
This guide provides information about command line interface (CLI) of Cisco NetFlow Generation Appliance (NGA). Cisco NGA is a network appliance that receives network traffic at its 4x10G data ports via SPAN feature of Cisco switches or network tap devices and produces NetFlow records that are transmitted to NetFlow collectors where further processing of the data is performed to achieve specific needs. Cisco NGA may be configured from the device’s graphical user interface (GUI) or the command line interface. This document gives information about the command line interface.

Version 1.0
May 2, 2012
Contents

About This Guide .................................................................................................................. 5

Audience .................................................................................................................................. 5

How This Guide is Organized .................................................................................................. 5

Product Documentation ........................................................................................................... 6

Obtaining Documentation and Submitting a Service Request .................................................. 6

Command-Line Interface ........................................................................................................ 7

Logging into the Cisco NetFlow Generation Appliance ................................................................. 7

Logging in from a console server ............................................................................................... 8

Logging in from KVM console ................................................................................................... 9

Logging in from direct telnet or ssh session ............................................................................. 9

Changing the Root Password .................................................................................................... 9

Resetting the Root Password .................................................................................................... 9

Getting Help ............................................................................................................................ 11

Command and Subcommand .................................................................................................... 12

CLI Commands ........................................................................................................................ 13

audit-trail enable ..................................................................................................................... 15

cdp enable .............................................................................................................................. 16

cdp hold-time .......................................................................................................................... 17

cdp interval ............................................................................................................................. 18

clock set .................................................................................................................................... 19

config clear .............................................................................................................................. 20

config network ........................................................................................................................ 22

config upload .......................................................................................................................... 24

coredump ................................................................................................................................. 25
debug log level ................................................................. 26
exit ....................................................................................... 27
exsession ............................................................................. 28
flow collector ....................................................................... 29
flow exporter ........................................................................ 32
flow filter .............................................................................. 36
flow monitor ......................................................................... 41
flow monitor name enable ..................................................... 44
flow record ........................................................................... 45
flow sampling rate ............................................................... 49
help ......................................................................................... 50
ip ............................................................................................ 51
ip http port ........................................................................... 53
ip http secure generate .......................................................... 54
ip http secure install certificate ............................................... 57
ip http secure port ................................................................. 59
ip http secure server .............................................................. 60
ip http server ......................................................................... 62
login banner .......................................................................... 64
logout ..................................................................................... 65
managed-device ..................................................................... 66
no ......................................................................................... 68
nslookup..........................................................................................................................69
password root....................................................................................................................70
password strong-policy......................................................................................................70
patch....................................................................................................................................72
ping.......................................................................................................................................73
reboot.................................................................................................................................75
rmwebusers .........................................................................................................................76
show ....................................................................................................................................78
shutdown ............................................................................................................................81
snmp ....................................................................................................................................82
terminal ...............................................................................................................................84
time .......................................................................................................................................85
traceroute ..............................................................................................................................87
upgrade ....................................................................................................................................89
About This Guide

This guide provides information for using the Cisco NetFlow Generation Appliance command line interface (CLI).

Audience

This guide is designed for network administrators who are responsible for setting up and configuring Cisco NetFlow Generation Appliance to monitor network traffic and produce NetFlow records that are sent to NetFlow collectors. As a network administrator, you should be familiar with:

• Basic concepts and terminology used in internetworking.
• Network topology and protocols.

How This Guide is Organized

This guide is organized as follows:

<table>
<thead>
<tr>
<th>Chapter</th>
<th>Title</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chapter 1</td>
<td>Logging into the Cisco NetFlow Generation Appliance</td>
<td>Describes how to log into the appliance from the console and gives information about the two CLI command modes (the command mode and subcommand mode.)</td>
</tr>
<tr>
<td>Chapter 2</td>
<td>Command-Line Interface</td>
<td>Describes how to access Cisco NetFlow Generation Appliance’s CLI, manage the CLI root account password, use the CLI help, and use command and subcommand modes.</td>
</tr>
<tr>
<td>Chapter 3</td>
<td>CLI Commands</td>
<td>Lists CLI commands alphabetically and provides detailed information about the commands.</td>
</tr>
</tbody>
</table>
This document uses the following conventions:

<table>
<thead>
<tr>
<th>Item</th>
<th>Convention</th>
</tr>
</thead>
<tbody>
<tr>
<td>Commands and keywords</td>
<td><strong>boldface</strong></td>
</tr>
<tr>
<td>Variables for which you supply values</td>
<td><strong>italic</strong></td>
</tr>
<tr>
<td>Displayed session and system information</td>
<td><strong>screen</strong> font</td>
</tr>
<tr>
<td>Information you enter</td>
<td><strong>boldface</strong> <strong>screen</strong> font</td>
</tr>
<tr>
<td>Variables you enter</td>
<td><strong>italic</strong> <strong>screen</strong> font</td>
</tr>
<tr>
<td>Menu items and button names</td>
<td><strong>boldface</strong> font</td>
</tr>
</tbody>
</table>

**Note** Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the publication.

**Caution** ⚠ Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

**Warning** ⚠ This symbol means danger. You are in a situation that could cause bodily injury.

**Product Documentation**

For more information about the documentation set for this product or other documentation including supported platforms, see the following URL:


**Obtaining Documentation and Submitting a Service Request**

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What’s New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

1

Command-Line Interface

This chapter provides information about how to access Cisco NetFlow Generation Appliance’s CLI and manage the CLI root account password. It also provides information on how to use the CLI help as well as move from command and subcommand modes.

This chapter includes the following sections:

- Logging into the Cisco NetFlow Generation Appliance
- Changing the Root Password
- Resetting the Root Password
- Getting Help
- Command and Subcommand

Logging into the Cisco NetFlow Generation Appliance

Initial configuration or reconfiguration of network settings requires access to the appliance CLI via its console. There are two ways to access the appliance’s console: from a console server connected to the appliance’s console port at the back panel, or direct access from the front panel’s KVM port which has an adapter to connect a keyboard, monitor, and optional mouse. A KVM port adapter is included with the appliance. There is only one access level, which is root.
Note The first time you access the console you will be prompted to provide the root user account password. Follow the prompt to provide the password.

After the initial network settings, you could optionally provide direct telnet or ssh to the appliance CLI. To enable telnet, use exssesion on command. To enable direct ssh, use exssion on ssh command.

Logging in from a console server
To log into the appliance console from a console server, the appliance’s console port, which is located at the back panel of the appliance, must be connected to a console server. Consult the console server’s documentation for configuration of the console line speed and console port number. The configuration must be done prior to accessing the appliance’s console. As an example, to log in to the appliance via a telnet session, do:

Step 1. Open a telnet session to the console port.
Example:

bash-3.2$ telnet 172.20.103.34 2007
Trying 172.20.103.34...
Connected to 172.20.103.34.
Escape character is '^]'.

Cisco Netflow Generation Agent

nga-ucs.cisco.com login:

Step 2. Provide the username as root, and follow the prompt to provide password. Upon a successful login, the NGA prompt will be displayed.

Example:

nga-ucs.cisco.com login: root
Password: (provide password, which is not displayed)
Last login: Mon Apr 9 17:58:29 2012 from example.cisco.com on pts/1

Cisco NetFlow Generation Agent on UCS (NGA3140-K9) Console, 1.0(1)
Copyright (c) 2012 by Cisco Systems, Inc.

root@nga-ucs.cisco.com#
Logging in from KVM console
The appliance’s KVM port is located at the front panel. A KVM port adapter is included with the appliance. Insert the KVM cable into the KVM port. Connect a VGA monitor, a keyboard, and optionally a mouse to the KVM cable. After the connections, you will have full access to the appliance console.

Logging in from direct telnet or ssh session
Logging in to the appliance CLI via direct telnet or SSH can only be achieved after the IP address is configured and the “exsession” feature is enabled via CLI commands applied at the console. To enable direct telnet, use `exsession on` command. To enable SSH, use `exsession on ssh` command. You can directly telnet or SSH to the appliance from any device that supports telnet or SSH.

Changing the Root Password
Root account is the only account to the Cisco NetFlow Generation Appliance’s CLI. To change the account login password, apply CLI command `password root` while you are in the CLI prompt. You will be prompted for the new password.

Example:
```
root@nga-ucs.cisco.com# password root
Enter new password:
Confirm new password:
Successfully changed password for user 'root'
root@nga-ucs.cisco.com#
```

Resetting the Root Password
If appliance CLI root account password is forgotten, follow steps below to reset the password.

Step 1. Access the appliance via console port or KVM port.

Step 2. Power cycle the appliance. Pay attention to the screen. When asked for image to boot, select helper
Note If you have the appliance CIMC port setup properly, you could power cycle the appliance from the CIMC graphical user interface.

Step 3. Type 4 for menu item 4 Reset application image passwords to default

Note This will clear the root account password. Upon the next login, you will be prompted to provide the root account password.

