel_name</td>
<td>Refers to the TLS tunnel.</td>
</tr>
<tr>
<td>add</td>
<td>Allows addition of up to 4 RSVP-TE LSPs to the TLS tunnel.</td>
</tr>
<tr>
<td>delete</td>
<td>Removes the specified LSP.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the LSP.</td>
</tr>
</tbody>
</table>

Default

N/A

Usage Guidelines

This command configures additional LSPs for a TLS tunnel. The add keyword may be used to add up to four RSVP-TE LSPs to the TLS tunnel specified by tunnel_name. TLS traffic across the TLS tunnel is aggregated across all configured LSPs. LSP traffic aggregation is described in Equal-cost Multipath LSP Support on page 3. The delete keyword will remove the LSP specified by the lsp_name parameter from the VC-LSP aggregation list. If all the LSPs are deleted, the VC-LSP will attempt to use the best-routed path LSP, if one exists. If no LSPs exist to the TLS tunnel endpoint, TLS tunnel connectivity to the endpoint IP address is lost.

Example

None

History

This command was first available in an ExtremeWare 7.3.0.

Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls vlan ip-mtu

configure mpls vlan [<vlan name> | all] ip-mtu <number>

Description
Configures the IP MTU for frames transmitted onto MPLS LSPs via the specified egress VLAN. The range is 42 to 9190 (using jumbo frame sizes).

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies an IP MTU size.</td>
</tr>
</tbody>
</table>

Default
1500 bytes

Usage Guidelines
This command configures the IP MTU for frames transmitted onto MPLS LSPs via the specified egress VLAN. The default settings is 1500 bytes. If all is selected, the configuring MTU applies to all MPLS-enabled VLANs.

This command applies to the ingress LSR only when a received IP packet is destined for an MPLS LSP. In this case, if the length of the IP packet exceeds the configured MTU size for the egress VLAN and the Don’t Fragment (DF) bit is not set in the IP header of the packet, the packet is fragmented before it is forwarded onto an MPLS LSP. If the DF bit is set in the packet header, Path MTU Discovery starts.

Fragmentation is based on either the minimum value of the configured MPLS IP MTU size or the configured IP MTU size for the egress VLAN. (The IP MTU size is configured using the `configure ip-mtu <number> vlan <vlan name>` command.)

Configure the MPLS IP MTU so that the addition of the MPLS label stack the link layer header does not cause the packet to be too large to be transmitted on the egress ports. To avoid potential problems, enable jumbo frame support on all ports that are members of an MPLS VLAN.

Example
The following command configures the IP MTU for frames transmitted onto MPLS LSPs:

```
configure mpls vlan vlan1 ip-mtu 1550
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls vlan ldp propagate

    configure mpls vlan [<vlan name> | all] ldp propagate [all | none | route-map <route_map>]

**Description**
Configures a filter to be used by LDP when propagating unsolicited label mappings to all LDP neighbors on one or all VLANs.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all VLANs.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies that all unsolicited label mappings are propagated to the VLAN.</td>
</tr>
<tr>
<td>none</td>
<td>Specifies that no unsolicited label mappings are propagated to the VLAN.</td>
</tr>
<tr>
<td>route_map</td>
<td>Specifies the route map used to permit or deny the propagation of unsolicited label mappings to the VLAN.</td>
</tr>
</tbody>
</table>

**Default**
All unsolicited label mappings are propagated to the VLAN.

**Usage Guidelines**
This command configures a filter to be used by LDP when propagating unsolicited label mappings to all LDP neighbors on the specified VLAN. If all VLANs are selected, the settings of this command apply to all MPLS-enabled VLANs.

**Example**
The following command configures a filter to be used by LDP when propagating unsolicited label mappings to vlan1:

    configure mpls vlan vlan1 ldp propagate route-map bgp_out

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
configure vlan add track-lsp

configure vlan <vlan name> add track-lsp [<lsp_name> | ipaddress <ipaddress>/<masklength>]

**Description**
Configures the LSPs tracked by ESRP in order to determine the ESRP state of the specified VLAN.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies a LSP name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the route entry to be tracked.</td>
</tr>
</tbody>
</table>

**Default**
No diagnostic tracking

**Usage Guidelines**

LSP tracking provides MPLS with specific ESRP selection criteria for determining the ESRP status of a VLAN. LSP tracking is similar to route tracking and ping tracking in ESRP. ESRP can be configured to protect the user VLAN from disruptions in the MPLS network core.

This type of LSP protection is especially useful when providing ESRP redundant TLS L2 VPN services using Traffic Engineered LSPs that take completely different paths.

Using ESRP domains, LSP tracking can be easily scaled to support several TLS VLANs that are tunnelled across an L2 VPN using a single LSP. Instead of each TLS VLAN tracking the same LSP, all of the TLS VLANs are placed into an ESRP domain for which there is one non-TLS VLAN, configured to track the state of the LSP. When ESRP detects that the LSP has failed, all of the VLANs in the configured ESRP domain transition to neutral state and the backup LSR becomes the master switch for all of the TLS VLANs.

The `add track-lsp` command configures ESRP to track up to eight LSPs. Fail over to the slave switch is based on the total number of established tracked LSPs. The switch with the greatest number of established tracked LSPs is elected the master switch for the specified VLAN. Specifying the parameter `<lsp_name>` instructs ESRP to track the status of an RSVP-TE LSP. Specifying the `ipaddress` keyword instructs ESRP to track the LSP status for the IP prefix as defined by the `<ipaddress/masklength>` parameter. Both types of LSPs can be tracked simultaneously.

**Example**
The following command enables LSP route failure tracking for routes to the specified subnet:

`configure vlan esrp-1 add track-lsp 192.168.46.0/24`

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure vlan delete track-lsp

configure vlan <vlan name> delete track-lsp [<lsp_name> | ipaddress <ipaddress>/<masklength> | all]

Description
Disables LSP route tracking for an ESRP-enabled VLAN.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies an ESRP-enabled VLAN name.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies a LSP name.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the route entry to be tracked.</td>
</tr>
<tr>
<td>all</td>
<td>Specifies all LSPs.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
The delete track-lsp command removes an LSP from ESRP tracking for the specified VLAN. If you specify the all keyword, all configured LSPs are removed from ESRP tracking for the specified VLAN.

Example
The following command disables diagnostic failure tracking for VLAN esrp-1:
configure vlan esrp-1 delete track-lsp

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls vpls

    config mpls vpls <vpls_name> {vman-id <vman_id>} {mtu <number>}

**Description**

Configures transmit parameters for packets received on the local VPLS interface as specified by vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>vman-id</td>
<td>Specifies the VLAN ID used internally in the switch to identify the vpls port list configured for vpls_name.</td>
</tr>
<tr>
<td>number</td>
<td>Specifies the MTU value of the VPLS transport payload packet.</td>
</tr>
</tbody>
</table>

**Default**

Priority - 0

ttl_value - 4

number (MTU) - 1500

**Usage Guidelines**

This command optionally configures transmit parameters for packets received on the local VPLS interface as specified by vpls_name.

By default, the vman_id is automatically chosen when the vpls is configured, but may be changed by specifying the vman-id keyword. The vman-id parameter specifies the VLAN ID used internally in the switch to identify the vpls port list configured for vpls_name. Valid values are 1 through 4096. The specified vman-id cannot conflict with any other configured VLAN ID.

The mtu keyword optionally specifies the MTU value of the VPLS transport payload packet (customer packet). The mtu value is exchanged with vpls configured peer nodes. All VPLS peer nodes must be configured with the same mtu value. If the mtu values do not match, VC-LSPs cannot be established between VPLS peers. By default the VPLS mtu is set to 1500. The configurable mtu range is 1492 through 9216. Changing the mtu setting will cause established VC-LSPs to terminate. VPLS payload packets may be dropped if the VPLS MTU setting is greater than the MPLS MTU setting for the VC-LSP interface. The vplsping command may be used to verify end-to-end path connectivity for specific payload packet sizes (see VPLS Ping Command on page 3).

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls vpls add

```bash
config mpls vpls <vpls_name> add [vlan <vlan_name> | ports <port-list>]
```

**Description**

Configures service for VPLS.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS interface within the switch (character string)</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Logically binds the VLAN to the specified vpls.</td>
</tr>
<tr>
<td>port-list</td>
<td>Specifies a list of ports.</td>
</tr>
</tbody>
</table>

**Default**

N/A

**Usage Guidelines**

This command configures a local Ethernet VPLS interface for the specified `vpls_name`. The VPLS interface may be a VLAN or a physical port. Specifying the `vlan_name` logically binds the VLAN to the specified vpls. Only one VLAN may be configured per VPLS. Specifying a port-list logically binds one or more physical ports to the specified vpls. Only ports configured for edge-service-mode port can be directly added to a vpls (see Configure MPLS Edge Service Mode on page 3 for additional information). Edge-service-mode vlan ports must be added to a VLAN and the VLAN assigned to a vpls, since the VLAN ID (and not the port) is the service identifier. If multiple ports are added or there are multiple ports configured for `vlan_name`, VPLS traffic local to the switch is forwarded within the switch. Simultaneous support for both vlan and ports for a single vpls is not supported.

When a vlan interface has been configured for a VPLS, the VLAN is added to the VPLS as specified by the `vpls_name`. The VLAN ID is locally significant to each VPLS. Thus, each VLAN VPLS interface within the H-VPLS network, may have a different VLAN ID. This greatly simplifies VLAN ID coordination between metro network access points. Traffic may be switched locally between VLAN ports if more than one port is configured for the VLAN.

When a port interface has been configured for a VPLS, the port-list is automatically added to a unique VMAN ID. The VMAN ID assigned, is the highest unallocated VLAN ID. The VMAN allocated for the VLAN ID has the same name as the configured VPLS instance (i.e., `vpls_name`). Any additional local switch ports added to the VPLS are implicitly added to the VMAN. The VMAN uniquely maps to a `vpls_name` and thus identifies the ports that have been added to the Port VPLS interface. Because the VMAN ID must uniquely identify the port, the port cannot be added to any other local VLAN.

**Example**

```bash
config mpls vpls myvpls add [vlan <vlan_name> | ports <port-list>]
config mpls vpls myvpls add myvlan
config mpls vpls myvpls add ports 1:5
```

**History**

This command was first available in an ExtremeWare 7.3.0.
Platform Availability

This command is available on the BlackDiamond switch only.
configure mpls vpls add peer

