To disable or enable autopolarity detection, use the following command:

```
configure ports [<port_list> | all] auto-polarity [off | on]
```

Where the following is true:

- **port_list**—Specifies one or more ports on the switch
- **all**—Specifies all of the ports on the switch
- **off**—Disables the autopolarity detection feature on the specified ports
- **on**—Enables the autopolarity detection feature on the specified ports

Under certain conditions, you might opt to turn autopolarity off on one or more ports. The following example turns autopolarity off for ports 5 to 7 on a Summit family switch:

```
configure ports 5-7 auto-polarity off
```

When autopolarity is disabled on one or more Ethernet ports, you can verify that status using the command:

```
show ports information detail
```

---

**IPFIX**

**BlackDiamond 8900 series modules and Summit X460 and X480 switches only**

The IP Flow Information Export (IPFIX) protocol was created by the IETF as a standard way to capture information about traffic flows passing through network elements in a data network. The protocol consists of a **metering process**, an **exporting process**, and a **collecting process**. This section discusses the metering and exporting processes; the collecting process is not defined by the standard and therefore is outside the scope of this document. The IPFIX protocol is a rival, but complimentary, protocol to sFlow.

This feature is supported on BlackDiamond 8900 G96Tc, G48T-xl, G48X-xl and 10G8X-xl modules and Summit X460 and X480 switches.

The Extreme Networks switch contains various metering processes that gather information about flows through different ports, or **observation points**, on the switch. This information includes: the link state, IPFIX state, flow count, byte count, packet count, flow record count and premature exports. The metering process then sends the information to the exporting process in the switch which handles communication, using TCP, UDP, or SCTP transport protocols, over the network to a collecting process.
**Limitations**

This feature has the following limitations:

- The flow key definition is limited to the L2 and L3 header fields the hardware provides.
- There is a 8K flow limit per port—4K for ingress and 4K for egress.

**Enabling IPFIX**

To enable IPFIX on a port and provide a check to ensure that the port being enabled has hardware support for IPFIX, use the following command:

```
enable ip-fix ports [<port_list> | all] {ipv4 | ipv6 | non-ip | all_traffic}
```

If the port does not support IPFIX, an error message is displayed.

To disable an enabled port, use the following command:

```
disable ip-fix ports [<port_list> | all]
```

To enable or disable IPFIX globally and override an individual port enable, use the following command:

```
[enable | disable] ip-fix
```
Configuring IPFIX Flow Key Masks

Flow keys define what data in the packet header identifies a unique flow to the hardware. On each port, there is a flow key for IPv4, IPv6, and non-IP traffic type data. Following are the flow keys together with the size of the field:

IPv4:
- Source IP Address (32)
- Destination IP Address (32)
- L4 Source Port (16)
- L4 Destination Port (16)
- L4 Protocol (8)
- TOS (DSCP +ECN) (8)

IPv6:
- Source IP Address (128)
- Destination IP Address (128)
- L4 Source Port (16)
- L4 Destination Port (16)
- Next Header (8)
- IPv6 Flow Label (20)
- TOS (DSCP +ECN) (8)

Non-IP:
- Source MAC Address (48)
- Destination MAC Address (48)
- VLAN ID (12)
- VLAN Priority (3)
- Ethertype (16)
- VLAN Tagged (1)

By default, IPFIX uses all the above listed flow keys and all bits. You can override this on a global basis and specify exactly which keys to use. The template that specifies the structure of the information that is communicated from the exporter to the collector will then contain only those specified keys.