Cisco Systems, Inc.
Netflow Agent (NGA3140-K9) helper utility
Version 1.1(0.1)

Main menu
1 - Download application image and write to HD
2 - Download application image and reformat HD
3 - Display software versions
4 - Reset application image CLI passwords to default
5 - Change file transfer method (currently)
6 - Send Ping
7 - Display RAID Settings
m - Configure network
r - Exit and reset Services Engine
h - Exit and shutdown Services Engine
Selection [1234567nrh]: 4
Restored default CLI passwords of application image.
Selection [1234567nrh]: 

Step 4. Type r for menu item r Exit and reset Service Engine
Getting Help

Cisco NetFlow Generation Appliance CLI provides help text by typing `? [enter]` or `help [enter]`. CLI will also auto-complete command keywords.

To auto-complete a command word, use the `tab` key. When there are multiple possible matches, a list of the available commands will be displayed. When there is only a single match, the command word will be auto-completed.

Example:

A single matching keyword for the command that has been typed at the prompt completes the command:

```
root@nga-ucs.cisco.com# show f[tab]
root@nga-ucs.cisco.com# show flow
```

Example:

A list of available matching commands are displayed following typing `[tab]` key:

```
root@nga-ucs.cisco.com# show l[tab]
log login
root@nga-ucs.cisco.com# show log
```

To obtain help text for a command, use `? [enter]` or `help [enter]`

Example:

```
root@nga-ucs.cisco.com# show flow ? [enter]
collector    - Show flow collector
exporter     - Show flow exporter
filter       - Show flow filter
monitor      - Show flow monitor
record       - Show flow record
sampling     - Show flow sampling information received at data ports
root@nga-ucs.cisco.com# show flow
```
Command and Subcommand

When you login to the Cisco NetFlow Generation Appliance CLI, you are at the main command prompt. Some commands will bring you into a subcommand mode, where you provide additional commands to complete the main command task. The prompt will change to indicate that you are in a particular subcommand mode. While entering commands in the subcommand mode, no actual changes to the configuration are made. When are finished entering commands and exit from the subcommand mode, that is when the configuration will be applied to the NGA.

Example: The following example shows the flow monitor subcommand. Notice that the CLI prompt changed to signify entering in subcommand mode of flow monitor.

```
root@nga-ucs.cisco.com# flow monitor?
<WORD>
   - Set monitor name

root@nga-ucs.cisco.com# flow monitor example-monitor

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@nga-ucs.cisco.com(sub-monitor)#
```
This chapter contains an alphabetical listing of all the CLI commands available in Cisco NetFlow Generation Appliance. Some commands are available only in the main command’s subcommand mode.

This chapter includes the following commands and subcommands:
- audit-trail enable
- cdp enable
- cdp hold-time
- cdp interval
- clock set
- config clear
- config network
- config upload
- coredump
- debug log level
- exit
- exsession
- flow collector
- flow exporter
- flow filter
- flow monitor
- flow monitor name enable
- flow record
- flow sampling rate
- help
- ip
- ip http port
- ip http secure generate
- ip http secure install certificate
- ip http secure port
- ip http secure server
- ip http server
- login banner
- logout
- managed-device
- no
- nslookup
- password root
- password strong-policy
- patch
- ping
- reboot
- rmwebusers
- show
- shutdown
- snmp
- terminal
- time
- traceroute
- upgrade
**audit-trail enable**

To enable logging of tasks performed from GUI and CLI, use **audit-trail enable** command. To disable logging of tasks performed from GUI and CLI, use the **no** form of this command.

- **audit-trail enable**
- **no audit-trail enable**

**Defaults**
Audit trail of the CLI and GUI accesses is enabled.

**Command Modes**
This command is available in command mode.

**Examples**
This example shows how to enable an audit trail for GUI and CLI accesses:

```
root@nga-ucs.cisco.com# audit-trail enable
Successfully enabled audit trail
root@nga-ucs.cisco.com#
```

**Related Commands**
- **show audit-trail**
**cdp enable**

To enable the Cisco Discovery Protocol (CDP) on the NGA, use the `cdp enable` command. To disable CDP on the NGA, use the `no` form of this command.

```
  cdp enable
  no cdp enable
```

**Defaults**

By default, cdp is enabled.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how to enable CDP:

```
root@nga-ucs.cisco.com# cdp enable
Successfully enabling cdp.
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show cdp settings`
- `cdp hold-time time`
- `cdb interval interval`
cdp hold-time

To set NGA CDP hold time, use `cdp hold-time time` command. This command will set the NGA’s CDP message holding time prior to expiring the CDP entry. Valid time input value is in between 10 and 255 seconds and must be larger than or equal to the CDP interval.

```
cdp hold-time time
```

**Defaults**

By default, CDP hold time value is 180 seconds.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how to set NGA CDP hold time to 60 seconds:

```
root@nga-ucs.cisco.com# cdp hold-time 60
Successfully set cdp hold time.
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show cdp settings`
- `[no] cdp enable`
- `cdp interval interval`
cdp interval
To set NGA CDP interval time, use `cdp interval time` command. This command sets how often NGA broadcasts a CDP message. Valid time input value is in between 5 and 254 seconds and must be less than or equal to the CDP hold time.

`cdp interval time`

Defaults
By default, CDP interval time value is 60 seconds.

Command Modes
This command is available in command mode.

Examples
This example shows how to set NGA CDP interval time to 10 seconds:
```
root@nga-ucs.cisco.com# cdp interval 10
Successfully set cdp message interval.
root@nga-ucs.cisco.com#
```

Related Commands

- `show cdp settings`
- `[no] cdp enable`
- `cdp hold-time time`
**clock set**

To set the NGA system clock, use `clock set hh:mm:ss mm/dd/yyyy` command. This command sets the current time and date for the NGA system clock. The time zone can be set with the `time` command.

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

**Defaults**
There is no default value.

**Command Modes**
This command is available in command mode.

**Examples**
This example shows how to set NGA system clock

```
root@nga-ucs.cisco.com# clock set 16:52:00 04/09/2012
Mon Apr  9 16:52:00 PDT 2012
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show clock details`
- `show date`
- `show time`
- `time`
**config clear**

This command clears the existing configuration on the NGA system. There are 3 levels of clearing available: clear the IP settings only, clear all existing configuration except IP settings, and clear all existing NGA configuration including IP settings. To only clear the IP settings on NGA, use `config clear ip` command. To clear existing NGA configuration and reset back to the factory default state, use `config clear all` command. To retain only the IP settings and clear all other configuration, use `config clear` command.

- `config clear`
- `config clear ip`
- `config clear all`

**Defaults**

There is no default value.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how existing NGA configuration is removed from the system.

```
root@nga-ucs.cisco.com# config clear
This operation will reset the NGA configuration (including disabling the web server).
This operation will also reboot the NGA to allow the changes to take effect.

Do you wish to continue? [y/n] [n]: y
(NGA is rebooting after this point.)
```
Related Commands

show configuration
**config network**

This command downloads a configuration text file, which was previously uploaded or saved with the command `config upload`, and applies that configuration to NGA.

`config network ftp-url-file`

**Defaults**

There is no default value.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how NGA configuration file is downloaded and applied to NGA.

```
root@nga-ucs.cisco.com# config network ftp://example@172.20.98.174//users/example/nga-upload.config
```

This operation will reboot NGA for the changes to take effect.

Do you wish to continue? {y/n} [n]: y

Downloading ftp://example@172.20.98.174//users/example/nga-upload.config, please wait ...

Password for example@172.20.98.174:

ftp://example@172.20.98.174//users/example/nga-upload.config (7K)

/tmp/lrcfile.txt.3170  [########################]  7K  |  580.06K/s

7363 bytes transferred in 0.01 sec (515.44k/sec)

Download completed.

Configuring the NGA. This may take a few minutes, please wait...

(NGA will reboot after applying the configuration line by line)
Related Commands

show configuration

config upload ftp-url-path [filename]
config upload
This command uploads or saves the NGA configuration at the provided FTP server location. You may optionally provide the configuration file name after the FTP path. If no file name is explicitly specified on the command line, an appropriate file name will be chosen for you and displayed on the screen during the upload process.

    config upload ftp-url-path [filename]

Defaults
There is no default value.

Command Modes
This command is available in command mode.

Examples
This example shows how NGA configuration is upload to an FTP server.

    root@nga-ucs.cisco.com# config upload ftp://example@172.20.98.174 example-nga.config
    Building configuration, please wait... Done.

    Uploading the configuration to 'example-nga.config'
    on 'ftp://example@172.20.98.174', This may take few minutes ...

    Password:
    Operation completed.
    root@nga-ucs.cisco.com#

Related Commands
    show configuration
    config network ftp-url-file
coredump
This command uploads all NGA core files to an FTP server. It is to be used only if the NGA system is unexpectedly out of service, and there are one or more core files in the NGA show tech-support output.