```
config mpls vpls <vpls_name> add peer [<ipaddress> | <host_name>]
[core-to-core | spoke-to-core {primary | secondary} | core-to-spoke {vpls |
  tls {vcid <vcid>} {dot1q ethertype <hex_number>}] {lsp <lsp_name>}
```

**Description**

Configures a VPLS peer for the specified vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>core-to-core</td>
<td>Specifies the VPLS peer relationship which represents a member of a fully meshed VPLS core peer group.</td>
</tr>
<tr>
<td>spoke-to-core</td>
<td>Specifies the spoke connectivity from a spoke node to a core node.</td>
</tr>
<tr>
<td>core-to-spoke</td>
<td>Specifies the spoke connectivity from the core node to the spoke node.</td>
</tr>
<tr>
<td>vcid</td>
<td>Specifies an option for VC-LSP between the core and spoke.</td>
</tr>
<tr>
<td>tps</td>
<td>Specifies an option for VC-LSP between the core and spoke.</td>
</tr>
<tr>
<td>hex_number</td>
<td>Specifies the ethtype for dot1q</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command configures a VPLS peer for the specified vpls_name. Up to 32 peers may be configured for each VPLS. Peers may belong to multiple VPLS instances. The ipaddress parameter identifies the peer node that is the endpoint of the VC-LSP. The ipaddress should be configured with a 32-bit prefix on the peer node. When the peer node is also an Extreme switch, then either OSPF/ISIS must also be enabled on the VLAN that the ipaddress is assigned, or the peer switch must be configured to distribute direct routes into the OSPF/ISIS domain. Note that the export command should be used when the tunnel LSP needs to cross OSPF area boundaries or when ESRP is enabled on the VLAN that the ipaddress is assigned. If the VPLS peer is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address.

Per node, each peer relationship for each VPLS must be configured. The peer relationships are defined as either a core-to-core, core-to-spoke, or spoke-to-core. This relationship implicitly defines the packet flooding behavior for the VC-LSP set up to the configured peer.

A VPLS peer relationship defined as core-to-core indicates that the peer is a member of a fully meshed VPLS core peer group. Flood traffic received from a core node by the core node is forwarded to spoke nodes only.

A VPLS peer relationship defined as spoke-to-core specifies the spoke connectivity from a spoke node to a core node. Flood traffic received by a spoke node from a core node is forwarded to the local egress interface. The spoke-to-core keyword may optionally be qualified with the redundant configuration mode. The core node is either the primary or secondary VPLS peer. One primary core
node and up to two secondary core nodes may be added to vpls_name. The configured core node defaults to primary when no primary core node has been configured and defaults to secondary if a primary core node has previously been configured for vpls_name. Configuration of the primary core node is not required. All configured primary and secondary core nodes for the vpls_name must be configured with a different endpoint IP address. Adding a secondary core node designates the node as a hot-standby redundant H-VPLS core node. A backup VC-LSP is established but is not used. Packets received on the backup VC-LSP are discarded. In the event that a VC-LSP cannot be established or the active VC-LSP fails, the VC-LSP to one of the secondary core nodes becomes the active VC-LSP. When a fail-over occurs, all secondary core nodes have equal preference; the first one available is chosen. If at any time the VC-LSP to the primary core node is re-established, the switch immediately terminates the VC-LSP to the secondary core node and begins using the VC-LSP to the primary core node. The VC-LSP to the secondary core node is re-established and returns to hot-standby state. Dropping the VC-LSP to the secondary core node forces the core node to flush its MAC FDB relative to the terminated VC-LSP and to propagate this information throughout the H-VPLS network. If the VC-LSP to the secondary core node fails while in-use, the VC-LSP to the remaining configured secondary core node becomes the active VC-LSP. The VC-LSP to the secondary core node remains the active VC-LSP unless the primary VC-LSP is re-established.

A VPLS peer relationship defined as core-to-spoke specifies the spoke connectivity from the core node to the spoke node. Flood traffic received from a spoke node by the core node is forwarded to all core-node and spoke-node peers. The core-to-spoke may be optionally qualified with the VC-LSP signaling mode. The VC-LSP between the core and spoke may be signaled as vpls, tls, or tps. VC-LSPs established to a tls configured spoke are signaled using the martini-draft VLAN FEC. Martini tls VC-LSPs carry traffic for a single VLAN. Thus, tls core-to-spoke VC-LSPs are incompatible with local egress VPLS port interfaces (i.e., tls VC-LSPs and local egress ports can not be configured for the same vpls). VC-LSPs established to an tps configured spoke are signaled using the martini-draft Ethernet FEC. Martini tps VC-LSPs carry traffic for a set of ports (i.e., port-list). Thus, tps core-to-spoke VC-LSPs are incompatible with local egress VPLS VLAN interfaces (i.e., tps VC-LSPs and a local egress VLAN can not be configured for the same vpls). The vcid of the martini VC-LSP can be optionally specified for either tls or tps. If the vcid is not specified, the configured VPLS VPN ID is used to signal the vcid. VC-LSPs established to a vpls configured spoke are signaled using the VPLS FEC. The spoke node must use the VC-LSP signaling method configured on the core node or the VC-LSP will not be established. If the VC-LSP signaling mode is not specified when the core-to-spoke keyword is specified, vpls signaling is selected by default. VPLS spoke nodes support additional features that are not defined in the martini-drafts. These features are automatically enabled when vpls is signaled and are disabled when tls or tps is signaled. These features include support for MAC Address Withdraw TLV, VPLS OAM packets, and purging looping packets based on the VC-FEC TTL.

Packets are never forwarded onto a VC-LSP from which the packet was received.

Optionally, the peer VC-LSP connection can be configured to use a specific RSVP-TE LSP. The lsp keyword specifies which LSP to use. The LSP must have previously been configured. If the lsp is configured and the LSP specified by lsp_name terminates, VPN connectivity to the VPLS peer also terminates. (To protect the LSP, backup paths can be configured to provide alternate paths to the peer ipaddress. See Add a Path to a Traffic Engineered LSP on page 3.) If the lsp keyword is omitted, the VC-LSP will use the best-routed path LSP to the peer ipaddress. If the best-routed path LSP fails, the next best routed path LSP will be used. In this case, failing over to the next best-routed path LSP will most likely require a route topology convergence.

Example

None
History
This command was first available in an ExtremeWare 7.3.

Platform Availability
This command is available on the BlackDiamond switch only
configure mpls vpls delete

    config mpls vpls <vpls_name> delete [vlan <vlan_name> | ports <port-list> | all]

**Description**

Deletes a VPLS peer from the specified vpls_name.

**Syntax Description**

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>vcid</td>
<td>Qualifies a specific core-to-spoke Martini VC-LSP.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all VPLS peers.</td>
</tr>
</tbody>
</table>

**Default**

N/A.

**Usage Guidelines**

This command deletes a VPLS peer from the specified vpls_name. When the VPLS peer is deleted, VPN connectivity to the VPLS peer is terminated. The optional `vcid` keyword may be specified to fully qualify a specific core-to-spoke Martini VC-LSP. The `all` keyword may be used to indicate that all VPLS peers be deleted.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
configure mpls vpls delete peer

    config mpls vpls <vpls_name> delete peer [<ipaddress> {vcid <vcid>} | <host_name> {vcid <vcid>} | all]

Description
Deletes a VPLS peer from the specified vpls_name.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>vcid</td>
<td>Qualifies a specific core-to-spoke Martini VC-LSP.</td>
</tr>
<tr>
<td>all</td>
<td>Deletes all VPLS peers.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command deletes a VPLS peer from the specified vpls_name. When the VPLS peer is deleted, VPN connectivity to the VPLS peer is terminated. The optional vcid keyword may be specified to fully qualify a specific core-to-spoke Martini VC-LSP. The all keyword may be used to indicate that all VPLS peers be deleted.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
configure mpls vpls peer

    config mpls vpls <vpls_name> peer [<ipaddress> | <host_name>] [add | delete] [lsp <lsp_name>]

Description
Configures additional LSPs to a VPLS peer.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for the peer node that is the endpoint of the VC-LSP</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the peer host name.</td>
</tr>
<tr>
<td>add</td>
<td>Permits addition of up to four RSVP-TE LSPs to the VPLS peer.</td>
</tr>
<tr>
<td>delete</td>
<td>Removes the LSP specified by the lsp_name parameter from the VC-LSP aggregation list.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Removes the specified lsp.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command configures additional LSPs to a VPLS peer. The add keyword may be used to add up to four RSVP-TE LSPs to the VPLS peer. Traffic to the VPLS peer is aggregated across all configured LSPs. LSP traffic aggregation is described in Equal-cost Multipath LSP Support on page 3. The delete keyword will remove the LSP specified by the lsp_name parameter from the VC-LSP aggregation list. If all the LSPs are deleted, the VC-LSP will attempt to use the best-routed path LSP, if one exists. If no LSPs exist to the VPLS peer, VPN connectivity to the VPLS peer is lost.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
disable mpls

Description
Disables MPLS on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Disabling MPLS causes all LSPs to be released and all LDP neighbor sessions to be terminated.

Example
The following command globally disables MPLS on the switch:

disable mpls

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
enable mpls

  enable mpls

Description
Enables MPLS on the switch.

Syntax Description
This command has no arguments or variables.

Default
Disabled.

Usage Guidelines
Disabling MPLS causes all LSPs to be released and all LDP neighbor sessions to be terminated.

Example
The following command globally enables MPLS on the switch:

  enable mpls

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
mplsping

mplsping {continuous} [[<ipaddress> | prefix <ipaddress/masklength> | <host_name>] {next-hop [<ipaddress> | <host_name>]}) | lsp <lsp_name>] {from <ipaddress>} {exp <exp_value>} {ping-address <ipaddress>} {start-size <size> {end-size <size}}> {reply-mode [ip | mpls]}

Description
Sends an MPLS ping packet to a FEC over an LSP.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Determines the tunnel LSP on which the MPLS echo request.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the source IP address in the MPLS echo request.</td>
</tr>
<tr>
<td>exp_value</td>
<td>Specifies the experimental bits in the MPLS shim header of the MPLS echo</td>
</tr>
<tr>
<td>start_size</td>
<td>Specifies the number of bytes to include as payload data in the MPLS ping</td>
</tr>
<tr>
<td>end_size</td>
<td>Determines whether size of the packet will increment by one byte for each</td>
</tr>
<tr>
<td>isp_name</td>
<td>Specifies the tunnel LSP on which to send the MPLS echo request.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the return path for the MPLS echo response. Routes back to the</td>
</tr>
<tr>
<td>mpls</td>
<td>Specifies the return path for the MPLS echo response. Switches the echo</td>
</tr>
</tbody>
</table>

Default
exp_value - 0
dot1p_value - 0

Usage Guidelines
This command sends an MPLS ping packet to a FEC over an LSP. The mplsping command can be used to verify data plane connectivity across an LSP. This is useful, since not all failures can be detected using the MPLS control plane. The FEC can be specified using the ipaddress, ipaddress/masklength or host_name parameter. If the FEC is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address. The resolved host name IP address is assumed to be a /32 prefix. If there is more than one outgoing LSP that matches the FEC, the MPLS echo request will be sent on each LSP in round-robin fashion. For RSVP-TE LSPs, the FEC is implied from the LSP configuration. The lsp keyword may be used to specify the tunnel LSP on which to send the MPLS echo request. The tunnel LSP on which the MPLS echo request is sent is specified by the lsp_name parameter. The TTL value in the MPLS Echo Request is set to 255.
The from keyword is used to specify the source IP address used in the MPLS echo request. This is the IP address used by the target LSR will use to send the MPLS echo reply. If not specified, the OSPF/ISIS router ID is used.

The optional exp keyword is used to specify the Experimental bits in the MPLS shim header of the MPLS echo request. Valid exp_value parameter values are 0 through 7. The default value is 0.

The optional dot1p keyword is used to specify the 802.1p bits in the MPLS echo request. Valid dot1p_value parameter values are 0 through 7. The default value is 0.

The optional continuous keyword specifies that MPLS ping packets be sent continuously. Pressing any key can interrupt the operation.

The optional size keyword specifies the number of bytes to include as payload data in the MPLS ping packet. If no start_size parameter is specified, the size of the payload data is eight bytes. The minimum valid start_size value is one. The maximum start_size value is variable, depending on the type of MPLS ping packet sent, but the total size of the MPLS ping packet cannot exceed the configured jumbo packet size, if jumbo frames are enabled, or 1518 if jumbo frames are disabled. If the end_size parameter is specified, the size of the packet will increment by one byte for each new MPLS echo request sent. The next MPLS echo request is not sent until the MPLS echo response for the previous packet is received. This is useful for detecting interface MTU mismatch configurations between LSRs. The switch ceases sending MPLS echo requests when the specified end_size value is reached, the MPLS ping is user interrupted, or a MPLS echo response is not received after four successive retries.

The optional reply-mode keyword is used to specify the return path for the MPLS echo response. When the ip option is specified, the MPLS echo reply is routed back to the sender via an IPv4 packet with the IP Router Alert option. When the mpls option is specified, the MPLS echo reply is switched back to the sender via an IPv4 packet over an LSP. If there is no return LSP available, the MPLS echo reply is not sent. This option is useful for determining if there is a failure along the return LSP. If the reply-mode is not specified, the mpls reply mode is used.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
mplstrace

mplstrace [<ipaddress> | prefix <ipaddress/masklength> | <hostname>] [<next-hop [<ipaddress> | <host_name>]]] | lsp <lsp_name>] {from <ipaddress>} {reply-mode [ip | mpls]} {ttl <max_ttl_value>} {ping-address <ipaddress>} {detail}

Description
Traces the path an LSP takes for the specified FEC.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Specifies the FEC.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the FEC. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the source IP address in the MPLS echo request.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the tunnel LSP on which to send the MPLS echo request.</td>
</tr>
<tr>
<td>ip</td>
<td>Specifies the return path for the MPLS echo response. Routes back to the sender via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Specifies the return path for the MPLS echo response. Switches the echo reply back to the sender via an IPv4 packet over an LSP.</td>
</tr>
<tr>
<td>max_ttl_value</td>
<td>Specifies the maximum TTL value in the MPLS echo request packet.</td>
</tr>
</tbody>
</table>

Default

max_ttl_value = 30.

Usage Guidelines
This command traces the path an LSP takes for the specified FEC. The mplstrace command works by repeatedly sending a MPLS echo request. The TTL value is incremented for each successive MPLS echo request sent. The sending LSR waits 5 seconds before sending the next MPLS echo request. This operation continues until either the egress LSR for the FEC is reached, the maximum TTL value is reached, or the operation is interrupted. For each response received, the following information is displayed on the console: IP address of the replying LSR, return code, and an indication of a MPLS echo reply timeout if no response was received.

The FEC can be specified using the ipaddress, ipaddress/masklength or hostname parameter. If the FEC is specified using the host_name parameter, the DNS client must be configured so that the host_name can first be resolved to an IP address. The resolved host name IP address is assumed to be a /32 prefix. The lsp keyword may be used to specify the LSP to trace. The selected LSP is specified by the lsp_name parameter.

The from keyword is used to specify the source IP address used in the MPLS echo request. This is the IP address used by the target LSR will use to send the MPLS echo reply. If not specified, the OSPF/ISIS router ID is used.

The optional reply-mode keyword is used to specify the return path for the MPLS echo response. When the ip option is specified, the MPLS echo reply is routed back to the sender via an IPv4 packet with the IP Router Alert option. When the mpls option is specified, the MPLS echo reply is switched back to the sender via an IPv4 packet over an LSP. If the reply-mode is not specified, the mpls reply mode is used.
The `ttl` keyword optionally specifies the maximum TTL value in the MPLS echo request packet. The TTL value is decremented along the path at each LSR. When the TTL value reaches zero, the packet is not forwarded but is redirected to the control plane for additional processing. When the TTL value specified by the `max_ttl_value` parameter is exceeded, the `mplstrace` command ends. The valid `max_ttl_value` range is one to 30 with a default value of 30.

**Example**

None

**History**

This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
show fdb vpls

    show fdb vpls {<vpls_name>} {peer [<ipaddress> | <host_name>]}
show mpls health-check mplsing

show mpls health-check mplsing {detail | <ipaddress> | prefix <ipaddress/masklength> | <host_name> | lsp <lsp_name>}

Description
Displays the configuration and status for MPLS tunnel LSP health-checks.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>detail</td>
<td>Displays the health-check information in comprehensive detail format.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Display specific mplsing information for the specified address.</td>
</tr>
<tr>
<td>ipaddress/masklength</td>
<td>Display specific mplsing information for the specified address.</td>
</tr>
<tr>
<td>host_name</td>
<td>Display specific mplsing information for the specified host. Must be able to be resolved to an IP address.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the LSP to trace.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays the configuration and status for MPLS tunnel LSP health-checks. If no optional keywords are specified, information is displayed in tabular format for all configured MPLS tunnel LSP health-checks. Health-check information displayed includes the type of health-check, current status, and relevant configuration parameters. If the optional detail keyword is specified, the health-check information is displayed in a comprehensive detail format. The detail format includes total state transition count from up to down and down to up, time of last failure, total up time, and total down time, and error code (if applicable). Optionally, an ipaddress, ipaddress/masklength, host_name, or lsp_name parameter can be specified to display specific mplsing information. This information is always displayed in the detailed format.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls health-check vplsping

show mpls health-check vplsping {detail | <vpls_name> {peer <ipaddress> | mac-address <macaddress>}} {detail}

Description
Displays the configuration and status for VPLS health-checks.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Displays only health-checks associated with the specified vpls.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays the health-check information in comprehensive detail format.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Restricts the vplsping information as specified.</td>
</tr>
<tr>
<td>macaddress</td>
<td>Restricts the vplsping information as specified.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays the configuration and status for VPLS health-checks. If no optional keywords are specified, information is displayed in tabular format for all configured VPLS health-checks. Optionally, if the vpls_name parameter is specified, only the health-checks associated with the specified vpls are displayed. Health-check information displayed includes the type of health-check, current status, and relevant configuration parameters. If the optional detail keyword is specified, the health-check information is displayed in a comprehensive detail format. The detail format includes total state transition count from up to down and down to up, time of last failure, total up time, and total down time, and error code (if applicable). The optional peer and mac-address keywords may be specified to further restrict the vplsping information displayed for the vpls_name. Information displayed for a specific ipaddress or macaddress is always displayed in the detailed format.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls ldp acl

   show mpls ldp acl {<ipaddress> | <host_name>}

Description
Displays the list of configured LDP ACL entries.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address for a specific LDP ACL.</td>
</tr>
<tr>
<td>host_name</td>
<td>Specifies the host name for a specific LDP ACL.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays the list of configured LDP ACL entries. Optionally, a specific LDP ACL can be displayed by specifying the ipaddress or host_name for the configured ACL.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls

    show mpls {vlan <vlan name>} {detail}

Description
Displays MPLS configuration information for one or all VLANs. Omitting the vlan keyword displays information for all VLANs.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan name</td>
<td>Specifies a VLAN name.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
When the \texttt{vlan} parameter is omitted, this command displays the values of all MPLS configuration parameters that apply to the entire switch, the current status of peer LSRs, and a list of the VLANs for which MPLS is enabled.

When the \texttt{vlan} parameter is specified, this command displays the current values of the MPLS configuration parameters that are specific to the VLAN.

If the optional \texttt{detail} keyword is specified, additional detailed VLAN information is displayed.

Example
The following command displays MPLS configuration information for the VLAN accounting:

```bash
show mpls vlan accounting
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls forwarding

show mpls forwarding {summary | detail | inactive | host <ipaddress> (detail | inactive) | prefix <ipaddress/masklength> (detail | inactive) | rsvp-te <ipaddress> (detail)}

Description
Displays information from the FEC-to-NHLFE database, used when forwarding non-MPLS packets onto an LSP. Also displays information for RSVP-TE LSPs.

Syntax Description

<table>
<thead>
<tr>
<th>Keyword</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays only the summary route information associated with labeled paths.</td>
</tr>
<tr>
<td>host</td>
<td>Displays information for a single FEC.</td>
</tr>
<tr>
<td>prefix</td>
<td>Displays information for a single FEC.</td>
</tr>
<tr>
<td>rsvp-te</td>
<td>Displays only the RSVP-TE forwarding label mapping</td>
</tr>
<tr>
<td>inactive</td>
<td>Causes inactive mappings to be displayed. This keyword does not apply to the rsvp-te keyword, because RSVP-TE operates in DoD mode.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays information from the Forwarding Equivalence Class (FEC)-to-Next Hop Label Forwarding Entry (NHLFE) database. This command also displays information for RSVP-TE LSPs.

If the host or prefix keywords are specified, summary information is displayed for a single FEC. Use the summary keyword to display summary route information associated with labeled paths.

By default, the information displayed includes:

- Next hop IP address
- Outgoing label
- Interface number of the outgoing VLAN

If the detail keyword is specified, the following additional information is displayed:

- Outgoing port number
- Counts of packets and bytes that have been transmitted using the database entry

By default, information is displayed for active mappings. To display information for liberally-retained inactive mappings, use the inactive keyword. An inactive mapping is a mapping that was received from an LDP peer, but is not being used to reach the associated FEC. Using the inactive keyword causes inactive mappings to be displayed. The inactive keyword does not apply to RSVP-TE LSPs, because RSVP-TE operates in downstream-on-demand mode.
Example
The following command displays information from the FEC-to-NHLFE database:
show mpls forwarding prefix 10.1.1.1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls interface

    show mpls interface {ldp | targeted-ldp | rsvp-te}

**Description**
Displays targeted LDP and RSVP-TE interface information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ldp</td>
<td>Specifies LDP interfaces.</td>
</tr>
<tr>
<td>targeted-ldp</td>
<td>Specifies targeted LDP interfaces.</td>
</tr>
<tr>
<td>RSVP-TE</td>
<td>Specifies RSVP-TE interfaces.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
Displays targeted LDP and RSVP-TE interface information, including targeted LDP and RSVP-TE peer IP address and peer state. Specifying the keyword `ldp`, `targeted-ldp`, or `rsvp-te` limits the information displayed to only those interface types.