To specify the flow keys to use for each of the three traffic types, use the following commands:

```
configure ip-fix flow-key ipv4 {src-ip} {src-port} {dest-ip} {dest-port} {protocol} {tos}

configure ip-fix flow-key ipv6 {src-ip} {src-port} {dest-ip} {dest-port} {next-hdr} {tos} {flow-label}

configure ip-fix flow-key nonip {src-mac} {dest-mac} {ethertype} {vlan-id} {priority} {tagged}
```

To reset to the all keys default, use the following command:

```
unconfigure ip-fix flow-key
```
You can then define masks for the IPv4 and IPv6 source and destination address fields on a per port basis. Use the following commands:

```
configure ip-fix ports <port_list> flow-key ipv4 mask [source | destination] ipaddress <value>

configure ip-fix ports <port_list> flow-key ipv6 mask [source | destination] ipaddress <value>
```

**Example.** You can use the flow keys and masks to minimize the information sent to the collector and aggregate certain types of flows. A common use of the non-default values may be to see all traffic from a user only instead of each individual flow. For example, in the case of IPv4:

```
configure ip-fix flow-key ipv4 src-ip dest-ip
```

Then, by configuring the mask on a port, the aggregation could be further restricted to meter only individual subnets. For example, with a 255.255.255.0 mask:

```
configure ip-fix ports 3:1 flow-key ipv4 mask source ipaddress 255.255.255.0
configure ip-fix ports 3:1 flow-key ipv4 mask destination ipaddress 255.255.255.0
```

To unconfigure the masks, use the following command:

```
unconfigure ip-fix ports <port_list> flow-key mask
```

**Configuring IPFIX Parameters on a Port**

These are optional commands; when not configured, the defaults are used:

To configure whether to meter on ingress and/or egress ports, use the following command:

```
configure ip-fix ports <port_list> [ingress | egress | ingress-and-egress]
```

(The default is ingress.)

To configure whether to meter all, dropped only, or non-dropped only records, use the following command:

```
configure ip-fix ports <port_list> record [all | dropped-only | non-dropped]
```

(The default is all)

To unconfigure these IPFIX settings on a port or group of ports, use the following command. This restores the configuration to the defaults for those ports. It does not enable or disable IPFIX.

```
unconfigure ip-fix ports <port_list>
```

**Configuring Domain IDs**

Observation points are aggregated into observation domains. The entire switch operates as one domain. The IPFIX protocol contains an observation domain ID in the flow records that are sent to the collector. The collector can use the domain to correlate records to their origin. How this field is used is up to a given collector. To configure a domain ID, use the following command:

```
configure ip-fix domain <domain_id>
```
Configuring a Collector

To export flow records using the IPFIX protocol, you must first configure a collector. Only a single collector is allowed. You can specify the source IP address and VR to use when sending from the switch to a given collector. When not specified, the system defaults to the switch IP address the traffic exits.

To specify, use the following command:

```
configure ip-fix source ip-address <ipaddress> {vr <vrname>}
```

To reset back to the default of using the switch IP, use the following command:

```
unconfigure ip-fix source ip-address
```

You can specify the IP address, port number, transport protocol and VR for a collector. Use the following command:

```
configure ip-fix ip-address <ipaddress> {protocol [sctp | tcp | udp]} {L4-port <portno>} {vr <vrname>}
```

To unconfigure this, use the following command:

```
unconfigure ip-fix ip-address
```

Unconfiguring IPFIX

To unconfigure IPFIX completely use the following command. This removes all port and collector configuration and disables all ports.

```
unconfigure ip-fix
```

Displaying IPFIX Information

To display the global state, the collector information and the ports that are enabled for IPFIX, use the following command:

```
show ip-fix
```

To display information about per port metering, use the following command:

```
show ports {<port_list>} ip-fix {detail | no-refresh}
```

To show whether IPFIX is enabled on a specific port together with port IPFIX configuration, use the following command:

```
show ports {mgmt | <port_list>} information {detail}
```

WAN PHY OAM

BlackDiamond 10808, 12800, and 20800 Series Switches, and Summit X450a and Summit X480 Series Switches only.

You can configure WAN PHY OAM on the BlackDiamond 10808, BlackDiamond 12800, and BlackDiamond 20800 series switches, and Summit X450a and Summit X480 series switches whether or not they are included in a SummitStack. The WAN-PHY OAM feature is a subset of the SONET/SDH overhead function and the WAN PHY interface is defined in IEEE 802.3ae.