```
coredump ftp-url-path
```

Defaults
There is no default value.

Command Modes
This command is available in command mode.

Examples
```
root@nga-ucs.cisco.com# coredump ftp://kluu@172.20.98.174
No core file present
root@nga-ucs.cisco.com#
```

Related Commands
```
show tech-support
```
**debug log level**

This command is used to set the debug log level (verbosity) of various internal features in NGA. By default, debug log level of all features are set to ERROR (1). At this level, a message will be logged in the debug log file only when an error or critical condition occurs. In some cases, such as when troubleshooting a specific problem, the log level can be set to different threshold for each individual features. This can cause more messages to be logged and may help in the troubleshooting process to determine what is happening. Valid debug levels are CRITICAL(0), ERROR(1), WARNING(2), NOTICE(3), INFO(4), DEBUG(5), DEBUG2(6), and DEBUG3(7). The larger the threshold value, the more debug messages will be produced.

**Defaults**
This command has no default setting.

**Command Modes**
Command and subcommand modes.

**Examples**
This example shows how set debug level for the internal netflow cache to DEBUG(5)

```bash
root@nga-ucs.cisco.com# debug log level NFA_CACHE 5
debug log level for NFA_CACHE changed from 'error' to 'debug'.
root@nga-ucs.cisco.com#
```

**Related Commands**

`none`
To log out of the system or to leave a subcommand mode, use the audit-trail enable

To enable logging of tasks performed from GUI and CLI, use `audit-trail enable` command. To disable logging of tasks performed from GUI and CLI, use the `no` form of this command.

```
audit-trail enable

no audit-trail enable
```

**Defaults**
Audit trail of the CLI and GUI accesses is enabled.

**Command Modes**
This command is available in command mode.

**Examples**
This example shows how to enable an audit trail for GUI and CLI accesses:

```
root@nga-ucs.cisco.com# audit-trail enable
Successfully enabled audit trail
root@nga-ucs.cisco.com#
```

**Related Commands**
`show audit-trail`
**cdp enable**

To enable the Cisco Discovery Protocol (CDP) on the NGA, use the `cdp enable` command. To disable CDP on the NGA, use the `no` form of this command.

```
   cdp enable

   no cdp enable
```

**Defaults**

By default, cdp is enabled.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how to enable CDP:

```
root@nga-ucs.cisco.com# cdp enable
Successfully enabling cdp.
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show cdp settings`
- `cdp hold-time time`
- `cdb interval interval`
cdp hold-time

To set NGA CDP hold time, use `cdp hold-time time` command. This command will set the NGA’s CDP message holding time prior to expiring the CDP entry. Valid time input value is in between 10 and 255 seconds and must be larger than or equal to the CDP interval.

`cdp hold-time time`

**Defaults**

By default, CDP hold time value is 180 seconds.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how to set NGA CDP hold time to 60 seconds:

```
root@nga-ucs.cisco.com# cdp hold-time 60
Successfully set cdp hold time.
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show cdp settings`
- `[no] cdp enable`
- `cdb interval interval`
**cdp interval**

To set NGA CDP interval time, use `cdp interval time` command. This command sets how often NGA broadcasts a CDP message. Valid time input value is in between 5 and 254 seconds and must be less than or equal to the CDP hold time.

```plaintext
  cdp interval time
```

**Defaults**

By default, CDP interval time value is 60 seconds.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how to set NGA CDP interval time to 10 seconds:

```plaintext
root@nga-ucs.cisco.com# cdp interval 10
Successfully set cdp message interval.
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show cdp settings`
- `[no] cdp enable`
- `cdp hold-time time`
clock set
To set the NGA system clock, use clock set hh:mm:ss mm/dd/yyyy command. This command sets the current time and date for the NGA system clock. The time zone can be set with the time command.

clock set hh:mm:ss mm/dd/yyyy

Defaults
There is no default value.

Command Modes
This command is available in command mode.

Examples
This example shows how to set NGA system clock

root@nga-ucs.cisco.com# clock set 16:52:00 04/09/2012
Mon Apr 9 16:52:00 PDT 2012
root@nga-ucs.cisco.com#

Related Commands

  show clock details
  show date
  show time
  time
config clear

This command clears the existing configuration on the NGA system. There are 3 levels of clearing available: clear the IP settings only, clear all existing configuration except IP settings, and clear all existing NGA configuration including IP settings. To only clear the IP settings on NGA, use **config clear ip** command. To clear existing NGA configuration and reset back to the factory default state, use **config clear all** command. To retain only the IP settings and clear all other configuration, use **config clear** command.

```
config clear
config clear ip
config clear all
```

Defaults
There is no default value.

Command Modes
This command is available in command mode.

Examples
This example shows how existing NGA configuration is removed from the system.

```
root@nga-ucs.cisco.com# config clear
This operation will reset the NGA configuration (including disabling the web server).
This operation will also reboot the NGA to allow the changes to take effect.

Do you wish to continue? [y/n] [n]: y
(NGA is rebooting after this point.)
```
Related Commands

show configuration
config network

This command downloads a configuration text file, which was previously uploaded or saved with the command `config upload`, and applies that configuration to NGA.

```
config network ftp-url-file
```

**Defaults**
There is no default value.

**Command Modes**
This command is available in command mode.

**Examples**
This example shows how NGA configuration file is downloaded and applied to NGA.

```
root@nga-ucs.cisco.com# config network ftp://example@172.20.98.174//users/example/nga-upload.config
```

This operation will reboot NGA for the changes to take effect.

Do you wish to continue? {y/n} [n]: y

Downloading ftp://example@172.20.98.174//users/example/nga-upload.config, please wait ...

Password for example@172.20.98.174:
ftp://example@172.20.98.174//users/example/nga-upload.config (7K)
/tmp/lrcfile.txt.3170  [########################################]  7K | 580.06K/s
7363 bytes transferred in 0.01 sec (515.44k/sec)

Download completed.

Configuring the NGA. This may take a few minutes, please wait...

(NGA will reboot after applying the configuration line by line)
Related Commands

- `show configuration`
- `config upload ftp-url-path [filename]`
**config upload**

This command uploads or saves the NGA configuration at the provided FTP server location. You may optionally provide the configuration file name after the FTP path. If no file name is explicitly specified on the command line, an appropriate file name will be chosen for you and displayed on the screen during the upload process.

```
config upload ftp-url-path [filename]
```

**Defaults**

There is no default value.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how NGA configuration is upload to an FTP server.

```
root@nga-ucs.cisco.com# config upload ftp://example@172.20.98.174 example-nga.config
Building configuration, please wait... Done.

Uploading the configuration to 'example-nga.config'
on 'ftp://example@172.20.98.174', This may take few minutes ...

Password:
Operation completed.
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show configuration`
- `config network ftp-url-file`
coredump

This command uploads all NGA core files to an FTP server. It is to be used only the NGA system is unexpectedly out of service, and there are one or more core files in the NGA show tech-support output.

    coredump ftp-url-path

Defaults
There is no default value.

Command Modes
This command is available in command mode.

Examples
root@nga-ucs.cisco.com# coredump ftp://kluu@172.20.98.174
No core file present
root@nga-ucs.cisco.com#

Related Commands

    show tech-support
debug log level

This command is used to set the debug log level (verbosity) of various internal features in NGA. By default, debug log level of all features are set to ERROR (1). At this level, a message will be logged in the debug log file only when an error or critical condition occurs. In some cases, such as when troubleshooting a specific problem, the log level can be set to different threshold for each individual features. This can cause more messages to be logged and may help in the troubleshooting process to determine what is happening. Valid debug levels are CRITICAL(0), ERROR(1), WARNING(2), NOTICE(3), INFO(4), DEBUG(5), DEBUG2(6), and DEBUG3(7). The larger the threshold value, the more debug messages will be produced.

Defaults
This command has no default setting.

Command Modes
Command and subcommand modes.

Examples
This example shows how set debug level for the internal netflow cache to DEBUG(5)

```
root@nga-ucs.cisco.com# debug log level NFA_CACHE 5
debug log level for NFA_CACHE changed from 'error' to 'debug'.
root@nga-ucs.cisco.com#
```

Related Commands

none
exit command. When typed from the subcommand level, all parameters provided while in the subcommand mode will be applied to the system and you will be placed back at the main command level. When typed from the main command mode, you will be logged out and your CLI session is terminated.

exit

Defaults
This command has no default setting.

Command Modes
Command and subcommand mode.

Examples
This example shows how to log out of the NGA:
root@nga-ucs.cisco.com# exit

Related Commands
none
exsession

To enable or disable direct telnet or ssh logins to NGA CLI, use the **exsession** command. CLI command **exsession on** enables telnet to NGA. CLI command **exsession off** disables telnet to NGA. CLI command **exsession on ssh** enables SSH to NGA. CLI command **exsession off ssh** disables SSH to NGA.

- **exsession on [ssh]**
- **exsession off [ssh]**

**Defaults**
This command has no default setting.

**Command Modes**
Command mode.

**Examples**
This example shows how to allow outside logins to the NGA:
```
root@nga-ucs.cisco.com# exsession on
```

**Related Commands**
- **show ip**
flow collector

Use flow collector name command to define a destination host where the NGA may send NetFlow records. The records are derived from network packets arriving at NGA’s data ports. This command has a set of subcommands. Upon typing flow collector name, you will be in the subcommand mode where you can specify all necessary parameters.

**Note** The collector name word in the command must be a unique word. Upon entering flow collector name, if a collector with that name already exists, you will be modifying the existing collector rather than defining a new one.

Follows is the list of subcommands:

- **address ipv4-address**: Use this subcommand to set the ipv4 address of the collector where NGA will send NetFlow packets to. You must provide the collector address prior to exiting the subcommand mode.

- **description description-string**: Use this subcommand to provide a descriptive string for the collector. It’s only for your reference, it is not used by the system.

- **dscp dscp-value**: Use this command to set the DSCP value of NetFlow packets that are sent out by this NGA. By default, DSCP value is 0.

- **no description**: Use this command to clear a description string that was previously set for this collector.

- **transport udp destination-port udp-port**: Use this command to set the UDP port where NGA sends NetFlow packets to. This is the UDP port that collector device is listening on for NetFlow packets. Many collector devices use UDP port 9995 as the receiving port. By default, NGA set this UDP port value to 3000.

- **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the main command mode.

- **cancel**: Use this command to cancel and exit the subcommand mode. You will be brought back to the command mode. Configuration does not change.

Use the no form of the command, no flow collector name, to delete a flow collector. You can only delete one flow collector at a time. An active flow monitor must not be using the collector at the time the collector is deleted.
Defaults
This command has no default setting.

Command Modes
This command is available in command mode.

Examples
This example shows a flow collector example-collector being created with collector address 1.2.3.4 and udp port 3000.