**Example**
The following command displays interface information for RSVP-TE interfaces:

```
show mpls interface rsvp-te
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
show mpls label

show mpls label {summary {detail} | <label_number> {detail} | host <ipaddress> {detail} | prefix <ipaddress/masklength> {detail} | rsvp-te <ipaddress> {detail}}

Description
Displays information from the Incoming Label Map (ILM), used when forwarding packets that arrive as labeled MPLS packets.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Specifies the number of labels allocated from each label range partition.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
<tr>
<td>label_number</td>
<td>Specifies an MPLS label number.</td>
</tr>
<tr>
<td>host &lt;ipaddress&gt;</td>
<td>Specifies a particular host FEC type.</td>
</tr>
<tr>
<td>prefix</td>
<td>Specifies a particular prefix FEC type.</td>
</tr>
<tr>
<td>rsvp-te</td>
<td>Specifies only RSVP-TE assigned labels</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays information from the Incoming Label Map (ILM), which is used when forwarding packets that arrive labeled as MPLS packets.

When the label_number parameter is omitted, summary information is displayed for all incoming label assignments that have been made by the switch. When the label_number is specified, summary information is displayed for the label.

Use the fec keyword to display the label associated with an FEC. You can specify both host and prefix FEC types. The summary keyword displays the number of labels allocated from each label range partition.

By default, the information displayed includes:

- Next hop IP address
- Outgoing and incoming labels
- Interface number of the outgoing VLAN
- FEC associated with the incoming label

If the detail keyword is specified, the following additional information is displayed:

- Outgoing port number
- Counts of packets and bytes that have been received with the incoming label
Counts of packets and bytes that have been transmitted with the outgoing label

LSP type

This command also displays information from the Incoming Label Map (ILM) for RSVP-TE LSPs.

**Example**

The following command displays the summary information from the Incoming Label Map:

```
show mpls label summary
```

**History**

This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**

This command is available on the BlackDiamond switch only.
show mpls ldp

    show mpls ldp {<ipaddress>} {detail}

Description
Displays MPLS LDP session information for one or all LSP sessions.

Syntax Description

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies an IP address.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
Omitting the ipaddress parameter displays LDP session information for all LDP sessions.

This command displays information about the status of LDP peers. Summary information is displayed for all known LDP peers and LDP peer sessions. If you specify the <ipaddress> of the LDP peer, information for a single LDP peer is displayed. To display additional information in the comprehensive detailed format, use the detail keyword.

Displayed summary information includes:

- Peer type (targeted or not targeted)
- Peer status
- Peer sessions
- Peer session state

If you specify the detail keyword, the following additional information is displayed:

- LDP error counts
- LDP status timers
- Maximum PDU length

Example
The following command displays MPLS LDP session information for the LDP entity 10.1.1.1:

    show mpls ldp 10.1.1.1

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.
Platform Availability

This command is available on the BlackDiamond switch only.
**show mpls qos-mapping**

```
show mpls qos-mappings
```

**Description**
Displays MPLS-specified QoS mappings for dot1p-to-exp and exp-to-dot1p.

**Syntax Description**
This command has no arguments or variables.

**Default**
N/A.

**Usage Guidelines**
Configured mappings for both dot1p-to-exp and exp-to-dot1p are displayed.

**Example**
The following command displays MPLS QoS mapping information:
```
show mpls qos-mappings
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
show mpls rsvp-te

    show mpls rsvp-te {<ipaddress>} {detail}

Description
Displays RSVP-TE LSP configuration information.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Specifies the IP address of the RSVP-TE interface.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays information about the status of RSVP-TE enabled interfaces. Summary information is displayed for all known RSVP-TE peers including the peer IP address and peer status. If you specify the ipaddress of the RSVP-TE interface, the information for a single RSVP-TE interface is displayed. Additional information is displayed in the detailed format if you specify the optional detail keyword. The more detailed RSVP-TE information includes the number and type of RSVP messages transmitted through the local RSVP-TE interface.

Example
The following displays detailed information about all configured RSVP-TE LSPs:

```
show mpls rsvp-te detail
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls rsvp-te lsp

    show mpls rsvp-te lsp {<lsp_name>} {detail}

Description
Displays the RSVP-TE LSP.

Syntax Description

<table>
<thead>
<tr>
<th>Argument</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>lsp_name</td>
<td>Specifies the name of the LSP.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays the configuration and status information for RSVP-TE LSPs. Information is listed in tabular format and includes the LSP name, LSP state, active path name, bandwidth requested, bandwidth actually reserved, ERO flag, egress LSR, LSP up-time, and RSVP error codes (if LSP setup failed). If you specify a specific LSP name, only information for the specified LSP is displayed. If you specify the optional `detail` keyword, additional information is displayed for each LSP. The detailed information includes a list of all configured paths, including the path state, error codes for the LSP associated with each path, up-time for each LSP, the bound profile name, and a list of TLS tunnels configured to use the LSP.

Example
The following displays the configuration and status information for all configured RSVP-TE LSPs in detailed format:

```
show mpls rsvp-te lsp detail
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls rsvp-te path

    show mpls rsvp-te path {<path_name>} {detail}

**Description**
Displays the RSVP-TE routed path.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>path_name</td>
<td>Specifies the name of the path.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
This command displays the configuration and status information for MPLS RSVP-TE routed paths. Information is listed in tabular format and includes the path name, path endpoint LSR IP address, and local VLAN (if configured). If the path endpoint is specified as a host name, the host name and the DNS resolved IP address are both displayed. If a specific path name is specified, only information for the specified path is displayed. If you specify the optional detail keyword, the list of subobjects specified for the explicit route object and any LSPs that are configured to use the path are displayed.

**Example**
The following displays information about all RSVP-TE routed paths in detailed format:

```plaintext
show mpls rsvp-te path detail
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
show mpls rsvp-te profile

    show mpls rsvp-te profile {<profile_name>}

Description
Displays the RSVP-TE path profile.

Syntax Description

| profile_name | Specifies the name of the profile. |

Default
N/A.

Usage Guidelines
By default, this command displays all configured profile parameters for the specified profile. If the profile name is omitted, the profile parameter values for all configured LSP profiles are displayed.

Example
The following command displays the profile parameter values for all configured LSP profiles:

```
show mpls rsvp-te profile
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls tls-tunnel

show mpls tls-tunnel {summary | detail | <tunnel_name> {detail} | vlan <vlan_name> {detail}}

Description
Displays configuration and status information for TLS tunnels.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Specifies to display summary TLS tunnel counts.</td>
</tr>
<tr>
<td>detail</td>
<td>Specifies to display the information in detailed format.</td>
</tr>
<tr>
<td>tunnel_name</td>
<td>Specifies a TLS tunnel name.</td>
</tr>
<tr>
<td>vlan_name</td>
<td>Specifies a VLAN name.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays configuration and status information for one or all TLS tunnels. The information displayed for each tunnel includes:

- The values of all configuration parameters for the tunnel.
- The current status of the tunnel LSP.
- Transmit and receive counts in terms of packets and bytes.

If the optional detail keyword is specified, TLS tunnel information is displayed using the comprehensive detail format.

If the optional summary keyword is specified, summary TLS tunnel counts are displayed. The summary counters displayed include the total number of active static and dynamic TLS tunnels.

Example
The following command displays configuration and status information for the TLS tunnel rt40:

```
show mpls tls-tunnel rt40
```

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
show mpls vpls

show mpls vpls {summary | detail | <vpls_name> {detail | | peer [<ipaddress> | <host_name>]}} | peer [<ipaddress> | <host_name>] {detail}}

**Description**
Displays VPLS configuration and status information.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>summary</td>
<td>Displays summary counts.</td>
</tr>
<tr>
<td>vpls_name</td>
<td>Displays information for the specified vpls.</td>
</tr>
<tr>
<td>detail</td>
<td>Displays additional information in comprehensive detail format.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
<tr>
<td>host_name</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
<tr>
<td>detail (peer)</td>
<td>Specifies all VPLS.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
This command displays VPLS configuration and status information. The `show mpls vpls` command (without specifying any optional parameters) displays all currently configured VPLS instances for the switch. Information displayed includes the VPLS name, IP addresses of peers, peer mode, VC-LSP state, and local egress VLAN or ports. If the `vpls_name` is specified, information is displayed for the specified vpls. If the optional `detail` keyword is specified, additional information is displayed in comprehensive detail format. The detail format additionally displays transmit and receive packet and byte counts. Optionally, specifying the peer keyword qualified by the `ipaddress` or `host_name`, displays VPLS information for the specified peer in detailed format. If the peer keyword is specified and is unqualified by a `vpls_name`, all VPLS instances that the peer is a member of are displayed. The `summary` keyword displays a set of summary counts. The counts include the number of VPLS instances, configured VPLS peers, active VPLS peers, targeted LDP sessions, VC-LSPs, and errors.

**Example**
None

**History**
This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**
This command is available on the BlackDiamond switch.
show mpls vpls nodes

    show mpls vpls {summary | detail | <vpls_name> {detail | | peer
                   [<ipaddress> | <host_name>]} | peer [<ipaddress> | <host_name>] {detail}}

Description
Displays information about all the nodes in the H-VPLS network.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vpls_name</td>
<td>Specifies the VPLS nodes that are members of the VPN.</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
<tr>
<td>host_name</td>
<td>Displays all VPLS instances of which the peer is a member, as specified.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command displays information about all the nodes in the H-VPLS network. When the optional vpls_name is specified, only VPLS nodes that are members of the VPN as specified by vpls_name are displayed. If vpls_name is omitted, information pertaining to all VPLS nodes is displayed. Information displayed includes IP address of each node, MAC address of each node, VPN ID, and immediate or remote node indication.

Example
None

History
This command was first available in an ExtremeWare 7.3.0.

Platform Availability
This command is available on the BlackDiamond switch.
unconfigure mpls

unconfigure mpls

Description
Resets MPLS configuration parameters to the default settings.

Syntax Description
This command has no arguments or variables.

Default
N/A.

Usage Guidelines
This command resets the following configuration parameters:

- IP-MTU
- LDP propagation filter settings on all VLANs
- LDP advertisement filter settings
- LDP session timers
- RSVP-TE interface parameters
- RSVP-TE profile parameters
- Settings for propagate-ip-ttl
- QoS mapping tables

Example
The following command resets MPLS configuration parameters to the default settings:
unconfigure mpls

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
unconfigure mpls

    unconfigure mpls [hello-hold-time | session-keep-alive-time]

Description
Restores the default values for hello-hold-time or session-keep-alive-time.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>hello-hold-time</td>
<td>Specifies a hello hold time.</td>
</tr>
<tr>
<td>session-keep-alive-time</td>
<td>Specifies a session keep alive time.</td>
</tr>
</tbody>
</table>

Default
The default hello-hold-time is 15 seconds.
The default session-keep-alive-time is 40 seconds.

Usage Guidelines
This command can only be executed when MPLS is disabled.
The hello-hold-time is the amount of time, in seconds, an LSR maintains a record of the label space requested by potential LDP peers. An LSR must receive an LDP hello packet at least hello-hold-time seconds after the last hello packet was received, or the LSR concludes that the LDP peer has failed or no longer wishes to label switch using the previously advertised label space.
The session-keep-alive-time specifies the minimum amount of time, in seconds, that an LSR must receive an LDP PDU from an LDP peer to which it has an established LDP session. If an LDP PDU is not received within the specified session-keep-alive-time since the reception of the last LDP PDU, the LDP session is torn down.

Example
The following command restores the default values for hello-hold-time:

    unconfigure mpls hello-hold-time

History
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.
This command was subsequently incorporated into ExtremeWare 7.0.0.

Platform Availability
This command is available on the BlackDiamond switch only.
unconfigure mpls qos-mapping

    unconfigure mpls qos-mapping [dotp-to-exp | exp-to-dot1p | lsp <lsp_name>]

**Description**
Restores the default values for the specified QoS mapping table.

**Syntax Description**

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dotp-to-exp</td>
<td>Specifies dot1p-to-exp mapping.</td>
</tr>
<tr>
<td>exp-to-dot1p</td>
<td>Specifies exp-to-dot1p mapping.</td>
</tr>
<tr>
<td>lsp_name</td>
<td>Specifies the name of an LSP.</td>
</tr>
</tbody>
</table>

**Default**
N/A.

**Usage Guidelines**
The default contents of either QoS mapping table maps an input value of $n$ to an output value of $n$.

**Example**
The following command restores the default values for the dot1p-to-exp QoS mapping table:

```
unconfigure mpls qos-mapping dotp-to-exp
```

**History**
This command was first available in an ExtremeWare IP Technology Services Release based on v6.1.8b12.

This command was subsequently incorporated into ExtremeWare 7.0.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
vplsping

vplsping {continuous} <vpls_name> [ip-address | mac-address <macaddress>] {next-hop [ip-address | <host_name>]} {from <source_macaddress>} {ping-address <ipaddress>} {start-size <size} {end-size <size}} {reply-mode [ip | mpls | vpls]}

Description

Sends VPLS ping packets to another VPLS node or to a specific destination MAC address.

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vplsping</td>
<td>Identifies the VPLS within the switch (character string)</td>
</tr>
<tr>
<td>ip-address</td>
<td>Specifies the address to look up the corresponding VPLS node's MAC address.</td>
</tr>
<tr>
<td>mac-address</td>
<td>Specifies the MAC address that is being “pinged.”</td>
</tr>
<tr>
<td>source-macaddress</td>
<td>Specifies the source MAC address used for the VPLS echo request.</td>
</tr>
<tr>
<td>start-size</td>
<td>Specifies the number of bytes to include as payload data in the VPLS ping packet.</td>
</tr>
<tr>
<td>end-size</td>
<td>Determines if the size of the packet will increment by one byte for each new VPLS echo request sent.</td>
</tr>
<tr>
<td>ip</td>
<td>Determines whether the VPLS echo reply is routed back to the sender, specified in the L2 VPN Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Determines if the VPLS echo reply is routed back to the sender over an MPLS LSP.</td>
</tr>
<tr>
<td>vpls</td>
<td>Determines if the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet.</td>
</tr>
</tbody>
</table>

Default

N/A.

Usage Guidelines

This command sends a VPLS ping packet to another VPLS node. The vplsping command can be used to verify data plane connectivity between any two VPLS nodes. This is useful, since not all failures can be detected using the MPLS or VPLS control plane. The VPLS ping is a modified MPLS ping sent in-band over a VC-LSP for a specific MAC address. The target MAC address of the VPLS echo request may represent a VPLS node's MAC address or a customer MAC address. VPLS nodes forward the VPLS echo request using their local MAC FDB. If the VPLS ping reaches a VPLS egress node, a VPLS echo reply is sent based on a local FDB lookup. VPLS ping packets are never forwarded out local VPLS egress interfaces. The TTL value in the VPLS echo request is set to 255.

The VPLS node can be specified using the ip-address parameter. When the ip-address parameter is specified, the IP address is used to look up the corresponding VPLS node's MAC address. If the MAC address has not been learned, the vplsping command will fail with a “No MAC address learned for IP address” error. The mac-address keyword specifies the MAC address that is being pinged. The mac-address may represent the MAC address of a VPLS node or a customer MAC address. The macaddress parameter must be a unicast MAC address and is specified as a colon separated list of six
bytes in hex format. The specified or learned MAC address is copied into the destination MAC address
field of the VPLS echo request and is included in the L2-VPN Prefix Target FEC TLV. By default, the
switch's MAC address is used for the source MAC address of the VPLS echo request. The from keyword
optionally specifies the source MAC address used for the VPLS echo request. This option allows the
VPLS echo request to be sent as if it originated from a customer's source MAC address. If link
aggregation is supported along the path to the destination MAC address, this insures that the VPLS
ping verifies connectivity through the VPLS network for the exact same path that the customer's traffic
would travel.

The optional continuous keyword specifies that VPLS ping packets be sent continuously. The operation
can be interrupted by pressing any key.

The optional size keyword specifies the number of bytes to include as payload data in the VPLS ping
packet. If no start_size parameter is specified, the size of the payload data is eight bytes. The
minimum valid start_size value is one. The maximum start_size value is variable, depending on
the type of VPLS ping packet sent, but the total size of the VPLS ping packet cannot exceed the
configured jumbo packet size, if jumbo frames are enabled, or 1518 if jumbo frames are disabled. If the
end_size parameter is specified, the size of the packet will increment by one byte for each new VPLS
echo request sent. The next VPLS echo request is not sent until the VPLS echo response for the previous
packet is received. This is useful for detecting interface MTU mismatch configurations between VPLS
nodes. The node ceases sending VPLS echo requests when the specified end_size value is reached, the
VPLS ping is interrupted, or a VPLS echo response is not received after four successive retries.

The optional reply-mode keyword is used to specify the return path for the VPLS echo response. When
the ip option is specified, the VPLS echo reply is routed back to the sender, specified in the L2 VPN
Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option. If the mpls option is specified, the
VPLS echo reply is routed back to the sender over an MPLS LSP. If no LSP is available, the VPLS echo
reply is not sent. When the vpls option is specified, the VPLS echo reply is switched in-band back to
the sender via a VPLS encapsulated IPv4 packet. This option is useful for determining if there is a
failure along the return VPLS VC-LSP path. If the reply-mode is not specified, the vpls reply mode is
used.

**Example**
None

**History**
This command was first available in an ExtremeWare 7.3.0.

**Platform Availability**
This command is available on the BlackDiamond switch only.
vplstrace

vplstrace <vpls_name> [<ipaddress> | mac-address <macaddress>]
{next-hop [<ipaddress> | <host_name>]}
{ping-address <ipaddress>}
{reply-mode [ip | mpls | vpls]}
{ttl <max_ttl_value>}
{detail}

Description
Traces the path a packet takes to another VPLS node, or to a specific destination MAC address.

Syntax Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipaddress</td>
<td>Determines whether the IP address is used to look up the corresponding VPLS node’s MAC address.</td>
</tr>
<tr>
<td>macaddress</td>
<td>Specifies the MAC address being “pinged.”</td>
</tr>
<tr>
<td>ipaddress</td>
<td>Specifies the source IP address in the MPLS echo request.</td>
</tr>
<tr>
<td>ip</td>
<td>Routes back to the sender as specified in the L2 VPN Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option.</td>
</tr>
<tr>
<td>mpls</td>
<td>Routes back to the sender over an MPLS LSP.</td>
</tr>
<tr>
<td>vpls</td>
<td>Determines if the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet.</td>
</tr>
<tr>
<td>max_ttl_value</td>
<td>Specifies the maximum TTL value in the VPLS echo request packet.</td>
</tr>
</tbody>
</table>

Default
N/A.

Usage Guidelines
This command traces the path a packet with a specific destination MAC address takes through the H-VPLS network for vpls_name. The vplstrace command works by sending a VPLS Ping or VPLS echo request (i.e., MPLS echo request for a VC-FEC in-band over the H-VPLS network). The TTL value in the VC-FEC label is initially set to 1. The TTL value is incremented for each successive VPLS echo request sent. The sending node waits 5 seconds before sending the next VPLS echo request. This operation continues until the egress VPLS node for the L2 VPN Prefix VC-FEC is reached, the maximum TTL value is reached, or the operation is interrupted. For each response received, the following information is displayed on the console: MAC address of the replying H-VPLS node, IP address of node (if known), return code, and an indication of a VPLS echo reply timeout if no response was received.

The VPLS node can be specified using the ipaddress parameter. When the ipaddress parameter is specified, the IP address is used to look up the corresponding VPLS node’s MAC address. If the MAC address has not been learned, the vplstrace command will fail with a “No MAC address learned for IP address” error. The mac-address keyword specifies the MAC address that is being pinged. The mac-address may represent the MAC address of a VPLS node or a customer MAC address. The macaddress parameter must be a unicast MAC address and is specified as a colon separated list of six bytes in hex format. The specified or learned MAC address is copied into the destination MAC address field of the VPLS echo request and is included in the L2-VPN Prefix Target FEC TLV.

The optional reply-mode keyword is used to specify the return path for the VPLS echo response. When the ip option is specified, the VPLS echo reply is routed back to the sender, specified in the L2 VPN Prefix sub-TLV, via an IPv4 packet with the IP Router Alert option. If the mpls option is specified, the
VPLS echo reply is routed back to the sender over an MPLS LSP. If no LSP is available, the VPLS echo reply is not sent. When the vpls option is specified, the VPLS echo reply is switched in-band back to the sender via a VPLS encapsulated IPv4 packet. This option is useful for determining if there is a failure along the return VPLS VC-LSP path. If the reply-mode is not specified, the vpls reply mode is used.

The ttl keyword optionally specifies the maximum TTL value in the VPLS echo request packet. The TTL value in the VC-FEC label is decremented along the path at each VPLS node. When the TTL value in the VC-FEC label reaches zero, the packet is not forwarded but is redirected to the control plane for additional processing. When the TTL value specified by the max_ttl_value parameter is exceeded, the vplstrace command ends. The valid max_ttl_value range is one to 30 with a default value of 4.

Example

None

History

This command was first available in an ExtremeWare 7.3.0.