```
root@nga-ucs.cisco.com# flow collector example-collector

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@nga-ucs.cisco.com(sub-collector)# address 1.2.3.4
root@nga-ucs.cisco.com(sub-collector)# description this is an example
root@nga-ucs.cisco.com(sub-collector)# transport udp destination-port 3000
root@nga-ucs.cisco.com(sub-collector)# exit
Successfully created flow collector example-collector.
root@nga-ucs.cisco.com# show flow collector example-collector

Collector name: example-collector
Description: this is an example
IP address: 1.2.3.4
DSCP value: 0
Transport: UDP
Port number: 3000
```

root@nga-ucs.cisco.com#
Related Commands

show flow collector
flow exporter

Use `flow exporter name` command to specify various parameters for an export session between the NGA and one or more collectors. Use this command to specify: the collector(s) that the exporter will use to send NetFlow packets, the version format of NetFlow packets to be sent, and frequencies that the exporter will send template and option data, if applicable. This command has a set of subcommands. Upon entering `flow exporter name`, you will be in the subcommand mode.

**Note** The exporter `name` in the command should be unique to define a new exporter session. Upon entering `flow exporter name`, if a flow exporter with that name already exists, you will be modifying the existing exporter.

**Note** The rules for evaluating a filter are as follows. When defining a particular field within one filter (e.g. source-port) you may provide multiple comma-separated values to be matched. These values are a logical OR, so that any one of the listed values may be matched. When multiple fields are used, it is a logical AND, so all of those fields must match one of the listed values. Filters may be applied at two different processing points – the exporter level, and the collector level. For all flows that may potentially be exported, filters defined at the exporter level are evaluated first. For any flows that pass that first level of filtering, additional filters may be specified at the collector level, which apply only to a single. Finally, you may specify more than one filter. When multiple filters are used, it is a logical OR, so that any one of them may match.

Following is the list of subcommands for this command:

- **description description-string**: Use this command to specify the description string of the exporter. This is for your reference only, it is not used by the system.

- **destination collector-name**: Use this command to specify one of your previously-defined collectors which will be used in this exporter. The collector must have already been configured prior to entering to this subcommand mode. Multiple flow exporters may use the same flow collector. An exporter must have at least one collector.

- **destination collector-name filter filter-names**: Use this command to set 1 or more filtering rules at the collector level. Filtering rules at this level only affect the collector `collector-name`. Other collectors in the exporter are not impacted by filtering rules of this collector. The `filter-names` is a comma-separated list of previously configured flow filters.
Note Collector level filtering rules are only applicable when the exporter policy is set to multi-destination.

- **destination collector-name weight packet-count**: Use this command to set round robin weight by packet count.

Note Collector weight is applicable only when the policy of the exporter is set to weighted-round-robin. Filtering at collector level with weighted-round-robin policy is not applicable.

- **filter filter-names**: Use this command to set filtering rules at the exporter level. Filtering rules at this level impact all collectors in the exporter. _filter-names_ is a comma-separated list of previously configured filters.

- **no description**: Use this command to clear the description string set in this exporter.

- **no destination collector-name**: Use this command to remove a collector that is being used by this exporter. Upon entering this command, the collector _collector-name_ and any filter rules at its level are removed from the exporter. Remember that an exporter must have at least one collector.

- **no destination collector-name filter filter-name**: Use this command to remove filter _filter-name_ from the collector _collector-name_. You can remove 1 filter at a time. Upon entering the command, the filter _filter-name_ is removed from the collector _collector-name_.

- **no filter**: Use this command to remove all filter rules at the exporter level.

- **no filter filter-name**: Use this command to remove a single filter _filter-name_ from the exporter. You can remove 1 filter at time.

- **option-period period**: Use this command to set how often (in minutes) the exporter will send option template and option data to collector devices.

Note The setting in this command is only applicable when the exporter version is set to v9 or IPFIX

- **policy multi-destination**: Use this command to set the exporting policy to multi-destination policy. In this policy, the exporter will send the same NetFlow packet to all collectors set in the exporter.

- **policy weighted-round-robin**: Use this command to load balance by NetFlow packet count among collectors set in this exporter. By default, all collectors set in the exporter have weight of 1. Use destination _collector-name weight packet-count_ command to set the weight. The exporter will send the specified number of packets to the collector, before moving on to start sending to the next collector on the list.
• **template-period period**: Use this command to set how often (in minutes) the exporter will send NetFlow data templates to collectors in the exporter. This command is applicable only when the exporter version is set to v9 or IPFIX.

• **version v5 | v9 | IPFIX**: Use this command to set the format of the NetFlow packets that are sent to collector devices.

• **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the command mode.

• **cancel**: Use this command to cancel the setting and exit the subcommand mode. You will be brought back to the command mode. Configuration does not change.

Use the no form of the command, **no flow exporter name** to delete a flow exporter. You can only delete 1 flow exporter at a time. An active flow monitor must not be using the exporter at the time the exporter is deleted.

**Defaults**
This command has no default settings.

**Command Modes**
This command is available in command mode.

**Examples**
This example shows how to create a flow exporter.