Platform Availability

This command is available on the BlackDiamond switch only.
Index of Commands

A
abort diagnostics cable 2232
C
clear account lockout 70
clear accounting counters 2069
clear APmgmt port history 1247
clear APmgmt redirect-db history 2084
clear APmgmt unknown-ap history 2085
clear bgp neighbor counters 1847
clear bgp neighbor flap-statistics 1848
clear counters 657
clear debug-trace 1124
clear dlcs 431
clear elrp stats 1485
clear elsm auto-restart ports 1486
clear elsm counters ports 1488
clear fdb 404
clear igmp group 1934
clear igmp snooping 1935
clear inline-power connection-history slot 2275
clear inline-power fault ports 2276
clear inline-power stats 2277
clear inline-power stats ports 2277
clear iparp 1586
clear ipfdb 1587
clear ipmc cache 1936
clear ipmc fdb 1937
clear isis adjacency 1707
clear isis lsd 1708
clear log 658
clear log counters 660
clear log diag error 662
clear log diag remap 663
clear mpls vpls counters 2425
clear nat 472
clear netlogin state 830
clear netlogin state mac-address 831
clear session 71
clear slb connections 492
clear slb persistence 493
clear slot 251
clear transceiver-test 664
clear wireless ports counters 1248
clear wireless ports interface ap-scan results 1249
clear wireless ports interface client-history counters 1250
clear wireless ports interface client-scan counters 1251
clear wireless ports interface client-scan results 1252
clear wireless ports logs 1253
configure access-profile add 832
configure access-profile delete 835
configure access-profile mode 836
configure account 72
configure account password-policy char-validation 74
configure account password-policy history 76
configure account password-policy lockout-on-log-in-failures 77
configure account password-policy max-age 78
configure account password-policy min-length 79
configure antenna-profile 1254
configure application examination ports 2233
configure aps 2108
configure aps add 2109
configure aps authenticate 2111
configure aps delete 2112
configure aps force 2113
configure aps lockout 2114
configure aps manual 2115
configure aps timers 2116
configure atm add pvc 2096
configure atm delete pvc 2098
configure atm scrambling 2100
configure auth mgmt-access local 837
configure auth mgmt-access radius 839
configure auth mgmt-access radius-accounting 840
configure auth mgmt-access tacacs 841
configure auth mgmt-access tacacs-accounting 843
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure auth netlogin radius</td>
<td>845</td>
</tr>
<tr>
<td>configure auth netlogin radius-accounting</td>
<td>846</td>
</tr>
<tr>
<td>configure backplane-ls-policy</td>
<td>252</td>
</tr>
<tr>
<td>configure banner</td>
<td>81</td>
</tr>
<tr>
<td>configure banner netlogin</td>
<td>82</td>
</tr>
<tr>
<td>configure bgp add aggregate-address</td>
<td>1850</td>
</tr>
<tr>
<td>configure bgp add confederation-peer sub-AS-number</td>
<td>1851</td>
</tr>
<tr>
<td>configure bgp add network</td>
<td>1852</td>
</tr>
<tr>
<td>configure bgp AS-number</td>
<td>1853</td>
</tr>
<tr>
<td>configure bgp cluster-id</td>
<td>1854</td>
</tr>
<tr>
<td>configure bgp confederation-id</td>
<td>1855</td>
</tr>
<tr>
<td>configure bgp delete aggregate-address</td>
<td>1856</td>
</tr>
<tr>
<td>configure bgp delete confederation-peer sub-AS-number</td>
<td>1857</td>
</tr>
<tr>
<td>configure bgp delete network</td>
<td>1858</td>
</tr>
<tr>
<td>configure bgp local-preference</td>
<td>1859</td>
</tr>
<tr>
<td>configure bgp med</td>
<td>1860</td>
</tr>
<tr>
<td>configure bgp neighbor as-path-filter</td>
<td>1861</td>
</tr>
<tr>
<td>configure bgp neighbor dampening</td>
<td>1862</td>
</tr>
<tr>
<td>configure bgp neighbor maximum-prefix</td>
<td>1864</td>
</tr>
<tr>
<td>configure bgp neighbor next-hop-self</td>
<td>1866</td>
</tr>
<tr>
<td>configure bgp neighbor nlri-filter</td>
<td>1867</td>
</tr>
<tr>
<td>configure bgp neighbor no-dampening</td>
<td>1868</td>
</tr>
<tr>
<td>configure bgp neighbor password</td>
<td>1869</td>
</tr>
<tr>
<td>configure bgp neighbor peer-group</td>
<td>1871</td>
</tr>
<tr>
<td>configure bgp neighbor route-map-filter</td>
<td>1872</td>
</tr>
<tr>
<td>configure bgp neighbor route-reflector-client</td>
<td>1873</td>
</tr>
<tr>
<td>configure bgp neighbor send-community</td>
<td>1874</td>
</tr>
<tr>
<td>configure bgp neighbor soft-reset</td>
<td>1875</td>
</tr>
<tr>
<td>configure bgp neighbor source-interface</td>
<td>1876</td>
</tr>
<tr>
<td>configure bgp neighbor timer</td>
<td>1877</td>
</tr>
<tr>
<td>configure bgp peer group timer</td>
<td>1894</td>
</tr>
<tr>
<td>configure bgp peer-group as-path-filter</td>
<td>1879</td>
</tr>
<tr>
<td>configure bgp peer-group dampening</td>
<td>1880</td>
</tr>
<tr>
<td>configure bgp peer-group maximum-prefix</td>
<td>1882</td>
</tr>
<tr>
<td>configure bgp peer-group next-hop-self</td>
<td>1884</td>
</tr>
<tr>
<td>configure bgp peer-group nlri-filter</td>
<td>1885</td>
</tr>
<tr>
<td>configure bgp peer-group no-dampening</td>
<td>1886</td>
</tr>
<tr>
<td>configure bgp peer-group password</td>
<td>1889</td>
</tr>
<tr>
<td>configure bgp peer-group remote-AS-number</td>
<td>1890</td>
</tr>
<tr>
<td>configure bgp peer-group route-map-filter</td>
<td>1891</td>
</tr>
<tr>
<td>configure bgp peer-group route-reflector-client</td>
<td>1887</td>
</tr>
<tr>
<td>configure bgp peer-group send-community</td>
<td>1888</td>
</tr>
<tr>
<td>configure bgp peer-group soft-reset</td>
<td>1892</td>
</tr>
<tr>
<td>configure bgp peer-group source-interface</td>
<td>1893</td>
</tr>
<tr>
<td>configure bgp peer-group weight</td>
<td>1895</td>
</tr>
<tr>
<td>configure bgp routerid</td>
<td>1896</td>
</tr>
<tr>
<td>configure bgp soft-reconfiguration</td>
<td>1897</td>
</tr>
<tr>
<td>configure bootprelay add</td>
<td>1588</td>
</tr>
<tr>
<td>configure bootprelay delete</td>
<td>1589</td>
</tr>
<tr>
<td>configure bootprelay dhcp-agent information option</td>
<td>1592</td>
</tr>
<tr>
<td>configure configuration-mode</td>
<td>1092</td>
</tr>
<tr>
<td>configure cpu-dos-protect</td>
<td>848, 849, 851, 852, 853</td>
</tr>
<tr>
<td>configure cpu-dos-protect (port-based)</td>
<td>854</td>
</tr>
<tr>
<td>configure cpu-dos-protect alert-threshold</td>
<td>847</td>
</tr>
<tr>
<td>configure cpu-dos-protect trusted-ports</td>
<td>855</td>
</tr>
<tr>
<td>configure debug elsm-port</td>
<td>1489, 1491</td>
</tr>
<tr>
<td>configure debug elsm-system</td>
<td>1489, 1491</td>
</tr>
<tr>
<td>configure debug-trace accounting</td>
<td>1125</td>
</tr>
<tr>
<td>configure debug-trace bootprelay</td>
<td>1127</td>
</tr>
<tr>
<td>configure debug-trace card-state-change</td>
<td>1128</td>
</tr>
<tr>
<td>configure debug-trace debug-link</td>
<td>1129</td>
</tr>
<tr>
<td>configure debug-trace dvmrp-cache</td>
<td>1130</td>
</tr>
<tr>
<td>configure debug-trace dvmrp-hello</td>
<td>1132</td>
</tr>
<tr>
<td>configure debug-trace dvmrp-message</td>
<td>1134</td>
</tr>
<tr>
<td>configure debug-trace dvmrp-neighbor</td>
<td>1136</td>
</tr>
<tr>
<td>configure debug-trace dvmrp-route</td>
<td>1138</td>
</tr>
<tr>
<td>configure debug-trace dvmrp-timer</td>
<td>1140</td>
</tr>
<tr>
<td>configure debug-trace eaps-system</td>
<td>1141</td>
</tr>
<tr>
<td>configure debug-trace flow-redirect</td>
<td>1143</td>
</tr>
<tr>
<td>configure debug-trace flowstats</td>
<td>1145</td>
</tr>
<tr>
<td>configure debug-trace health-check</td>
<td>1146</td>
</tr>
<tr>
<td>configure debug-trace iparp</td>
<td>1149</td>
</tr>
<tr>
<td>configure debug-trace ixpgns-message</td>
<td>1151</td>
</tr>
<tr>
<td>configure debug-trace ixrip-message</td>
<td>1153</td>
</tr>
<tr>
<td>configure debug-trace ixrip-route</td>
<td>1155</td>
</tr>
<tr>
<td>configure debug-trace ixssap-entry</td>
<td>1156</td>
</tr>
<tr>
<td>configure debug-trace ixssap-message</td>
<td>1157</td>
</tr>
<tr>
<td>configure debug-trace isis-cli</td>
<td>1159</td>
</tr>
<tr>
<td>configure debug-trace isis-event</td>
<td>1160</td>
</tr>
<tr>
<td>configure debug-trace isis-hello</td>
<td>1161</td>
</tr>
<tr>
<td>configure debug-trace isis-lsp</td>
<td>1162</td>
</tr>
<tr>
<td>configure debug-trace isis-spf</td>
<td>1163</td>
</tr>
<tr>
<td>configure debug-trace isis-spf</td>
<td>1164</td>
</tr>
<tr>
<td>configure debug-trace mpls</td>
<td>1165</td>
</tr>
<tr>
<td>configure debug-trace mpls-signalling</td>
<td>1168</td>
</tr>
<tr>
<td>configure debug-trace mpls-signalling</td>
<td>1168</td>
</tr>
<tr>
<td>configure debug-trace mpls-npcard</td>
<td>1170</td>
</tr>
<tr>
<td>configure debug-trace pim-cache</td>
<td>1171</td>
</tr>
<tr>
<td>configure debug-trace pim-hello</td>
<td>1173</td>
</tr>
<tr>
<td>configure debug-trace pim-message</td>
<td>1175</td>
</tr>
<tr>
<td>configure debug-trace pim-neighbor</td>
<td>1177</td>
</tr>
<tr>
<td>configure debug-trace pim-rp-mgmt</td>
<td>1179</td>
</tr>
<tr>
<td>configure debug-trace rip-message</td>
<td>1181</td>
</tr>
<tr>
<td>configure debug-trace rip-route-change</td>
<td>1182</td>
</tr>
<tr>
<td>configure debug-trace rip-triggered-update</td>
<td>1183</td>
</tr>
<tr>
<td>configure debug-trace slb-3dns</td>
<td>1184</td>
</tr>
<tr>
<td>configure debug-trace slb-connection</td>
<td>1185</td>
</tr>
<tr>
<td>configure debug-trace slb-failover</td>
<td>1186</td>
</tr>
<tr>
<td>configure debug-trace stacking</td>
<td>1187</td>
</tr>
<tr>
<td>configure debug-trace transceiver-test</td>
<td>1189</td>
</tr>
<tr>
<td>configure debug-trace udp-forwarding</td>
<td>1191</td>
</tr>
<tr>
<td>configure debug-trace vrrp</td>
<td>1192</td>
</tr>
<tr>
<td>configure debug-trace vrrp-hello</td>
<td>1193</td>
</tr>
<tr>
<td>configure debug-trace wireless</td>
<td>1195</td>
</tr>
<tr>
<td>configure diagnostics</td>
<td>1197</td>
</tr>
</tbody>
</table>
configure diagnostics cable 2234
configure diffserv dscp-mapping ports 2117
configure diffserv examination code-point qosprofile ports 432
configure diffserv ingress replacement ports 2236
configure diffserv replacement priority code-point ports 434
configure dns-client add 83
configure dns-client add domain-suffix 84
configure dns-client add name-server 85
configure dns-client default-domain 86
configure dns-client delete 87
configure dns-client delete domain-suffix 88
configure dns-client delete name-server 89
configure dot1p type 436
configure dot1q ethertype 360
configure dot1q tagmapping ports 2119
configure download server 1093
configure dvmrp add vlan 1938
configure dvmrp delete vlan 1939
configure dvmrp timer 1940
configure dvmrp vlan cost 1941
configure dvmrp vlan export-filter 1942
configure dvmrp vlan import-filter 1943
configure dvmrp vlan timer 1944
configure dvmrp vlan trusted-gateway 1945
configure eaps add control vlan 1404
configure eaps add protect vlan 1405
configure eaps delete control vlan 1406
configure eaps delete protect vlan 1407
configure eaps failtime 1408
configure eaps failtime expiry-action 1409
configure eaps fast-convergence 1411
configure eaps hellotime 1412
configure eaps mode 1413
configure eaps name 1414
configure eaps port 1415
configure eaps shared-port domain 1416
configure eaps shared-port mode 1417
configure elrp-client one-shot 1493
configure elrp-client periodic 1495
configure elsm hellotime 1497
configure elsm hold-threshold 1499
configure enhanced-dos-protect ipfdb agingtime 856
configure enhanced-dos-protect ipfdb cache-size 857
configure enhanced-dos-protect ipfdb learn-limit 858
configure enhanced-dos-protect ipfdb learn-window 859
count Configure enhanced-dos-protect ports 860
configure enhanced-dos-protect rate-limit 861
configure esrp port-mode ports 1503
configure ext-mcast loopback-port 1946
configure fdb agingtime 406
configure fdb-scan failure-action 407
configure fdb-scan period 409
configure flow-redirect add next-hop 494
configure flow-redirect delete next-hop 495
configure flow-redirect service-check ftp 496
configure flow-redirect service-check http 497
configure flow-redirect service-check 14-port 498
configure flow-redirect service-check nntp 499
configure flow-redirect service-check ping 500
configure flow-redirect service-check pop3 501
configure flow-redirect service-check smtp 502
configure flow-redirect service-check telnet 503
configure flow-redirect timer ping-check 504
configure flow-redirect timer service-check 505
configure flow-redirect timer tcp-port-check 506
configure flowstats export 2123
configure flowstats export add port 666
configure flowstats export delete 2125
configure flowstats export delete port 668
configure flowstats filter ports 669, 2127
configure flowstats source 671
configure flowstats source ipaddress 2129
configure flowstats timeout ports 672
configure gvrp port 361
configure idletimeouts 90
configure igmp 1947
configure igmp snooping add static group 1948
configure igmp snooping add static router 1950
configure igmp snooping delete static group 1951
configure igmp snooping delete static router 1952
configure igmp snooping filter 1953
configure igmp snooping flood-list 1954
configure igmp snooping leave-timeout 1956
configure igmp snooping timer 1957
configure inline-power backup-source 2279
configure inline-power backup-source 2279
configure inline-power budget 2280
configure inline-power detection 2281
configure inline-power disconnect-precedence 2282
configure inline-power display-string 2283
configure inline-power display-string 2283
configure inline-power label 2283
configure inline-power label 2283
configure inline-power operator-limit 2285
configure inline-power power-supply 2287
configure inline-power priority 2288
configure inline-power reserved budget 2289
configure inline-power type 2290
configure inline-power usage-threshold 2292
configure inline-power violation-precedence 2293
configure iparp add 1597
configure iparp add proxy 1598
configure iparp delete 1600
configure iparp delete proxy 1601
configure iparp max-entries 1602
configure iparp max-pending-entries 1603
configure iparp timeout 1604
configure ip-down-vlan-action 1596
configure ipfdb route-add 1605
configure ip-mtu vlan 253
configure iproute add 1606
configure iproute add blackhole 1607
configure iproute add blackhole default 1608
configure iproute add default 1609
configure iproute delete 1610
configure iproute delete blackhole 1611
configure iproute delete blackhole default 1612
configure iproute delete default 1613
configure iproute priority 1614
configure iproute route-map 1616
configure ip-subnet-lookup maskbits 863
configure ipxmaxhops 2024
configure ipxrip add vlan 2025
configure ipxrip delete vlan 2026
configure ipxrip vlan delay 2027
configure ipxrip vlan export-filter 2028
configure ipxrip vlan import-filter 2029
configure ipxrip vlan max-packet-size 2030
configure ipxrip vlan trusted-gateway 2031
configure ipxrip vlan update-interval 2032
configure ipxroute add 2033
configure ipxroute delete 2034
configure ipxsap add vlan 2035
configure ipxsap delete vlan 2036
configure ipxsap vlan delay 2037
configure ipxsap vlan export-filter 2038
configure ipxsap vlan gns-delay 2043
configure ipxsap vlan import-filter 2039
configure ipxsap vlan max-packet-size 2040
configure ipxsap vlan trusted-gateway 2041
configure ipxsap vlan update-interval 2042
configure ipxservice add 2045
configure ipxservice delete 2045
configure irdp 1619
configure irpd 1619
configure irpp 1619
configure isis add area-address 1709, 1715
configure isis add vlan 1710
configure isis add domain-summary 1711
configure isis add delete domain-summary 1712
configure isis add domain-filter 1713
configure isis authentication 1714
configure isis delete vlan 1716
configure isis external-filter 1717
configure isis holddown interval 1718
configure isis lsp lifetime 1719
configure isis lsp refresh interval 1720
configure isis metric-size 1721
configure isis spf-hold-time 1722
configure isis system-identifier 1723
configure isis vlan authentication 1725
configure isis vlan cost 1726
configure isis vlan hello-multiplier 1727
configure isis vlan non-passive 1724
configure isis vlan passive 1724
configure isis vlan priority 1728
configure isis vlan timer 1729
configure jumbo-frame size 255
configure lldp port management-address 2338
configure lldp port description 2339
configure lldp port system-capabilities 2340
configure lldp port system-description 2341
configure lldp port system-name 2342
configure lldp port vendor-specific dot1 port-vlan-ID 2344
configure lldp port vendor-specific dot1 protocol-identity 2345
configure lldp port vendor-specific dot1 vlan-name 2346
configure lldp port vendor-specific dot3 link-aggregation 2347
configure lldp port vendor-specific dot3 mac-phy 2348
configure lldp port vendor-specific dot3 max-framesize 2349
configure lldp port vendor-specific dot3 power-via-mdi 2350
configure lldp ports vendor-specific dot1 port-protocol-vlan-ID 2343
configure lldp reinitialize-delay 2351
configure lldp snmp-notification-interval 2352
configure lldp transmit-delay 2353
configure lldp transmit-hold 2354
configure lldp transmit-interval 2355
configure log display 673
configure log filter events 675
configure log filter set severity 682
configure log filter set severity match 684
configure log target filter 686
configure log target format 688
configure log target match 692
configure log target severity 694
configure mac-lockdown-timeout ports 864
configure mac-vlan add mac-address 363
configure mac-vlan delete 365
configure mcast-queue-mgmt 1959
configure mirroring add 257
configure mirroring delete 259
configure mpls 2426
configure mpls add vlan 2433
configure mpls add vpls 2375, 2428
configure mpls delete tls-tunnel 2436
configure mpls delete vlan 2437
configure mpls delete vpls 2377, 2387, 2435, 2438
configure mpls health-check add mpls-ping 2388, 2441
configure mpls health-check add vplsping 2391, 2444
configure mpls health-check delete mpls-ping 2390, 2443
configure mpls health-check delete vpls-ping 2394, 2446, 2447
configure mpls ldp acl 2379, 2448
configure mpls ldp acl add 2380, 2449
configure mpls ldp acl delete peer 2381, 2450
configure mpls ldp advertise 2451
configure mpls ldp advertise vlan 2453
configure mpls php 2454
configure mpls propagate-ip-ttl 2455
configure mpls qos-mapping 2457
configure mpls rsvp-te add ero 2471
configure mpls rsvp-te add lsp 2459
configure mpls rsvp-te add path 2460
configure mpls rsvp-te add profile 2395
configure mpls rsvp-te delete ero 2473
configure mpls rsvp-te delete lsp 2465
configure mpls rsvp-te delete path 2466, 2470
configure mpls rsvp-te delete profile 2467
configure mpls rsvp-te lsp add path 2468
configure mpls rsvp-te profile 2396, 2474
configure mpls slot edge-service-mode 2378, 2439
configure mpls tls-tunnel lsp 2397, 2478
configure mpls vlan ip-mtu 2479
configure mpls vlan ldp propagate 2481
configure mpls vpls 2398, 2400, 2485
configure mpls vpls add 2382, 2487
configure mpls vpls add peer 2384, 2489
configure mpls vpls counters 2374
configure mpls vpls delete peer 2402, 2405, 2406, 2492, 2493
configure mpls vpls peer 2407, 2494
configure mroute 1961
configure mroute add 1960
configure msm-failover ersp-failover-mode 1505
configure msm-failover link-action 261
configure msm-failover slave-config 263
configure msm-failover slave-timeout 264
configure multilink add 2176
configure multilink delete 2177
configure nat add vlan map 473
configure nat delete 477
configure nat finst-timeout 479
configure nat icmp-timeout 480
configure nat syn-timeout 481
configure nat tcp-timeout 482
configure nat timeout 483
configure nat udp-timeout 484
configure nat vlan 485
configure netlogin base-url 865
configure netlogin mac-addr auth-retry-count 867
configure netlogin mac-addr reauth-period 868
configure netlogin mac-address 866
configure netlogin redirect-page 869
configure ospf add virtual-link 1731
configure ospf add vlan area 1732
configure ospf add vlan area link-type 1734
configure ospf area add range 1735
configure ospf area delete range 1736
configure ospf area external-filter 1737
configure ospf area interarea-filter 1738
configure ospf area normal 1739
configure ospf area nssa stub-default-cost 1740
configure ospf area stub stub-default-cost 1741
configure ospf asbr-filter 1742
configure ospf as-limint 1743
configure ospf ase-summary add cost 1744
configure ospf ase-summary delete 1745
configure ospf authentication 1758
configure ospf cost 1746
configure ospf delete virtual-link 1747
configure ospf delete vlan 1748
configure ospf direct-filter 1749
configure ospf is-a-lsa-batching-timer 1750
configure ospf metric-table 1751
configure ospf priority 1752
configure ospf routerid 1753
configure ospf spf-hold-time 1755
configure ospf timer 1756
configure ospf vlan area 1759
configure ospf vlan neighbor add 1760
configure ospf vlan neighbor delete 1761
configure ospf vlan timer 1762
configure packet-mem-scan-recovery-mode 696
configure pim add vlan 1962
configure pim cbr 1964
configure pim crp static 1932, 1965
configure pim crp timer 1966
configure pim crp vlan access-policy 1967
configure pim delete vlan 1968
configure pim register-checksum-to 1969
configure pim register-rate-limit-interval 1970
configure pim register-suppress-interval register-probe-interval 1971
configure pim spt-threshold 1972
configure pim timer vlan 1973
configure pim vlan trusted-gateway 1974
configure port aggregate-bandwidth percent 265
configure ports 267
configure ports auto off 271
configure ports auto on 273
configure ports auto-polarity 270
configure ports clock source 2178
configure ports display-string 275
configure ports e1 clock source 2178
configure ports e1 framing 2179
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure ports e1 receivergain</td>
<td>2180</td>
</tr>
<tr>
<td>configure ports e1 timeslots</td>
<td>2181</td>
</tr>
<tr>
<td>configure ports egress-rate-limit</td>
<td>2238</td>
</tr>
<tr>
<td>configure ports interpacket-gap</td>
<td>266</td>
</tr>
<tr>
<td>configure ports link-detection-level</td>
<td>277</td>
</tr>
<tr>
<td>configure ports monitor vlan</td>
<td>366</td>
</tr>
<tr>
<td>configure ports preferred-medium</td>
<td>278</td>
</tr>
<tr>
<td>configure ports qosprofile</td>
<td>438</td>
</tr>
<tr>
<td>configure ports redundant</td>
<td>280</td>
</tr>
<tr>
<td>configure ports snmp alert</td>
<td>2182</td>
</tr>
<tr>
<td>configure ports t1 cablelength</td>
<td>2183</td>
</tr>
<tr>
<td>configure ports t1 clock source</td>
<td>2178</td>
</tr>
<tr>
<td>configure ports t1 fdl</td>
<td>2184</td>
</tr>
<tr>
<td>configure ports t1 framing</td>
<td>2185</td>
</tr>
<tr>
<td>configure ports t1 ldetect</td>
<td>2186</td>
</tr>
<tr>
<td>configure ports t1 linecoding</td>
<td>2187</td>
</tr>
<tr>
<td>configure ports t1 yellow</td>
<td>2188</td>
</tr>
<tr>
<td>configure ports t3 cablelength</td>
<td>2189</td>
</tr>
<tr>
<td>configure ports t3 clock source</td>
<td>2178</td>
</tr>
<tr>
<td>configure ports t3 framing</td>
<td>2190</td>
</tr>
<tr>
<td>configure ports tunnel hdlc</td>
<td>2130</td>
</tr>
<tr>
<td>configure ports vdsl</td>
<td>282</td>
</tr>
<tr>
<td>configure ppp</td>
<td>2191</td>
</tr>
<tr>
<td>configure ppp authentication</td>
<td>2193</td>
</tr>
<tr>
<td>configure ppp authentication multilink</td>
<td>2193</td>
</tr>
<tr>
<td>configure ppp authentication ports</td>
<td>2133, 2193</td>
</tr>
<tr>
<td>configure ppp delayed-down-time ports</td>
<td>2134</td>
</tr>
<tr>
<td>configure ppp echo ports</td>
<td>2135</td>
</tr>
<tr>
<td>configure ppp ports</td>
<td>2131</td>
</tr>
<tr>
<td>configure ppp pos checksum ports</td>
<td>2136</td>
</tr>
<tr>
<td>configure ppp pos scrambling ports</td>
<td>2137</td>
</tr>
<tr>
<td>configure ppp quality ports</td>
<td>2138</td>
</tr>
<tr>
<td>configure ppp user</td>
<td>2194</td>
</tr>
<tr>
<td>configure ppp user multilink</td>
<td>2194</td>
</tr>
<tr>
<td>configure ppp user ports</td>
<td>2139, 2194</td>
</tr>
<tr>
<td>configure protocol add</td>
<td>367</td>
</tr>
<tr>
<td>configure protocol delete</td>
<td>369</td>
</tr>
<tr>
<td>configure qosprofile</td>
<td>439, 2140, 2195</td>
</tr>
<tr>
<td>configure qosprofile ingress</td>
<td>2239</td>
</tr>
<tr>
<td>configure qosprofile min-bps</td>
<td>2195</td>
</tr>
<tr>
<td>configure qosprofile wanqos maxbuf</td>
<td>2197</td>
</tr>
<tr>
<td>configure qostype ingress priority</td>
<td>2241</td>
</tr>
<tr>
<td>configure qostype priority</td>
<td>441</td>
</tr>
<tr>
<td>configure radius server</td>
<td>870</td>
</tr>
<tr>
<td>configure radius shared-secret</td>
<td>872</td>
</tr>
<tr>
<td>configure radius timeout</td>
<td>873</td>
</tr>
<tr>
<td>configure radius-accounting server</td>
<td>875</td>
</tr>
<tr>
<td>configure radius-accounting shared-secret</td>
<td>876</td>
</tr>
<tr>
<td>configure radius-accounting timeout</td>
<td>877</td>
</tr>
<tr>
<td>configure reboot-loop-protection</td>
<td>1199</td>
</tr>
<tr>
<td>configure red</td>
<td>2142</td>
</tr>
<tr>
<td>configure red drop-probability</td>
<td>443</td>
</tr>
<tr>
<td>configure red min-threshold ports</td>
<td>2144</td>
</tr>
<tr>
<td>configure rf-preamble</td>
<td>1259</td>
</tr>
<tr>
<td>configure rf-profile beacon-interval</td>
<td>1255</td>
</tr>
<tr>
<td>configure rf-profile dtim-interval</td>
<td>1256</td>
</tr>
<tr>
<td>configure rf-profile frag-length</td>
<td>1257</td>
</tr>
<tr>
<td>configure rf-profile long-retry</td>
<td>1258</td>
</tr>
<tr>
<td>configure rf-profile rts-retry</td>
<td>1260</td>
</tr>
<tr>
<td>configure rf-profile short-retry</td>
<td>1261</td>
</tr>
<tr>
<td>configure rip add vlan</td>
<td>1764</td>
</tr>
<tr>
<td>configure rip delete vlan</td>
<td>1765</td>
</tr>
<tr>
<td>configure rip garbagetime</td>
<td>1766</td>
</tr>
<tr>
<td>configure rip routetimeout</td>
<td>1767</td>
</tr>
<tr>
<td>configure rip rxmode</td>
<td>1768</td>
</tr>
<tr>
<td>configure rip txmode</td>
<td>1769</td>
</tr>
<tr>
<td>configure rip updatetime</td>
<td>1770</td>
</tr>
<tr>
<td>configure rip vlan cost</td>
<td>1771</td>
</tr>
<tr>
<td>configure rip vlan export-filter</td>
<td>1772</td>
</tr>
<tr>
<td>configure rip vlan import-filter</td>
<td>1773</td>
</tr>
<tr>
<td>configure rip vlan trusted-gateway</td>
<td>1774</td>
</tr>
<tr>
<td>configure route-map add</td>
<td>878</td>
</tr>
<tr>
<td>configure route-map add goto</td>
<td>880</td>
</tr>
<tr>
<td>configure route-map add match</td>
<td>881</td>
</tr>
<tr>
<td>configure route-map add set</td>
<td>883</td>
</tr>
<tr>
<td>configure route-map delete gto</td>
<td>885</td>
</tr>
<tr>
<td>configure route-map delete match</td>
<td>887</td>
</tr>
<tr>
<td>configure route-map delete set</td>
<td>889</td>
</tr>
<tr>
<td>configure route-map set accounting-index</td>
<td>2070</td>
</tr>
<tr>
<td>configure route-map set iphost-routing</td>
<td>2072</td>
</tr>
<tr>
<td>configure route-map set lpm-routing</td>
<td>2073</td>
</tr>
<tr>
<td>configure security-profile default-user-vlan</td>
<td>891</td>
</tr>
<tr>
<td>configure security-profile dot11-auth network-auth encryption</td>
<td>892</td>
</tr>
<tr>
<td>configure security-profile dot1x-wpa-timers group-update-timer</td>
<td>895</td>
</tr>
<tr>
<td>configure security-profile dot1x-wpa-timers pairwise-update-timer</td>
<td>896</td>
</tr>
<tr>
<td>configure security-profile dot1x-wpa-timers reauth-period</td>
<td>897</td>
</tr>
<tr>
<td>configure security-profile ess-name</td>
<td>898</td>
</tr>
<tr>
<td>configure security-profile ssid-in-beacon</td>
<td>899</td>
</tr>
<tr>
<td>configure security-profile use-dynamic-vlan</td>
<td>900</td>
</tr>
<tr>
<td>configure security-profile wep default-key-index</td>
<td>902</td>
</tr>
<tr>
<td>configure security-profile wep key add</td>
<td>902</td>
</tr>
<tr>
<td>configure security-profile wep key add hex plaintext</td>
<td>903</td>
</tr>
<tr>
<td>configure security-profile wep key delete</td>
<td>904</td>
</tr>
<tr>
<td>configure security-profile wpa2-psk</td>
<td>906</td>
</tr>
<tr>
<td>configure security-profile wpa-only</td>
<td>907</td>
</tr>
<tr>
<td>configure security-profile wpa-psk</td>
<td>905</td>
</tr>
<tr>
<td>configure sflow agent</td>
<td>698</td>
</tr>
<tr>
<td>configure sflow backoff-threshold</td>
<td>699</td>
</tr>
<tr>
<td>configure sflow collector</td>
<td>701</td>
</tr>
<tr>
<td>configure sflow poll-interval</td>
<td>703</td>
</tr>
<tr>
<td>configure sflow sample-rate</td>
<td>704</td>
</tr>
<tr>
<td>configure sharing address-based</td>
<td>283</td>
</tr>
</tbody>
</table>
configure slb esrp 507
configure slb failover alive-frequency 508
configure slb failover dead-frequency 509
configure slb failover failback now 510
configure slb failover ping-check 511
configure slb failover unit 512
configure slb global connection-block 513
configure slb global connection-timeout 514
configure slb global ftp 515
configure slb global http 516
configure slb global nntp 518
configure slb global persistence-level 519
configure slb global persistence-method 520
configure slb global ping-check 521
configure slb global pop3 522
configure slb global service-check 523
configure slb global smtp 524
configure slb global synguard 525
configure slb global tcp-port-check 526
configure slb global telnet 527
configure slb gogo-mode health-check 528
configure slb gogo-mode ping-check 529
configure slb gogo-mode service-check ftp 531
configure slb gogo-mode service-check http 532
configure slb gogo-mode service-check pop3 534
configure slb gogo-mode service-check smtp 535
configure slb gogo-mode service-check telnet 536
configure slb gogo-mode service-check timer 537
configure slb gogo-mode tcp-port-check add 539
configure slb gogo-mode tcp-port-check delete 541
configure slb gogo-mode tcp-port-check timer 543
configure slb L4-port 545
configure slb node max-connections 547
configure slb node ping-check 549
configure slb node tcp-port-check 550
configure slb pool add 552
configure slb pool delete 554
configure slb pool lb-method 556
configure slb pool member 557
configure slb proxy-client-persistence 559
configure slb vip 560
configure slb vip client-persistence-timeout 561
configure slb vip max-connections 562
configure slb vip service-check frequency 563
configure slb vip service-check ftp 564
configure slb vip service-check http 565
configure slb vip service-check nntp 567
configure slb vip service-check pop3 568
configure slb vip service-check smtp 569
configure slb vip service-check telnet 570
configure slot module 285
configure snmp access-profile readonly 123
configure snmp access-profile readwrite 125
configure snmp add community 127
configure snmp add trapreceiver 129
configure snmp community 133
configure snmp delete community 135
configure snmp delete trapreceiver 137
configure snmp syscontact 139
configure snmp sysloglocation 140
configure snmp sysname 141
configure snmpv3 add access 142
configure snmpv3 add community 144
configure snmpv3 add filter 146
configure snmpv3 add filter-profile 148
configure snmpv3 add group user 149
configure snmpv3 add mib-view 151
configure snmpv3 add notify 153
configure snmpv3 add target-addr 154
configure snmpv3 add target-params 156
configure snmpv3 add user 158
configure snmpv3 add user clone-from 160
configure snmpv3 delete access 161
configure snmpv3 delete community 163
configure snmpv3 delete filter 164
configure snmpv3 delete filter-profile 165
configure snmpv3 delete group user 166
configure snmpv3 delete mib-view 168
configure snmpv3 delete notify 170
configure snmpv3 delete target-addr 171
configure snmpv3 delete target-params 172
configure snmpv3 delete user 173
configure snmpv3 engine-boots 174
configure snmpv3 engine-id 175
configure snmpv3 extreme-target-addr-ext 176
configure snntp-client server 178
configure snntp-client update-interval 179
configure sonet clocking ports 2145
configure sonet framing ports 2146
configure sonet loop 2147
configure sonet signal label ports 2148
configure sonet threshold signal degrade ports 2149
configure sonet threshold signal fail ports 2150
configure sonet trace path ports 2151
configure sonet trace section ports 2152
configure ssh2 908
configure ssl certificate pregenerated 910
configure ssl certificate privkeylen country organization common-name 911
configure ssl privkey pregenerated 913
configure stacking fallback-ip-address 1389
configure stacking priority 1391
configure stacking requested-slot 1392
configure stacking slot-binding module 1393
configure stpd add vlan 1439
configure stpd delete vlan 1441
configure stpd forwarddelay 1442
configure stpd hellotime 1443
configure stpd maxage 1444
configure stpd mode 1445
configure stpd port link-type 1448
configure stpd ports cost 1446
configure stpd ports link-type edge edge-safeguard disable 1450
configure stpd ports link-type edge edge-safeguard enable 1451
configure stpd mode 1452
configure stpd priority 1453
configure stpd priority 1455
configure stpd tag 1456
configure switch 1094
configure sys-health-check alarm-level 705
configure sys-health-check auto-recovery 708
configure sys-health-check scan-recovery 711
configure syslog add 715
configure syslog delete 717
configure sys-recovery-level 713
configure system-dump server 1200
configure system-dump timeout 1201
configure tacacs server 914
configure tacacs server timeout 916
configure tacacs shared-secret 917
configure tacacs timeout 918
configure tacacs-accounting server 919
configure tacacs-accounting shared-secret 920
configure tacacs-accounting timeout 921
configure time 91
configure timezone 92
configure transceiver-test failure-action 718
configure transceiver-test period 720
configure transceiver-test threshold 721
configure transceiver-test window 722
configure udp-profile add 1620
configure udp-profile delete 1621
configure vlan access-profile 922
configure vlan add domain-member vlan 1506
configure vlan add elrp-poll ports 1507, 1519
configure vlan add member-vlan 370
configure vlan add multilink 2198
configure vlan add ports 371
configure vlan add ports loopback-vid 373
configure vlan add ports no-restart 1508
configure vlan add ports restart 1509
configure vlan add ports stpd 1457
configure vlan add secondary-ip 375
configure vlan add track-bgp 1510
configure vlan add track-diagnostic 1511
configure vlan add track-environment 1512
configure vlan add track-iproute 1513
configure vlan add track-lsp 2482
configure vlan add track-ospf 1514
configure vlan add track-ping 1515
configure vlan add track-rip 1516
configure vlan add track-vlan 1517
configure vlan delete domain-member vlan 1518
configure vlan delete member-vlan 377
configure vlan delete multilink 2199
configure vlan delete port 378
configure vlan delete secondary-ip 379
configure vlan delete track-bgp 1520
configure vlan delete track-diagnostic 1521
configure vlan delete track-environment 1522
configure vlan delete track-iproute 1523
configure vlan delete track-lsp 2484
configure vlan delete track-ospf 1524
configure vlan delete track-ping 1525
configure vlan delete track-rip 1526
configure vlan delete track-vlan 1527
configure vlan dhcp-address-range 924
configure vlan dhcp-lease-timer 926
configure vlan dhcp-options 927
configure vlan esrp elrp-master-poll disable 1528
configure vlan esrp elrp-master-poll enable 1529
configure vlan esrp elrp-premaster-poll disable 1531
configure vlan esrp elrp-premaster-poll enable 1532
configure vlan esrp election 1534
configure vlan esrp esrp-neutral-timeout 1536
configure vlan esrp esrp-premaster-timeout 1536
configure vlan esrp group 1537
configure vlan esrp group add esrp-aware-ports 1538
configure vlan esrp group delete esrp-aware-ports 1540
configure vlan esrp priority 1541
configure vlan esrp timer 1542
configure vlan ipaddress 380
configure vlan name 381
configure vlan netlogin-lease-timer 930
configure vlan priority 444
configure vlan protocol 382
configure vlan qosprofile 445
configure vlan qosprofile ingress 2243
configure vlan secondary-ip 1622
configure vlan slb-type 571
configure vlan subvlan 1624
configure vlan subvlan-address-range 1625
configure vlan tag 383
configure vlan udp-profile 1626
configure vlan xnetid 2046
configure vrrp add vlan 1571
configure vrrp delete 1572
configure vrrp add vlan 1571
configure vrrp add vrid 1575
configure vrrp add vrid 1576
configure wanqos egress map dot1p_priority 2200
configure web login-timeout 180
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure wireless bind</td>
<td>2086</td>
</tr>
<tr>
<td>configure wireless country-code</td>
<td>1262</td>
</tr>
<tr>
<td>configure wireless default-gateway</td>
<td>1264</td>
</tr>
<tr>
<td>configure wireless device-db</td>
<td>2087</td>
</tr>
<tr>
<td>configure wireless management-vlan</td>
<td>1265</td>
</tr>
<tr>
<td>configure wireless port antenna-profile</td>
<td>1266</td>
</tr>
<tr>
<td>configure wireless port bind</td>
<td>2088</td>
</tr>
<tr>
<td>configure wireless port interface ap-scan added-trap</td>
<td>1271</td>
</tr>
<tr>
<td>configure wireless ports antenna-location</td>
<td>1267</td>
</tr>
<tr>
<td>configure wireless ports detected-station-timeout</td>
<td>1268</td>
</tr>
<tr>
<td>configure wireless ports force-disassociation</td>
<td>1269</td>
</tr>
<tr>
<td>configure wireless ports health-check</td>
<td>1270</td>
</tr>
<tr>
<td>configure wireless ports image</td>
<td>1096</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan off-channel continuous</td>
<td>1273</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan off-channel max-wait</td>
<td>1274</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan off-channel min-wait</td>
<td>1275</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan probe-interval</td>
<td>1276</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan removed-trap</td>
<td>1277</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan results size</td>
<td>1278</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan results timeout</td>
<td>1279</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan send-probe</td>
<td>1280</td>
</tr>
<tr>
<td>configure wireless ports interface ap-scan updated-trap</td>
<td>1281</td>
</tr>
<tr>
<td>configure wireless ports interface channel</td>
<td>1282</td>
</tr>
<tr>
<td>configure wireless ports interface client-history size</td>
<td>1284</td>
</tr>
<tr>
<td>configure wireless ports interface client-history timeout</td>
<td>1285</td>
</tr>
<tr>
<td>configure wireless ports interface client-scan added-trap</td>
<td>1286</td>
</tr>
<tr>
<td>configure wireless ports interface client-scan removed-trap</td>
<td>1287</td>
</tr>
<tr>
<td>configure wireless ports interface client-scan results size</td>
<td>1288</td>
</tr>
<tr>
<td>configure wireless ports interface client-scan results timeout</td>
<td>1289</td>
</tr>
<tr>
<td>configure wireless ports interface max-clients</td>
<td>1290</td>
</tr>
<tr>
<td>configure wireless ports interface rf-profile</td>
<td>1291</td>
</tr>
<tr>
<td>configure wireless ports interface security-profile</td>
<td>1292</td>
</tr>
<tr>
<td>configure wireless ports interface transmit-power</td>
<td>1293</td>
</tr>
<tr>
<td>configure wireless ports interface transmit-rate</td>
<td>1294</td>
</tr>
<tr>
<td>configure wireless ports interface wireless-bridging</td>
<td>1295</td>
</tr>
<tr>
<td>configure wireless ports ipaddress</td>
<td>1296</td>
</tr>
<tr>
<td>configure wireless ports location</td>
<td>1297</td>
</tr>
<tr>
<td>configure wireless redirect-db</td>
<td>2089</td>
</tr>
<tr>
<td>create access-list</td>
<td>931</td>
</tr>
<tr>
<td>create access-list icmp destination source</td>
<td>933</td>
</tr>
<tr>
<td>create access-list ip destination source ports</td>
<td>935</td>
</tr>
<tr>
<td>create access-list tcp destination source ports</td>
<td>937</td>
</tr>
<tr>
<td>create access-list udp destination source ports</td>
<td>939</td>
</tr>
<tr>
<td>create access-mask</td>
<td>941</td>
</tr>
<tr>
<td>create access-profile type</td>
<td>943</td>
</tr>
<tr>
<td>create account</td>
<td>96</td>
</tr>
<tr>
<td>create account pppuser</td>
<td>2153, 2201</td>
</tr>
<tr>
<td>create antenna-profile</td>
<td>1298</td>
</tr>
<tr>
<td>create application examination</td>
<td>2244</td>
</tr>
<tr>
<td>create aps</td>
<td>2154</td>
</tr>
<tr>
<td>create bgp neighbor peer-group</td>
<td>1898</td>
</tr>
<tr>
<td>create bgp neighbor remote-AS-number</td>
<td>1899</td>
</tr>
<tr>
<td>create bgp peer-group</td>
<td>1900</td>
</tr>
<tr>
<td>create eaps</td>
<td>1418</td>
</tr>
<tr>
<td>create eaps shared-port</td>
<td>1419</td>
</tr>
<tr>
<td>create fdbentry secure-mac</td>
<td>410</td>
</tr>
<tr>
<td>create fdbentry vlan blackhole</td>
<td>411</td>
</tr>
<tr>
<td>create fdbentry vlan dynamic</td>
<td>413</td>
</tr>
<tr>
<td>create fdbentry vlan ports</td>
<td>415</td>
</tr>
<tr>
<td>create flow-redirect</td>
<td>572</td>
</tr>
<tr>
<td>create isis area</td>
<td>1775</td>
</tr>
<tr>
<td>create log filter</td>
<td>723</td>
</tr>
<tr>
<td>create multilink</td>
<td>2202</td>
</tr>
<tr>
<td>create ospf area</td>
<td>1776</td>
</tr>
<tr>
<td>create protocol</td>
<td>384</td>
</tr>
<tr>
<td>create rate-limit</td>
<td>945</td>
</tr>
<tr>
<td>create rf-profile copy</td>
<td>1299</td>
</tr>
<tr>
<td>create rf-profile mode</td>
<td>1300</td>
</tr>
<tr>
<td>create route-map</td>
<td>947</td>
</tr>
<tr>
<td>create security-profile</td>
<td>948</td>
</tr>
<tr>
<td>create slb pool</td>
<td>574</td>
</tr>
<tr>
<td>create slb vip</td>
<td>575</td>
</tr>
<tr>
<td>create stpd</td>
<td>1459</td>
</tr>
<tr>
<td>create trusted-mac-address</td>
<td>949</td>
</tr>
<tr>
<td>create upd-profile</td>
<td>1627</td>
</tr>
<tr>
<td>create vlan</td>
<td>385</td>
</tr>
</tbody>
</table>