```
root@nga-ucs.cisco.com# flow exporter example-exporter

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.
```

```
root@nga-ucs.cisco.com(sub-exporter)# version v9
root@nga-ucs.cisco.com(sub-exporter)# template-period 20
root@nga-ucs.cisco.com(sub-exporter)# option-period 30
root@nga-ucs.cisco.com(sub-exporter)# destination example-collector
root@nga-ucs.cisco.com(sub-exporter)# description this is an example
root@nga-ucs.cisco.com(sub-exporter)# exit
Successfully created flow exporter example-exporter.
```
root@nga-ucs.cisco.com# show flow exporter example-exporter

Exporter name: example-exporter
Description: this is an example
Export version: v9
Template timeout: 20 minutes
Options timeout: 30 minutes
Policy: Multi-destination
Destination name: example-collector

root@nga-ucs.cisco.com#

Related Commands

show flow exporter
flow filter

Use the command `flow filter name` to set up a filter that could be used within a flow exporter. You may re-use the same filter in multiple flow collectors as well as multiple exporters. In a single flow filter, you can filter on multiple fields. Flow filter fields are classified into two types: address type and scalar type.

- Address type: Filter fields of this type include MAC, IPv4, and IPv6 address fields. Filter fields of this type take one address or an address and mask length. For example, 1.2.3.0/24.

- Scalar type: Filter fields of this type apply to all remaining filter fields aside from address type fields. Filter fields of this type take a combination of single values and a range of values in a comma-separated list format. For example: 1, 3, 9-23, 29

**Note** The filter name in the command must be a unique to create a new filter. If a filter with the same name already exists, you will be modifying the existing filter.

**Note** In evaluating a filter, multiple values specified for a single field are logical OR, so any value may be a match. For multiple fields specified in a single filter, it is a logical AND, so all fields must match one of their target values.

**Note** NGA filter fields will accept values which may considered “invalid” for that field within flows that normally appear on a network. The idea is to allow NGA to catch malformed packets on the network.

**Note** NGA will only export flow records that pass the filter rules (i.e. the filter specifies which flows to accept and export, not which flows are to be dropped). Filtering is applied at the flow level, not the packet level. In the case of NetFlow version 9 or IPFIX, all fields to be filtered must also be included and configured in the flow record in order for the filter rule to function correctly. If the flow record itself does not include a particular field, then the behavior for a filter operating on that field is undefined. In the case of NetFlow version 5, the filters must be defined only for fields that appear in a standard v5 record.

Upon entering command `flow filter name`, you will be in the subcommand mode for the filter named `name`. Changes are only applied when you exit from the subcommand mode. Following is the list of subcommands.

- **application-id scalar-list:** This is a scalar type filter field. Application ID is a 4-byte unsigned integer value mapping to an application name. Network traffic received by NGA
will be processed and classified as an application based on L4-ports. Packets of a flow that are well classified to an application will be assigned a specific application ID. Any unclassifiable network traffic will be assigned the “unknown” application ID value. The application ID field is not available in NetFlow version 5, but is available for version 9 and IPFIX via configuration of \textbf{flow record} command.

\textbf{Note} A mapping of application ID value to application name is periodically sent to collectors via NDEv9 or IPFIX option data. The frequency of option template and option data is configured via \textbf{flow exporter} command.

- \textit{cos scalar-list}: This is a scalar type filter field. Use this command to setup a filter for accepting flows that have COS value equal to any of the \textit{scalar-list} values. Valid input COS value for this field is 0 – 7 inclusive. COS is an abbreviation for Class Of Service, and refers to the 3-bit 802.1p “Priority” field inside the 802.1q VLAN header.

- \textit{description description-string}: Use this command to set the description string for this flow filter.

- \textit{destination-port scalar-list}: This is a scalar type filter field. Use this command to setup a filter accepting flows that have L4 (TCP/UDP) destination port value equal to any of the \textit{scalar-list} values. Valid input value for this field is 0 – 65535 inclusive.

- \textit{ethertype scalar-list}: This is a scalar type filter field. Use this command to setup a filter accepting flows that have 2-byte ether-type field value equal to any of the \textit{scalar-list} values. Valid input value for this field is 2-byte hex in the range of 0x0000 – 0xFFFF inclusive. This field corresponds to the “ethertype” field found in the standard Ethernet packet header.

- \textit{flow-label scalar-list}: This is a scalar type filter field. Use this command to setup a filter accepting IPv6 flows that have flow label value equal to any of the values in \textit{scalar-list}. Valid input for this filter field is 0 – 1048575 inclusive. This field corresponds to the IPv6 flow label field.

- \textit{icmp-code-ipv4 scalar-list}: This is a scalar type filter field. Use this command to setup a filter accepting IPv4 flows that have IPv4 ICMP “code” value equal to any of the values in \textit{scalar-list}. Valid input in this field is 0 – 255 inclusive.

- \textit{icmp-code-ipv6 scalar-list}: This is a scalar type filter field. Use this command to setup a filter accepting IPv6 flows that have IPv6 ICMP “code” value equal to any of the values in \textit{scalar-list}. Valid input in this field is 0 – 255 inclusive.

- \textit{icmp-type-ipv4 scalar-list}: This is a scalar type filter field. Use this command to setup a filter accepting IPv4 flows that have IPv4 ICMP “type” value equal to any of the values in \textit{scalar-list}. Valid input in this field is 0 – 255 inclusive.
• **icmp-type-ipv6 scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting IPv6 flows that have IPv6 ICMP “type” value equal to any of the values in `scalar-list`. Valid input in this field is 0 – 255 inclusive.

• **input-snmp scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting flows that have input interface SNMP index value equal to any of the values in `scalar-list`. Valid input value in this field is 0 – 2147483647 inclusive.

• **ip-protocol scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting flows that have IP protocol numbers equal to any of the `scalar-list` values. Valid input value in this field is 0 – 255 inclusive.

• **ipv4-destination v4-address/mask**: This is an address type field. Use this command to setup a filter for accepting IPv4 flows that have destination address matching `v4-address` after logical bit-wised AND with the `mask` bits. `v4-address` is dot format notation of an IPv4 address. `mask` is the number of bits.

• **ipv4-source v4-address/mask**: This is an address type field. Use this command to setup a filter for accepting IPv4 flows that have source address matching `v4-address` after logical bit-wised AND with the `mask` bits. `v4-address` is dot format notation of an IPv4 address. `mask` is the number of bits.

• **ipv6-destination v6-address/mask**: This is an address type field. Use this command to setup a filter for accepting IPv6 flows that have destination address matching `v6-address` after logical bit-wised AND with the `mask` bits. `v6-address` is short colon format notation of an IPv6 address (e.g. FE00:ABC::0100:00A0). `mask` is the number of bits. If `mask` is not provided, value 128 is assumed.

• **ipv6-source v6-address/mask**: This is an address type field. Use this command to setup a filter for accepting IPv6 flows that have source address matching `v6-address` after logical bit-wised AND with the `mask` bits. `v6-address` is short colon format notation of an IPv6 address. `mask` is the number of bits. If `mask` is not provided, value 128 is used.

• **mac-destination mac-address/mac-mask**: This is an address type field. Use this command to setup a filter accepting flows that have destination MAC address matching `mac-address` after performing logical bit-wised AND with the `mac-mask`. Valid MAC address is the format of XX:XX:XX:XX:XX:XX. `mac-address` is the number of bits set and must be in the range of 1 – 48 inclusive. If `mac-mask` is not provided, a mask value 48 is used.

• **mac-source mac-address/mac-mask**: This is an address type field. Use this command to setup a filter for accepting flows that have source MAC address matching `mac-address` after logical bit-wised AND with the `mac-mask`. Valid MAC address is the format of XX:XX:XX:XX:XX:XX. `mac-mask` is the number of bits set and must be in the range of 1 – 48 inclusive. If `mac-mask` is not provided, a mask value 48 is used.

• **mpls-label scalar-list**: This is a scalar type field. Use this command to setup a filter for accepting flows that have to topmost MPLS label matching any value in the list of `scalar-list`. Valid input value is in the range of 0 – 1048575 inclusive.
• **network-encapsulation scalar-list**: This is a scalar type field. Use this command to setup a filter that accepts flows which have the NGA derived network encapsulation value matching with any value in the *scalar-list*. NGA supports encapsulation IP(1), IPv6(2), IPIP4(3), GREIP(4), IPESP(5), GTP(6), and IPIP6(7). A number between 1 – 7 represents the encapsulation in CLI.

• **no filter-field-keyword**: Use this command to remove a particular field from this filter. *filter-field-keyword* is all the filter field described in this command. For example: **no application-id**, **no mpls-label**, and **no ipv6-source**. Upon exiting the subcommand mode the change is applied.

• **output-snmp scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting flows that have output SNMP interface index value equal to any of the values in *scalar-list*. Valid input value in this field is 0 – 2147483647 inclusive.

• **source-port scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting flows that have L4 source port value equal to any of the *scalar-list* values. Valid input value for this field is 0 – 65535 inclusive.

• **tcp-flags scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting flows that have TCP flag value equal to any of the *scalar-list* values. Valid input value for this field is 0 – 255 inclusive. This field is a bitwise OR of all the TCP flags that have been observed on the flow.

• **tos scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting IPv4 flows that have IPv4 TOS byte value equal to any of the *scalar-list* values. Valid input value for this field is 0 – 255 inclusive.

• **traffic-class scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting IPv6 flows that have IPv6 traffic class byte value equal to any of the *scalar-list* values. Valid input value for this field is 0 – 255 inclusive.

• **vlan-id scalar-list**: This is a scalar type filter field. Use this command to setup a filter accepting flows that have VLAN ID value equal to any of the *scalar-list* values. Valid input value for this field is 0 – 4095 inclusive.

• **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the main command mode.

• **cancel**: Use this command to cancel the setting and exit the subcommand mode. You will be brought back to the main command mode. Configuration does not change.

Use the no form of the command, **no flow filter name** to delete a flow filter. You can only delete 1 flow filter at a time. An active flow monitor must not be using the exporter that is using the flow filter at the time the filter is deleted.
Defaults
This command does not have default setting.

Command Modes
This command is available in command mode.

Examples
This example shows the how to create a flow filter to accept flows that originated from subnet 1.2.3.0/24 with TCP port 80, 8080, or 4343.

```
root@nga-ucs.cisco.com# flow filter example-filter

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@nga-ucs.cisco.com(sub-filter)# description this is an example
root@nga-ucs.cisco.com(sub-filter)# ipv4-source 1.2.3.0/24
root@nga-ucs.cisco.com(sub-filter)# destination-port 80,8080,4343
root@nga-ucs.cisco.com(sub-filter)# source-port 80,8080,4343
root@nga-ucs.cisco.com(sub-filter)# exit

Successfully created flow filter example-filter.

root@nga-ucs.cisco.com# show flow filter example-filter

<table>
<thead>
<tr>
<th>Filter name:</th>
<th>example-filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td>this is an example</td>
</tr>
<tr>
<td>IPv4 source address:</td>
<td>1.2.3.0/24</td>
</tr>
<tr>
<td>Destination port:</td>
<td>80,8080,4343</td>
</tr>
<tr>
<td>Source port:</td>
<td>80,8080,4343</td>
</tr>
</tbody>
</table>
```

root@nga-ucs.cisco.com#
flow monitor

Flow monitor is a conceptual device that takes network traffic from data ports and generates flow records based on parameters configured at the exporter and monitor. It forwards the flow information to the exporter, which further applies filter rules, packs the flow records into NetFlow packets, and sends the NetFlow packets to collectors. NGA supports up to 4 ACTIVE flow monitors at the same time. Across all 4 ACTIVE monitors, NGA supports up to 6 flow collectors.

**Note** A flow collector that is used in 2 different ACTIVE monitors is counted as 2 flow collectors toward the 6 flow collector limit in the system.

**Note** The monitor *name* in the command must be unique to create a new flow monitor. If a flow monitor with that name already exists, you are modifying the existing monitor.

Upon entering command `flow monitor name`, you will be brought to the subcommand of flow monitor. Prior to exiting the subcommand mode, changes to the flow monitor *name* are not yet applied to the system. Upon exiting the subcommand via `exit` subcommand, the changes are applied. Following is the list of subcommands in `flow monitor name` command:

- **cache size percent**: Use this command to set the percentage of total cache memory space to allocate for this monitor instance, before flows are aged out of the cache and forwarded to the exporter. In general, the larger the cache size, the more concurrent flows can be handled by this particular monitor. Note that the system as a whole can simultaneously track 64 million flows. If you plan to only configure a single flow monitor, you can specify 100 (= 100%) for this parameter. If you plan to configure multiple monitors, then you must decide what percentage of the total cache memory should be used for each monitor instance. For example, you may decide to configure four flow monitors and give each one 25% of the total cache space. The default value is 25.

- **cache timeout active seconds**: Use this command to set how often (in seconds) flow statistics will be exported to collectors for flows which are continuously active. The default value is 1800 (30 minutes), which means for long-lived active flows, a flow record will be exported to the collector(s) once every 30 minutes. You may change the default to any value in the range 5-65535, inclusive.

- **cache timeout inactive seconds**: Use this command to set the maximum time (in seconds) a flow that has not been updated with network traffic will stay in the cache before it is deleted and forwarded to the flow exporter. The default value is 15 seconds.
Note Depending on network traffic pattern, cache timeout values are used to fine how often flows will be sent to collector devices (active timeout), and to help prevent cache overflow (inactive timeout).

- **cache type permanent** | **standard**: Use this command to set the cache mode. In permanent cache mode, flows are never deleted from the cache to free space for new flows. In standard cache mode, inactive flows will be completely removed from the cache, and the memory space is made available for a new flow to use. Most often you will want to use standard type, which is the default. Permanent mode is only useful for rare deployments where there will be very few flows, or a fixed number of flows, and you do not want them to be aged out of the cache.

- **dataport number**: Use this command to set the data port(s) on which this flow monitor will receive packets and populate flow records. **number** is a comma-separated list of data port numbers. E.g. 1,3,4 for data ports 1, 3, and 4. Note that the same data port may be used to populate multiple different flow monitors.

- **description description-string**: Use this command to set the description string for this flow monitor. This is only for your reference, it is not used by the system.

- **exporter name**: Use this command to set the exporter to which this monitor will forward flow information. Upon receiving flow information from the flow monitor, the flow exporter will perform filter rules (if any), construct NetFlow packets, and send the packets to collector device(s). Only one flow exporter is allowed per flow monitor. However, the same exporter can be used in multiple different monitors.

- **no dataport**: Use this command to remove a data port previously assigned to this monitor. A flow monitor must have at least one data port on which to receive packets. To remove a single previously set data port, use **no dataport** command.

- **no description**: Use this command to clear the description string that was previously configured for this flow monitor.

- **no record**: Use this command to remove all flow records previously set to this monitor. Upon entering the command, previously set flow records are removed from this monitor. A flow monitor with exporter version v9 or IPFIX must have at least one flow record. You may configure at most one IPv4, one IPv6, and one Layer-2 record type in a single monitor. To remove a single previously configured flow record, use **no record** command.

- **record record-names**: Use this command to configure a previously defined record for use with this monitor. A flow monitor with exporter version v9 or IPFIX must have at least one flow record. You may configure at most one IPv4, one IPv6, and one Layer-2 record type in a single monitor. Configuring a record for use in a monitor that is associated with an exporter of type v5 is unnecessary, and not allowed. NetFlow v5 has a fixed, pre-defined record format which cannot be changed.
- **tunnel inner | outer**: Use this command to instruct the flow monitor how to handle network packets that are tunneled and have more than one set of IP addresses. You may configure the monitor to track either the innermost IP addresses, or the outermost IP addresses. The default value is “inner.”

- **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the command mode.

- **cancel**: Use this command to cancel the setting and exit the subcommand mode. You will be brought back to the command mode. Configuration does not change.

Use the no form of the command, **no flow monitor name**, to delete a flow monitor. You can only delete 1 flow monitor at a time. Deleting an active flow monitor is not allowed. You must first deactivate it using the command **flow monitor name disable**.

**Defaults**
This command has no default settings.

**Command Modes**
This command is available in command mode.

**Examples**
This example show how to create a flow monitor

```
root@NG
root@nga-ucs.cisco.com# flow monitor example-monitor

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@nga-ucs.cisco.com(sub-monitor)# exporter example-exporter
root@nga-ucs.cisco.com(sub-monitor)# record example-record
root@nga-ucs.cisco.com(sub-monitor)# dataport 2,3
root@nga-ucs.cisco.com(sub-monitor)# cache size 40
root@nga-ucs.cisco.com(sub-monitor)# exit
Successfully created monitor example-monitor.
root@nga-ucs.cisco.com# show flow monitor example-monitor
```

<table>
<thead>
<tr>
<th>Monitor name:</th>
<th>example-monitor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description:</td>
<td></td>
</tr>
<tr>
<td>Exporter name:</td>
<td>example-exporter</td>
</tr>
<tr>
<td>Record name:</td>
<td>example-record</td>
</tr>
<tr>
<td>Dataport:</td>
<td>2,3</td>
</tr>
<tr>
<td>Tunnel:</td>
<td>Inner</td>
</tr>
<tr>
<td>Cache size:</td>
<td>40 %</td>
</tr>
</tbody>
</table>
flow monitor name enable

Use this command, `flow monitor name enable`, to activate a flow monitor. When a flow monitor is configured, it is in INACTIVE state. A successfully activated flow monitor will change from INACTIVE state to ACTIVE state, and will begin to process network traffic arriving at its data ports. From the packets arriving at its data ports, the monitor will begin to produce flow information for the flow exporter, which then generates NetFlow packets to send to collector devices. An INACTIVE state flow monitor does not have any functionality in the system. At the time a flow monitor is activated, flow components (exporter, collector, record, and filter) that are used by the flow monitor must have been defined. You will not be able to activate a flow monitor if any of the necessary components is not yet configured. When a flow monitor is in ACTIVE state, the flow monitor and all flow components that it is using cannot be modified. Use command `flow monitor name disable` prior to any modification and deletion.

Defaults
This command has no default settings.

Command Modes
This command is available in command mode.

Examples
This example show how a flow monitor is enabled.

```
root@nga-ucs.cisco.com# flow monitor example-monitor enable
Successfully enabled example_monitor.

root@nga-ucs.cisco.com#
```
Flow records are used only for NetFlow v9 and IPFIX. A flow record is the definition of which fields are to be used to construct the flow information that is sent to collectors. Flow monitors use these definitions to construct flow information from network traffic received on NGA data ports. In NetFlow v9 and IPFIX terminology, an NGA flow record is the template.

A flow record consists of several fields. Some of the fields are keys used to uniquely identify a flow, and others are the statistics of the flow. No field that may be used both as key field and a statistics field. Key fields are defined with subcommand `match`. Statistics fields are defined with subcommand `collect`. There are 3 types of flow records: IPv6, IPv4, and Layer-2.

- **IPv6 record type**: This record type consists of at least one IPv6 address as the key of the record. Other IPv6 packet fields are optional in the keys of the record.
- **IPv4 record type**: This record type has at least one IPv4 address key field. Other IPv4 packet fields are optional in the keys of the record.
- **Layer-2 record type**: This record type has at least one MAC address key field. Other layer 2 packet fields are optional in the keys of the record.

**Note** A flow record must have at least one packet or byte statistic field.

**Note** When a flow monitor processes an IPv6 packet to create flow information, it only uses the IPv6 record type. If there is no IPv6 record type configured, it uses the Layer-2 record type. If there is no Layer-2 record type configured, the IPv6 packet is dropped.

**Note** When a flow monitor processes an IPv4 packet to create flow information, it only uses the IPv4 record type. If there is no IPv4 record type configured, it uses the Layer-2 record type. If there is no Layer-2 record type configured, the IPv4 packet is dropped.

Upon entering command `flow record name` you will be brought to the subcommand level. Prior to exiting the subcommand mode, changes to the flow record `name` are not yet applied to the system. Upon exiting the subcommand via `exit` subcommand, the changes are applied. Following is the list of subcommands in `flow monitor name` command.

**Note** The record `name` in the command must be unique to define a new record. If a flow record already exists with that name, you will be modifying the existing record.

- **collect**: Use this command to define statistic fields for a record. Available statistic fields are the following:
- **classification application-id**: Use this subcommand to define the application ID field as a statistic field.
- **classification net-encap**: Use this subcommand to define the network encapsulation as a statistic field.
- **counter packets | bytes**: Use these 2 subcommands to define packet and/or byte counters as statistic fields. All flow records must have at least one of the two.
- **icmp code | type**: Use these 2 subcommands to define ICMP code and/or type as statistic fields of a record.
- **ip max-ttl | min-ttl**: Use these 2 subcommands to define max/min IPv4 TTL field as statistic fields of a record.
- **ipv6 flow-label | max-hop-limit | min-hop-limit**: Use these 3 subcommands to define IPv6 flow label and hop limit as statistic fields of a record.
- **timestamp sysuptime first | last**: Use these 2 subcommands to define flow start and end timestamp as statistic fields of a record.

**Note** Although the command has keyword *sysuptime*, the units of the actual timestamp sent to collectors will depend upon which version of NetFlow is used, v5, v9, or IPFIX.

- **transport tcp flags**: Use this command to define TCP header flag as a statistics field of a record.

**description description-string**: Use this subcommand to set the description string for this flow record. This is for your reference only, it is not used by the system.

**match**: Use this subcommand to define key fields of a record. The following fields are available:

- **datalink cos | ethertype | mac-destination | mac-source | mpls | vlan**: These subcommands are available for IPv4, IPv6, and Layer-2 record types.
- **input-interface**: This subcommand is available for both IPv4, IPv6, and Layer-2 record types.
- **output-interface**: This subcommand is available for IPv4, IPv6, and Layer-2 record types.
- **destination**: This subcommand is available for IPv4 and IPv6 record types. Use this command to define the destination address as key field of the record.
- **ip protocol**: This command is available for IPv4 and IPv6 record types.
- **ip tos**: This command is available for IPv4 record type only.
- **ip traffic-class**: This command is available for IPv6 record type only.
- **source**: This command is available for IPv4 and IPv6 record types. Use this command to define the source address as a key field of the record.

- **transport destination-port | source-port**: These 2 subcommands are available for IPv4 and IPv6 record types. Use these commands to select the TCP/UDP source/destination port as key fields of the record.

  - **no collect**: Use this subcommand to remove a previously configured statistic field in the record. All the statistic fields described in the subcommand `collect` are available in this `no collect` subcommand.

  - **no description**: Use this subcommand to clear the description string of the record.

  - **no match**: Use this subcommand to remove previously configured key field in the record. All the key fields described in subcommand `match` above are available.

  - **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the command mode.

  - **cancel**: Use this command to cancel the setting and exit the subcommand mode. You will be brought back to the command mode. Configuration does not change.

Use the no form of the command, `no flow record name`, to delete a flow record. You can only delete 1 flow record at a time. Deleting a record that is being used by an active flow monitor is not allowed.

### Defaults
This command has no default settings.

### Command Modes
This command is in command mode.

### Examples
This example shows how to create an IPv4 record type.