**D**
- delete access-list | 951
- delete access-mask | 952
- delete access-profile | 953
- delete account | 98
- delete account pppuser | 2155, 2203
- delete antenna-profile | 1301
- delete application examination | 2246
- delete aps | 2156
- delete bgp neighbor | 1901
- delete bgp peer-group | 1902
- delete eaps | 1420
Index of Commands

delete eaps shared-port 1421
delete fdbentry 417
delete flow-redirect 576
delete isis area 1777
delete log filter 725
delete multilink 2204
delete ospf area 1778
delete protocol 387
delete rate-limit 954
delete rf-profile 1302
delete route-map 955
delete security-profile 956
delete slb pool 577
delete slb vip 578
delete stpd 1461
delete trusted-mac-address 957
delete udp-profile 1628
delete vlan 388
disable access-list 959
disable accounting 2074
disable alt-queue-management 181
disable application examination ports 2247
disable app-protection 2157
disable arp-learning 960
disable arp-learning ports 961
disable arp-learning vlan 962
disable arp-learning vlan ports 963
disable bgp 1903
disable bgp aggregation 1904
disable bgp always-compare-med 1905
disable bgp community format 1906
disable bgp export 1907
disable bgp neighbor 1909
disable bgp neighbor remove-private-AS-numbers 1910
disable bgp neighbor soft-in-reset 1911
disable bgp peer-group 1912
disable bgp peer-group remove-private-AS-numbers 1912
disable bgp synchronization 1913
disable bootp vlan 1629
disable bootprelay 1630
disable card-scan 288, 301
disable cli-config-logging 726
disable clipaging 100
disable cpu-dos-protect 964
disable dhcp ports vlan 182, 965
disable diagnostics cable 2248
disable diffserv examination ports 446
disable diffserv ingress replacement ports 2249
disable diffserv replacement ports 447
disable dlcs 448
disable dot1p replacement ports 449
disable dvmrp 1975
disable dvmrp rxmode vlan 1976
disable dvmrp txmode vlan 1977
disable eapol-flooding 183, 197, 214
disable eaps 1422
disable edp ports 289
disable elrp-client 1544
disable esrp vlan 1548
disable ext-mcast 1978
disable fdb vlan 418
disable flooding ports 291
disable flow-control ports 2250
disable flow-redirection 579
disable flowstats 727
disable flowstats filter ports 728
disable flowstats ping-check 730
disable flowstats ports 731
disable gyrp 389
disable icmp access-list 1631
disable icmp address-mask 1632
disable icmp parameter-problem 1633
disable icmp port-unreachables 1634
disable icmp redirects 1635
disable icmp time-exceeded 1636
disable icmp timestamp 1637
disable icmp unreachables 1638
disable icmp user redirects 1639
disable idle-timeouts 101
disable igmp 1979
disable igmp snooping 1980
disable igmp snooping with-proxy 1982
disable ignore-bpdu vlan 1462
disable ignore-stp vlan 1463
disable inline-power 2295
disable inline-power legacy 2296
disable inline-power ports 2298
disable inline-power slots 2300
disable iparp checking 1645
disable iparp refresh 1646
disable ipforwarding 1647
disable ipforwarding lpm-routing 1649, 2075
disable ipmforwarding 1983
disable ip-option loose-source-route 1640
disable ip-option record-route 1641
disable ip-option record-timestamp 1642
disable ip-option strict-source-route 1643
disable ip-option use-router-alert 1644
disable iproute sharing 1650
disable ip-subnet-lookup 967
disable ipxrip 2047
disable ipxsap 2048
disable ipxsap gns-reply 2049
Index of Commands

disable irdp 1651
disable isis 1779
disable isis export 1780
disable isis ignore-attached-bit 1782
disable isis originate-default 1783
disable isis overload 1784
disable jumbo-frame ports 292
disable lbdetect port 293
disable learning ports 294
disable lldp port 2356
disable log debug-mode 732, 1202
disable log display 733
disable log target 734
disable log temperature 742
disable loopback-mode vlan 1652
disable lpm 2076
disable mac-lockdown-timeout ports 968
disable mac-vlan port 390
disable mcast-queue-mgmt 1984
disable mirroring 295
disable mpls 2495
disable multilink 2205
disable multinetting 1653
disable nat 486
disable netlogin 969
disable netlogin logout-privilege 971
disable netlogin ports mac 973
disable netlogin ports vlan 972
disable netlogin session-refresh 974
disable ospf 1785
disable ospf capability opaque-lsa 1786
disable ospf export 1787
disable ospf originate-router-id 1789
disable peer-group 1912
disable pim 1985
disable pim snooping 1986
disable ports 296
disable ports e1 loopback 2206
disable ports loopback 2206
disable ports t1 loopback 2206
disable ports t3 loopback 2206
disable qosmonitor 450
disable radius 975
disable radius-accounting 976
disable red ports 451
disable red ports queue 2158
disable rip 1790
disable rip aggregation 1791
disable rip export 1792
disable rip exportstatic 1794
disable rip originate-default 1795
disable rip poisonreverse 1796
disable rip splitlorizon 1797
disable rip triggerupdate 1798
disable rmon 736
disable sflow 737
disable sflow backoff-threshold 738
disable sflow ports 739
disable sharing 298
disable slb 580
disable slb 3dns 581
disable slb failover 582
disable slb failover manual-failback 583
disable slb failover ping-check 584
disable slb global synguard 585
disable slb gogo-mode 586
disable slb gogo-mode ping-check 587
disable slb gogo-mode service-check 588
disable slb gogo-mode tcp-port-check 589
disable slb L4-port 591
disable slb node 593
disable slb node ping-check 595
disable slb node tcp-port-check 596
disable slb proxy-client-persistence 598
disable slb vip 599
disable slb vip client-persistence 601
disable slb vip service-check 602
disable slb vip sticky-persistence 603
disable slb vip svcdown-reset 604
disable slot 299
disable smartredundancy 300
disable snmp access 184
disable snmp dot1dTpFdbTable 185
disable snmp traps 186
disable snmp traps exceed-committed-rate ports 187
disable snmp traps lldp port 2357
disable snmp traps port-up-down ports 189
disable snmp client 190
disable source-ip-lockdown ports 977
disable ssh2 978
disable stacking 1394
disable stpd 1464
disable stpd 1465
disable stpd ports 1465
disable stpd rapid-root-failover 1467
disable subvlan-proxy-arp vlan 1654
disable sys-health-check 740
disable syslog 741
disable system-watchdog 191
disable tacacs 979
disable tacacs-accounting 980
disable tacacs-authorization 981
disable telnet 192
disable temperature-logging 742
disable transceiver-test 744
disable trusted-mac-address 982
disable type20 forwarding 2050
disable udp-echo-server 1655
disable vrrp 1578
disable wanqos 2207
disable web 193, 983
disable web http 984
disable web https 985
disable wireless ports 1303
disable wireless ports cancel-scheduler 1304
disable wireless ports every 1305
disable wireless ports interface 1306
disable wireless ports interface ap-scan 1307
disable wireless ports interface ap-scan off-channel 1308
disable wireless ports interface client-history 1309
disable wireless ports interface iapp 1311
disable wireless ports interfacesvp 1312
disable wireless ports time 1313
download bootrom 1098
download configuration 1100
download configuration cancel 1102
download configuration every 1103
download file-name 1104
download firmware slot 2302
download image 1105
download image hostname filename 1108
download ssl certificate 986
download ssl privkey 987
enable access-list 989
enable accounting 2077
enable alt-queue-management 194
enable application examination ports 2251
enable aps 2159
enable arp-learning 990
enable arp-learning ports 991
enable arp-learning vlan 992
enable arp-learning vlan ports 993
enable bgp 1914
enable bgp aggregation 1915
enable bgp always-compare-med 1916
enable bgp community format 1917
enable bgp export 1918
enable bgp neighbor 1920
enable bgp neighbor remove-private-AS-numbers 1921
enable bgp neighbor soft-in-reset 1922
enable bgp peer-group 1923
enable bgp synchronization 1924
enable bootprelay 1657
enable bootpvlan 1656
enable cli-config-logging 746
enable clipping 102
enable cpu-dos-protect 994
enable cpu-dos-protect simulated 995
enable dhcp ports vlan 196, 996
enable diagnostics cable 2252
enable diffserv examination ports 452
enable diffserv ingress replacement ports 2253
enable diffserv replacement ports 453
enable dlscs 454
enable dot1p replacement ports 456
enable dvmrp 1987
enable dvmrp rxmode vlan 1988
enable dvmrp txmode vlan 1989
enable eaps 1423
enable edp ports 302
enable elrp-client 1549
enable elsm auto-restart ports 1550
enable elsm ports 1551
enable enhanced-dos-protect 997
enable esrp vlan 1553
enable ext-mcast 1990
enable fdb-scan 420
enable flooding ports 304
enable flow-control ports 2255
enable flow-redirect 605
enable flowstats 747
enable flowstats filter ports 748
enable flowstats ping-check 750
enable flowstats ports 751
enable gvrp 391
enable icmp access-list 1658
enable icmp address-mask 1659
enable icmp parameter-problem 1660
enable icmp port-unreachables 1661
enable icmp redirects 1662
enable icmp time-exceeded 1663
enable icmp timestamp 1664
enable icmp unreachable 1665
enable icmp use-directed 1666
enable idletimeouts 103
enable igmp 1990
enable igmp snooping 1992
enable igmp snooping with-proxy 1994
enable ignore-bpdu vlan 1468
enable ignore-stp vlan 1469
enable inline-power 2303
enable inline-power legacy 2304
enable inline-power ports 2306
enable inline-power slots 2308
enable iparp checking 1672
enable ipforwarding 1674
enable ipforwarding lpm-routing 1676, 2078
enable ipmcforwarding 1995
enable ip-option loose-source-route 1667
enable ip-option record-route 1668
enable ip-option record-timestamp 1669
enable ip-option strict-source-route 1670
enable ip-option use-router-alert 1671
<table>
<thead>
<tr>
<th>Index of Commands</th>
</tr>
</thead>
<tbody>
<tr>
<td>enable iproute sharing</td>
</tr>
<tr>
<td>enable ip-subnet-lookup</td>
</tr>
<tr>
<td>enable ipxrip</td>
</tr>
<tr>
<td>enable ipxsap</td>
</tr>
<tr>
<td>enable ipxsap gns-reply</td>
</tr>
<tr>
<td>enable irdp</td>
</tr>
<tr>
<td>enable isis</td>
</tr>
<tr>
<td>enable isis export</td>
</tr>
<tr>
<td>enable isis ignore-attached-bit</td>
</tr>
<tr>
<td>enable isis originate-default</td>
</tr>
<tr>
<td>enable isis overload</td>
</tr>
<tr>
<td>enable jumbo-frame ports</td>
</tr>
<tr>
<td>enable ldetect port</td>
</tr>
<tr>
<td>enable learning ports</td>
</tr>
<tr>
<td>enable license</td>
</tr>
<tr>
<td>enable ldmp port</td>
</tr>
<tr>
<td>enable log debug-mode</td>
</tr>
<tr>
<td>enable log display</td>
</tr>
<tr>
<td>enable log target</td>
</tr>
<tr>
<td>enable log temperature</td>
</tr>
<tr>
<td>enable loopback-mode vlan</td>
</tr>
<tr>
<td>enable lpm</td>
</tr>
<tr>
<td>enable mac-lockdown-timeout ports</td>
</tr>
<tr>
<td>enable mac-vlan mac-group</td>
</tr>
<tr>
<td>enable mcast-queue-mgmt</td>
</tr>
<tr>
<td>enable mirroring to port</td>
</tr>
<tr>
<td>enable mpls</td>
</tr>
<tr>
<td>enable multilink</td>
</tr>
<tr>
<td>enable multinetting</td>
</tr>
<tr>
<td>enable nat</td>
</tr>
<tr>
<td>enable netlogin</td>
</tr>
<tr>
<td>enable netlogin logout-privilege</td>
</tr>
<tr>
<td>enable netlogin ports mac</td>
</tr>
<tr>
<td>enable netlogin ports vlan</td>
</tr>
<tr>
<td>enable netlogin session-refresh</td>
</tr>
<tr>
<td>enable ospf</td>
</tr>
<tr>
<td>enable ospf capability opaque-lsa</td>
</tr>
<tr>
<td>enable ospf export</td>
</tr>
<tr>
<td>enable ospf export direct</td>
</tr>
<tr>
<td>enable ospf export rip</td>
</tr>
<tr>
<td>enable ospf export static</td>
</tr>
<tr>
<td>enable ospf export vip</td>
</tr>
<tr>
<td>enable ospf originate-default</td>
</tr>
<tr>
<td>enable ospf originate-router-id</td>
</tr>
<tr>
<td>enable pim</td>
</tr>
<tr>
<td>enable pim snooping</td>
</tr>
<tr>
<td>enable ports</td>
</tr>
<tr>
<td>enable ports e1 loopback</td>
</tr>
<tr>
<td>enable ports loopback</td>
</tr>
<tr>
<td>enable ports loopback remote</td>
</tr>
<tr>
<td>enable ports t1 loopback</td>
</tr>
<tr>
<td>enable ports t1 loopback network payload</td>
</tr>
<tr>
<td>enable ports t1 loopback remote</td>
</tr>
<tr>
<td>enable ports t3 loopback</td>
</tr>
</tbody>
</table>

| enable ports t3 loopback remote | 2210 |
| enable qosmonitor | 458 |
| enable radius | 1007 |
| enable radius-accounting | 1008 |
| enable red port | 459 |
| enable red ports queue | 2160 |
| enable rip | 1819 |
| enable rip aggregation | 1820 |
| enable rip export cost | 1821 |
| enable rip export static cost | 1823 |
| enable rip exportstatic | 1824 |
| enable rip originate-default cost | 1825 |
| enable rip poisonreverse | 1826 |
| enable rip splitlhorizon | 1827 |
| enable rip triggerupdate | 1828 |
| enable rmon | 756 |
| enable sflow | 758 |
| enable sflow backoff-threshold | 759 |
| enable sflow ports | 760 |
| enable sharing grouping | 312 |
| enable slb | 606 |
| enable slb 3dns | 607 |
| enable slb failover | 608 |
| enable slb failover manual-failback | 609 |
| enable slb failover ping-check | 610 |
| enable slb global synguard | 611 |
| enable slb gogo-mode | 612 |
| enable slb gogo-mode ping-check | 613 |
| enable slb gogo-mode service-check | 614 |
| enable slb gogo-mode tcp-port-check | 615 |
| enable slb l4-port | 617 |
| enable slb node | 619 |
| enable slb node ping-check | 621 |
| enable slb node tcp-port-check | 622 |
| enable slb proxy-client-persistence | 624 |
| enable slb vip | 625 |
| enable slb vip client-persistence | 627 |
| enable slb vip service-check | 628 |
| enable slb vip sticky-persistence | 629 |
| enable slb vip svcdn-down-reset | 630 |
| enable slot | 315 |
| enable smartredundancy | 316 |
| enable snmp access | 198 |
| enable snmp dot1dtpfdbtable | 200 |
| enable snmp traps | 201 |
| enable snmp traps exceed-committed-rate ports | 202 |
| enable snmp traps llmp port | 2359 |
| enable snmp traps port-up-down | 205 |
| enable sntp-client | 206 |
| enable source-ip-lockdown ports | 1009 |
| enable ssh2 | 1010 |
| enable stacking | 1396 |
| enable stpd | 1470 |
| enable stpd ports | 1471 |
enable stpd rapid-root-failover 1473
enable subvlan-proxy-arp vlan 1681
enable sys-health-check 761
enable syslog 763
enable system-watchdog 207
enable tacacs 1012
enable tacacs accounting 1013
enable tacacs-authorization 1014
enable telnet 208
enable temperature-logging 764
enable transceiver-test 766
enable trusted-mac-address 1015
enable type20 forwarding 2054
enable udp-echo-server 1682
enable vman termination 2212
enable vrrp 1579
enable wanqos 2213
enable web 210, 1016
enable web http 1017
enable web http access-profile 1018
enable web https 984, 1019
enable web https access-profile 1020
enable wireless ports 1314
enable wireless ports cancel-scheduler 1315
enable wireless ports every 1316
enable wireless ports interface 1317
enable wireless ports interface ap-scan 1318
enable wireless ports interface ap-scan off-channel 1319
enable wireless ports interface client-history 1320
enable wireless ports interface client-scan 1321
enable wireless ports interface iapp 1322
enable wireless ports interface svp 1323
enable wireless ports interface time 1324
exit 211