```
root@nga-ucs.cisco.com# flow record ipv4 example-record

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@nga-ucs.cisco.com(sub-record)# collect counter packets
root@nga-ucs.cisco.com(sub-record)# collect counter bytes
root@nga-ucs.cisco.com(sub-record)# collect ip max-ttl
root@nga-ucs.cisco.com(sub-record)# collect ip min-ttl
```
root@nga-ucs.cisco.com(sub-record)# collect timestamp sys-uptime first
root@nga-ucs.cisco.com(sub-record)# collect timestamp sys-uptime last
root@nga-ucs.cisco.com(sub-record)# collect transport tcp flags
root@nga-ucs.cisco.com(sub-record)# match datalink mac-source
root@nga-ucs.cisco.com(sub-record)# match datalink mac-destination
root@nga-ucs.cisco.com(sub-record)# match datalink ethertype
root@nga-ucs.cisco.com(sub-record)# match input-interface
root@nga-ucs.cisco.com(sub-record)# match output-interface
root@nga-ucs.cisco.com(sub-record)# match destination
root@nga-ucs.cisco.com(sub-record)# match source
root@nga-ucs.cisco.com(sub-record)# match ip protocol
root@nga-ucs.cisco.com(sub-record)# match transport destination-port
root@nga-ucs.cisco.com(sub-record)# match transport source-port
root@nga-ucs.cisco.com(sub-record)# description this is an example
root@nga-ucs.cisco.com(sub-record)# exit
Successfully created example-record flow record configuration.
root@nga-ucs.cisco.com# show flow record example-record

Record name: example-record
Record type: IPv4
Record description: this is an example
Number of match fields: 10
Match field: MAC source address
Match field: MAC destination address
Match field: Ethertype field
Match field: Input Interface
Match field: Output Interface
Match field: IPv4 destination address
Match field: IPv4 source address
Match field: IP protocol
Match field: Destination port
Match field: Source port
Number of collect fields: 7
Collect field: Packet count
Collect field: Byte count
Collect field: Maximum TTL/hop limit
Collect field: Minimum TTL/hop limit
Collect field: First timestamp
Collect field: Last timestamp
Collect field: TCP header flags

root@nga-ucs.cisco.com#
flow sampling rate

Use this command, `flow sampling rate rate`, to set the packet-sampling ratio of the network traffic that arrives at NGA data ports. Packet sampling is a feature that may be available at the managed device, for example the Cisco Nexus series switches support SPAN sampling (Switch Port ANalyzer). If the switch is configured to replicate samples of network traffic to NGA data port, you should use this command to set the sampling ratio information in NGA. After this is configured, NGA sends the packet sampling information to collector device via NetFlow v9 or IPFIX option data. To remove flow sampling information, use `no flow sampling`.

**Defaults**
This command has no default settings.

**Command Modes**
This command is available in command mode.

**Examples**
Assuming network traffic arrives at NGA data port is being sample by 1 packet out of 10000, this example show how the information is configured on NGA.

```
root@nga-ucs.cisco.com# flow sampling rate 10000
Successfully set sampling rate.
```

This example shows how to remove sampling information.

```
root@nga-ucs.cisco.com# no flow sampling
Successfully removed sampling rate.
```

```
root@nga-ucs.cisco.com#```
help

To display help, use the help command or ?. You must press the Enter key after entering the ? or help.

    help | ?

Defaults
This command has no default settings.

Command Modes
Command mode or subcommand mode.

Examples
This example shows how to display help:

    root@nga-ucs.cisco.com# help
    ?       - Display help
    audit-trail   - Enable logging Web GUI and CLI accesses
    cdp       - Set cdp settings
    clock     - Set system clock
    config    - Configure NGA
    coredump  - Retrieve the coredump file
    debug     - Configure debug parameters
    exit      - Log out of system
    exsession - Enable/disable outside logins
    flow      - Netflow agent(NGA) configuration
    help      - Display help
    (there are more output after this point)

Related Commands

    none
**ip**

The `ip` command sets the basic network connectivity for NGA.

- **ip address ipv4-address mask:** Use this command to set the management address for NGA.
- **ip broadcast ipv4-address:** Use this command to set the broadcast address for NGA. After the `ip address` command, broadcast address on NGA is automatically derived and set with the provided mask, therefore only in rare cases is it ever necessary to execute this command.
- **ip domain domain.name:** Use this command to set the domain name for NGA.
- **ip gateway ipv4-address:** Use this command to set the IP gateway address for NGA.
- **ip host host-name:** Use this command to set the host name of the NGA.
- **ip nameserver ipv4-address:** Use this command to set up to three name servers for NGA.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to set the system IP parameters:

```
root@nga-ucs.cisco.com# ip address 172.20.103.86 255.255.255.128
root@nga-ucs.cisco.com# ip gateway 172.20.103.1
root@nga-ucs.cisco.com# ip domain cisco.com
root@nga-ucs.cisco.com# ip host nga-ucs
root@nga-ucs.cisco.com# show ip
```

- IP address: 172.20.103.86
- Subnet mask: 255.255.255.128
- IP Broadcast: 172.20.103.127
- DNS Name: nga-ucs.cisco.com
- Default Gateway: 172.20.103.1
- Nameserver(s): 171.68.226.120
- HTTP server: Disabled
- HTTP secure server: Enabled
- HTTP port: 80
- HTTP secure port: 443
- TACACS+ configured: No
- Telnet: Disabled
- SSH: Disabled
Related Commands

show ip
ip http server enable
ip http server disable
exsession on
exsession off
**ip http port**

This command changes the NGA WEB graphical user interface (GUI) access from a default TCP port 80 to other TCP port value.

```
ip http port port-number
```

**Defaults**

By default, NGA WEB TCP port is set to 80.

**Command Modes**

Command mode

**Examples**

This example shows how to set WEB GUI port to 8080

```
root@nga-ucs.cisco.com# ip http port 8080
```

Successfully changed HTTP port to 8080.

```
root@nga-ucs.cisco.com#
```

**Related Commands**

- `show ip`
- `ip http server enable`
ip http secure generate

For security reasons, you may want to use the NGA secure HTTP server to have all HTTP network traffic from and to NGA encrypted. Prior to enabling the secure HTTP server, a certificate is needed. You could use either a self-signed certificate or submit a request to Certificate Authority (CA) for a certificate. To use a self-signed certificate, use command **ip http secure generate self-signed-certificate**. To generate a certificate request to submit to Certificate Authority (CA) for a certificate, use **ip http secure generate certificate-request**. You will need to cut and paste the generated certificate to fill in a form obtained from Certificate Authority (CA) and mail the form to the Certificate Authority (CA).

**ip http secure generate self-signed-certificate**

**ip http secure generate certificate-request**

---

**Defaults**
There is no default value. If self-signed certificate is desired, the command **ip http secure generate self-signed-certificate** will also install the certificate. If a certificate is obtained from a Certificate Authority (CA), install the certificate to NGA by using the command **ip http secure install certificate** command.