P
ping 1205

Q
quit 213

R
reboot 107
reset inline-power ports 2310
reset inline-power slot 2311
reset wireless ports 1325
reset wireless ports interface 1326
restart multilink 2214
restart ports 317
rlookup 1683
run diagnostics 1207
run diagnostics cable port 2256
run diagnostics cable ports 1212
run diagnostics packet-memory slot 1214
run diagnostics_noslot 1210
run fdb-check 422
run ipf-check 1684
run ipmcfdb-check 2003
run msm-failover 318

S
save configuration 1109
save log 768
scp2 1021
scp2 configuration 1023
show access-list 1024
show access-list source-ip-lockdown 1027
show access-list-fdb 1028
show access-list-monitor 1029
show access-mask 1031
show access-profile 1032
show accounting 2080
show accounts password-policy 109
show accounts pppuser 111, 2161, 2215
show antenna-profile 1327
show APmgmt port 1328
show APmgmt redirect-db history 2090
show APmgmt unknown-ap history 2091
show application examination 2258
show aps 2162
show arp-learning vlan 1033
show arp-learning vlan ports 1034
show atm 2101
show atm pvc 2104
show auth 1035
show banner 113
show bgp 1925
show bgp neighbor 1926

H
history 106

L
logout 212

M
mplsping 2408, 2497
mplstrace 2410, 2499
mrinfo 1999
mtrace 2001
mvplsping 2418, 2524

N
nslookup 1204
show bgp peer-group 1928  show ip-subnet-lookup 1040
show configuration 270, 1111  show ipxconfig 2055
show cpu-dos-protect 1036  show ipxfdb 2056
show debug-trace 1217  show ipxrip 2057
show diagnostics 1221  show ipxroute 2058
show diagnostics backplane arm mapping 1224  show ipxsap 2059
show diagnostics backplane mpls mapping 1225  show ipxservice 2060
show diagnostics backplane utilization 1226  show ipxstats 2061
show diagnostics cable 2259  show 12stats 2011
show diagnostics packet-memory slot 1229  show ldp 2360
show diagnostics slot fdb 1231  show lldp neighbor 2362
show dcs 460  show lldp port statistics 2364
show dns-client 114  show lldp ports 2366
show dot1p 461  show lldp ports neighbors 2368
show dvmrp 2004  show log 775
show eaps 1424  show log components 779
show eaps shared-port 1429  show log configuration 781
show eaps summary 1431  show log configuration filter 783
show edp 319  show log configuration target 785
show elrp 1554  show log counters 786
show elsm 1557  show log events 788
show elsm ports 1558  show lpm 2081
show enhanced-dos-protect 1038  show mac-lockdown-timeout ports 1041
show esrp 1560  show mac-lockdown-timer fdb ports 1042
show esrp vlan 1563  show mac-vlan 395
show esrp-averse 115  show management 215
show esrp-aware vlan 1565  show mcast-queue-mgmt 2012
show esrp-aware-ports 1566  show memory 790
show fdb 424  show mirroring 321
show fdb vpls 2412, 2501  show mpls 2505
show flow-redirect 631  show mpls forwarding 2506
show flowstats 770, 772, 2164  show mpls health-check mplsnping 2413, 2502
show flowstats export 774  show mpls health-check vplsping 2414, 2503
show gwtp 394  show mpls interface 2508
show igmp group 2005  show mpls label 2509
show igmp snooping 2006  show mpls ld 2511
show igmp snooping filter 2007  show mpls qos-mappings 2513
show igmp snooping static group 2008  show mpls rsve-te 2514
show inline-power 2312  show mpls rsve-te lsp 2515
show inline-power configuration port 2314  show mpls rsve-te path 2516
show inline-power configuration slot 2316  show mpls rsve-te profile 2517
show inline-power info 2318  show mpls tls-tunnel 2518
show inline-power info port 2318  show mpls vpls 2415, 2416, 2504, 2519
show inline-power slot 2322  show mpls vpls nodes 2417, 2520
show inline-power stats ports 2324  show mrout 2013
show inline-power stats slot 2326  show msm-failover 322
show iparp 1685  show multilink 2216
show iparp proxy 1686  show multilink alarms 2217
show ipconfig 1687  show multilink e1 alarms 2217
show ipfdb 1689  show multilink e1 errors 2218
show ipmc cache 2009  show multilink errors 2218, 2220
show ipmc fdb 2010  show multilink stats 2219
show iproute 1691  show multilink t1 alarms 2217
show ipstats 1694  show multilink t1 errors 2220
Index of Commands

show nat 488  show qosprofile ingress 2267
show netlogin 1044  show qostype ingress priority 2269
show netlogin mac 1046  show qostype priority 466
show odometer 218  show radius 1047
show ospf 1829  show radius-accounting 1049
show ospf area 1830  show rate-limit 1051
show ospf area detail 1831  show rf-profile 1330
show ospf ase-summary 1832  show rip 1838
show ospf interfaces 1833  show rip stat 1839
show ospf interfaces detail 1834  show rip stat vlan 1840
show ospf lsd 1835  show rip vlan 1841
show ospf virtual-link 1837  show route-map 1053
show packet miscompare 794  show security-profile 1054
show packet-mem-scan-recovery-mode 792  show session 220
show pim 2015  show sflow configuration 804
show pim rp-set 2015  show sflow statistics 806
show pim snooping 2016  show sharing address-based 343
show ports alarms 2221  show slb 3dns members 633
show ports cable diagnostics 1227, 1232  show slb connections 634
show ports collisions 325  show slb esrp 636
show ports configuration 327, 2222  show slb failover 637
show ports e1 alarms 2221  show slb global 639
show ports e1 configuration 2222  show slb gogo-mode 641
show ports e1 errors 2224  show slb L4-port 642
show ports e1 info 2225  show slb node 644
show ports e1 stats 2226  show slb persistence 646
show ports egress-rate-limit 2262  show slb pool 647
show ports errors 2223  show slb stats 648
show ports info 329, 2225  show slb vip 649
show ports ingress stats 2264  show slot 344
show ports packet 333  show snmpv3 access 222
show ports qosmonitor 462  show snmpv3 context 225
show ports redundant 335  show snmpv3 counters 226
show ports rxerrors 795  show snmpv3 engine-info 228
show ports sharing 336  show snmpv3 filter 230
show ports stats 798, 2226  show snmpv3 filter-profile 231
show ports t1 alarms 2221  show snmpv3 group 232
show ports t1 configuration 2222  show snmpv3 mib-view 234
show ports t1 errors 2223  show snmpv3 notify 236
show ports t1 info 2225  show snmpv3 target-addr 229, 237
show ports t1 stats 2226  show snmpv3 target-params 238
show ports t3 alarms 2221  show snmpv3 user 239
show ports t3 configuration 2222  show sntp-client 241
show ports t3 errors 2223  show sonet 2168
show ports t3 info 2225  show source-ip-lockdown ports 1057
show ports t3 stats 2226  show ssl 1058
show ports txerrors 801  show stacking 1397
show ports utilization 338  show stacking port 1400
show ports vlan info 341  show stanza 1474
show ports vlan stats 324  show stpd ports 1477
show ppp 2166, 2227  show switch 116
show ppp info 2228  show system-dump 1234
show protocol 396  show tacacs 1061
show qosprofile 464  show tacacs-accounting 1063
Index of Commands

show tech-support 1236
show trusted-mac-address 1065
show udp-profile 1697
show version 808
show vlan 397
show vlan dhcp-address-allocation 243
show vlan dhcp-config 244
show vlan security 1066
show vlan stdp 1480
show vrrp 1580
show vrrp vlan stats 1582
show wireless ap-scan results 1335
show wireless ap-scan results mac_address 1337
show wireless client-scan results 1338
show wireless configuration 1340
show wireless device-db 2092
show wireless ports 1341
show wireless ports configuration 1343
show wireless ports debug-trace 1345
show wireless ports img-configuration 1112
show wireless ports interface ap-scan configuration 1347
show wireless ports interface ap-scan results 1349
show wireless ports interface ap-scan status 1353
show wireless ports interface client mac-statistics 1354
show wireless ports interface client-scan configuration 1356
show wireless ports interface client-history diagnostics 1357
show wireless ports interface client-history mac-layer 1359
show wireless ports interface client-history status 1361
show wireless ports interface clients 1370
show wireless ports interface client-scan configuration 1363
show wireless ports interface client-scan results 1365
show wireless ports interface client-scan results mac-address 1367
show wireless ports interface configuration 1372
show wireless ports interface pae-diagnostics 1375
show wireless ports interface pae-statistics 1376
show wireless ports interface rf-status 1377
show wireless ports interface security-status 1379
show wireless ports interface stats 1381
show wireless ports interface status 1382
show wireless ports log 1383
show wireless redirect-db 2093
ssh2 1067
synchronize 1113
T
telnet 246
top 1238
traceroute 120
U
unconfigure stacking requested-slot 1402
unconfigure aps 2169
unconfigure auth mgmt-access 1069
unconfigure auth netlogin 1070
unconfigure configuration-mode 1114
unconfigure cpu-dos-protect 1071
unconfigure diffserv dscp-mapping ports 2170
unconfigure diffserv examination ports 467
unconfigure diffserv ingress replacement ports 2270
unconfigure diffserv replacement ports 468
unconfigure dvrmrp 2017
unconfigure eaps port 1433
unconfigure eaps shared-port 1434
unconfigure eaps shared-port mode 1435
unconfigure elrp-client 1567
unconfigure enhanced-dos-protect ipfdb agingtime 1072
unconfigure enhanced-dos-protect ipfdb cache-size 1073
unconfigure enhanced-dos-protect ipfdb learn-limit 1074
unconfigure enhanced-dos-protect learn-window 1075
unconfigure enhanced-dos-protect ports 1076
unconfigure enhanced-dos-protect rate-limit 1077
unconfigure ext-mcast 2018
unconfigure fdb-scan failure-action 427
unconfigure fdb-scan period 428
unconfigure flowstats filter ports 811
unconfigure flowstats ports 812
unconfigure icmp 1701
unconfigure igmp 2019
unconfigure iparp 1702
unconfigure ipxrip 2062
unconfigure ipxsap 2063
unconfigure irdp 1703
unconfigure lldp 2370
unconfigure lldp port 2371
unconfigure log filter 813
<table>
<thead>
<tr>
<th>Command</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>unconfigure log target format</td>
<td>814</td>
</tr>
<tr>
<td>unconfigure management</td>
<td>248</td>
</tr>
<tr>
<td>unconfigure mcast-queue-mgmt</td>
<td>2020</td>
</tr>
<tr>
<td>unconfigure mpls</td>
<td>2521</td>
</tr>
<tr>
<td>unconfigure mpls hello-hold-time</td>
<td>2522</td>
</tr>
<tr>
<td>unconfigure mpls qos-mapping</td>
<td>2523</td>
</tr>
<tr>
<td>unconfigure msm-failover</td>
<td>353</td>
</tr>
<tr>
<td>unconfigure netlogin mac-addr</td>
<td>1079</td>
</tr>
<tr>
<td>unconfigure netlogin mac-addr auth-retry-count</td>
<td>1080</td>
</tr>
<tr>
<td>unconfigure ospf</td>
<td>1842</td>
</tr>
<tr>
<td>unconfigure packet-mem-scan-recovery-mode</td>
<td>816</td>
</tr>
<tr>
<td>unconfigure pim</td>
<td>2021</td>
</tr>
<tr>
<td>unconfigure port aggregate-bandwidth</td>
<td>354</td>
</tr>
<tr>
<td>unconfigure ports display-string</td>
<td>355</td>
</tr>
<tr>
<td>unconfigure ports monitor vlan</td>
<td>400</td>
</tr>
<tr>
<td>unconfigure ports redundant</td>
<td>356</td>
</tr>
<tr>
<td>unconfigure ppp</td>
<td>2229</td>
</tr>
<tr>
<td>unconfigure ppp ports</td>
<td>2172</td>
</tr>
<tr>
<td>unconfigure qostype ingress priority</td>
<td>2271</td>
</tr>
<tr>
<td>unconfigure qostype priority</td>
<td>469</td>
</tr>
<tr>
<td>unconfigure radius</td>
<td>1082</td>
</tr>
<tr>
<td>unconfigure radius-accounting</td>
<td>1083</td>
</tr>
<tr>
<td>unconfigure rip</td>
<td>1843</td>
</tr>
<tr>
<td>unconfigure sflow agent</td>
<td>817</td>
</tr>
<tr>
<td>unconfigure sflow backoff-threshold</td>
<td>818</td>
</tr>
<tr>
<td>unconfigure sflow collector</td>
<td>819</td>
</tr>
<tr>
<td>unconfigure slb all</td>
<td>651</td>
</tr>
<tr>
<td>unconfigure slb gogo-mode health-check</td>
<td>652</td>
</tr>
<tr>
<td>unconfigure slb gogo-mode service-check</td>
<td>653</td>
</tr>
<tr>
<td>unconfigure slb vip service-check</td>
<td>654</td>
</tr>
<tr>
<td>unconfigure slot</td>
<td>357</td>
</tr>
<tr>
<td>unconfigure sonet ports</td>
<td>2173</td>
</tr>
<tr>
<td>unconfigure stacking fallback-ip-address</td>
<td>1401</td>
</tr>
<tr>
<td>unconfigure stpd</td>
<td>1482</td>
</tr>
<tr>
<td>unconfigure switch</td>
<td>1115</td>
</tr>
<tr>
<td>unconfigure system-dump</td>
<td>1243</td>
</tr>
<tr>
<td>unconfigure tacacs</td>
<td>1084</td>
</tr>
<tr>
<td>unconfigure tacacs-accounting</td>
<td>1085</td>
</tr>
<tr>
<td>unconfigure transceiver-test failure-action</td>
<td>820</td>
</tr>
<tr>
<td>unconfigure transceiver-test period</td>
<td>821</td>
</tr>
<tr>
<td>unconfigure transceiver-test threshold</td>
<td>822</td>
</tr>
<tr>
<td>unconfigure transceiver-test window</td>
<td>823</td>
</tr>
<tr>
<td>unconfigure udp-profile</td>
<td>1704</td>
</tr>
<tr>
<td>unconfigure vlan dhcp-address-range</td>
<td>1086</td>
</tr>
<tr>
<td>unconfigure vlan dhcp-options</td>
<td>1088</td>
</tr>
<tr>
<td>unconfigure vlan ipaddress</td>
<td>401</td>
</tr>
<tr>
<td>unconfigure vlan xnetid</td>
<td>2064</td>
</tr>
<tr>
<td>unconfigure wireless ports image-configuration</td>
<td>1117</td>
</tr>
<tr>
<td>unconfigure wireless ports ipaddress</td>
<td>1385</td>
</tr>
<tr>
<td>unconfigure netlogin mac-addr reauth-period</td>
<td>1081</td>
</tr>
<tr>
<td>upload configuration</td>
<td>1118</td>
</tr>
<tr>
<td>upload configuration cancel</td>
<td>1120</td>
</tr>
<tr>
<td>upload log</td>
<td>824</td>
</tr>
<tr>
<td>upload system-dump</td>
<td>1244</td>
</tr>
</tbody>
</table>

Index of Commands