---

**Command Modes**

Command mode

---

**Examples**
This example shows how to generate a certificate request

```
root@nga-ucs.cisco.com# ip http secure generate certificate-request
A certificate-signing request already exists. Generating a new one will invalidate the existing one and any certificates already generated from the existing request. Do you still want to generate a new one? [y/n] y
5243 semi-random bytes loaded
Generating RSA private key, 2048 bit long modulus
  .+++ 
  ........+++ 
e is 65537 (0x10001)
```
You are about to be asked to enter information that will be incorporated into your certificate request.

What you are about to enter is what is called a Distinguished Name or a DN.

There are quite a few fields but you can leave some blank

For some fields there will be a default value,

If you enter `.`, the field will be left blank.

-----

Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: California
Locality Name (eg, city) []: San Jose
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Cisco Systems, Inc.
Organizational Unit Name (eg, section) []: NMTG
Common Name (eg, YOUR name) [nga-ucs.cisco.com]:
Email Address []: example@cisco.com

-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwgagxCzAJBgNVBAYTAlVTMRMwEQYDVQQIEwpDYVQQIExwZm9ybmlh
MREwDwYDVQQHEw9TYW4gSm9zZTEgMB4GA1UEChQXQ2lzY28gc3kICFN5c3RlbXMs
IEluYy4xETAPBgNVBAsUCE5HCE1HCFRHMRowGAYDVQQDExFuZ2tEdWNzLmNpc2Nv
LmNvbTEgMB4GCSqGSIb3DQEJARYRZXhhbXBsZUBjaXNjby5jb20wYwYDVQQDExM2
S1b3QEBQUAA4IBDwAwgqEKAoIBAQC17KrIMyheIAqgWLDazmYlQQak05m0f4
JryAaFvWXzLg0Kn7aACLCpTH6NjtsTm8isgVaxzJFGICQSQmpf/0mOWeAJ1Rf6i5
KXadrug1ZhrnYG4/eeefCtXq40swgFmBa3AbUTm1FkunPJC05InaDliK+Ibjmyyz
i6v65M7sb/yVhpjNYjwpe9OXa8+c5X5XHjJsOrDn0w1BExC07VxmEn94WJx4v
h9EkQ1YUtzbGgw6EqdF38hQt7C7InRrhydZwzTt15nQT9gtZ/nKQmKpczuzMJSG
/Xswr/YVEfjVhqtHLy/9voaig04UUV3su3Eg4zoaYc101Rw145AgMBAAAgADAN
BkgkhkiG9w0BAQUFUAAOCQAEAZo6TsXn/4/vHf0rqTJ9oiWb09iQSeIbvpvvsTuFp
c08XZKRRMQSMYukw2SCFRgd/BU5TaNyFhNqgSUeW5Eq6t6MJGq0gPcM8Ths
Dr1rsHhfrmInLW8P8W+hbtwu9f+n0XqvhY3XRTi8FgPGfj6vOpDuW14rSHHKLJ
CkQbr700UHiZW35/3dwa77Fqx5S9w4yQq5fBBtwQio98aNDHFxNTuxXs8tSKPz
r4S48A0ryw7qwdIsupdKyuULZI4HvBUC+bAPpWVZrIs671RcQ1pmFVcO/1aYriJ
PJjsEsAJayJ500MrpxeF0VIaJslE68TqouIXdEuN/igpg==
-----END CERTIFICATE REQUEST-----
root@nga-ucs.cisco.com#
Related Commands

- show ip
- ip http secure port port
- ip http secure server enable
- ip http secure install certificate
ip http secure install certificate

This command is to install the certificate that you obtained from a Certificate Authority (CA). Once the certificate is installed, NGA HTTP secure server will use the certificate for encryption and decryption of WEB traffic from and to NGA.

Defaults
There is no default value.

Command Modes
Command mode

Examples
This example shows how to install a certificate.

root@nga-ucs.cisco.com# ip http secure install certificate

Cut and paste the certificate you received from Certificate Authority. Enter a period (.), then press enter to indicate the end of the certificate.

MIIE6DCCAgAwIBAgIJAOYR5M9q3JogMA0GCSqGSIb3DQEBAQUAA4IBDAwIBAgIMAQoGCCsGAQUFBzAChFUwUQYDVQQIDBat55ICB2Zl9mLiB3QXJ0aWZpY2F0ZS1Ob3RzLmN0cm90ZWFsMB8GA1UEAxMRbmdhLXVjcy5jaXNjby5jb20gU2F1dGhvc2UgQ2VydGlmaWNhdGlvbiBUaW1lIHRoaW5nIFowgXBTMREwDwYDVQQDDA55ICBDYW4gU2VydGlmaWNhdGlvbiBQdHJ1ZSBBc3NpZ25hdGlvbiBCaXNjcyBDb3JzaW9uIHJlbWxvZ2UgSW5mb3JtZHMuIEN1c3Rvb21Vc2VyaXZlciB0cGxvdzEhGz也算是certificate

Cisco NetFlow Generation Appliance Command Reference

OL-26439-01
The certificate could not be installed. You have not generated the certificate-signing request or the certificate is not in a valid certificate format.

root@nga-ucs.cisco.com#
**ip http secure port**

This command sets the NGA secure HTTPS server port.

```
ip http secure port port-number
```

**Defaults**
By default, NGA secure WEB TCP port is set to 443.

**Command Modes**
Command mode

**Examples**
This example shows how to set WEB GUI port to 4343

```
root@nga-ucs.cisco.com# ip http secure port 4343
Successfully changed HTTP secure port to 4343.
root@nga-ucs.cisco.com#
```

**Related Commands**

- show ip
- ip http secure server enable
- ip http secure generate
- ip http secure install
ip http secure server
To enable secure HTTPS server for accessing NGA from graphical user interface (GUI), use `ip http secure server enable` command. To disable the HTTPS server, use `ip http secure server disable` command. If there is no WEB user account configured in the system, you will be prompted to do so. Follow the prompt to create the WEB user account.

```
ip http secure server enable
ip http secure server disable
```

**Defaults**
By default, NGA secure HTTPS server is disabled.

**Command Modes**
Command mode

**Examples**
This example shows the NGA secure server being enabled and the user is prompted to create a WEB user account.

```
root@nga-ucs.cisco.com# ip http secure server enable

No web users are configured.
Please enter a web administrator user name [admin]:
New password:
Confirm password:

User admin added.
Starting httpd
root@nga-ucs.cisco.com# show ip
IP address: 172.20.103.86
Subnet mask: 255.255.255.128
IP Broadcast: 172.20.103.127
DNS Name: nga-ucs.cisco.com
Default Gateway: 172.20.103.1
```
Nameserver(s): 171.68.226.120
HTTP server: Disabled
HTTP secure server: Enabled
HTTP port: 4343
HTTP secure port: 8080
TACACS+ configured: No
Telnet: Enabled
SSH: Disabled
root@nga-ucs.cisco.com#

Related Commands

show ip
ip http port port
ip http server disable
ip http secure
ip http server

To enable HTTP server for accessing NGA from graphical user interface (GUI), use `ip http server enable` command. To disable the HTTP server, use `ip http server disable` command. When there is no WEB user account configured in the system, you will be prompted to do so. Follow the prompt to create the WEB user account.

```
   ip http server enable
   ip http server disable
```

**Defaults**

By default, NGA HTTP server is disabled.

**Command Modes**

Command mode

**Examples**

This example shows the NGA web server being enabled and the user is prompted to create a WEB user account.

```
root@nga-ucs.cisco.com# ip http server enable

No web users are configured.

Please enter a web administrator user name [admin]:

New password:

Confirm password:

User admin added.

Enabling web server...

Successfully enabled web server.

root@nga-ucs.cisco.com#
```

**Related Commands**

```
show ip
ip http port port
```
ip http server disable
ip http secure
**login banner**
Use this command to set the login banner string. To remove the login banner, use the `no login banner` command.

**Defaults**
This command has no default settings.

**Command Modes**
This command is available in command mode.

**Examples**
This example shows how to create your own login banner string:

```
root@nga-ucs.cisco.com# login banner
Enter Login Banner Text
Terminate with a single '.' or Ctrl-D [Limit 1024 characters]:
This is an example
.
root@nga-ucs.cisco.com#
```
**logout**

To log out of the system, use the `logout` command. This command is the same as the `exit` command at the main command mode.

**Defaults**

This command has no default settings.

**Command Modes**

This command is available in command mode.

**Examples**

This example shows how to log out of the Cisco NGA:

```
root@nga-ucs.cisco.com# logout
localhost>
```
managed-device

A managed device replicates network packets to NGA data ports for monitoring and producing NetFlow packets to collector devices. Each NGA data port can be connected to a different managed device, such as a Cisco Nexus series switch. When a managed device is configured, NGA will communicate with the managed device and download internal information about the device, so that the NGA can populate the input and output interface for flow records that are sent to collectors.

If no managed device is configured for a particular dataport, then the NGA will populate the input and output interface fields in flow records with a value corresponding to its own local dataport on which the flow was received. With a managed device configured however, the NGA will attempt to compute the correct interfaces on that device through which the flow passed. It will use those values in the flow records instead of the values corresponding to its own local data ports.

Upon entering `managed-device netconf address v4-address`, you will be in the subcommand mode. Configuration is not changed until you exit the subcommand mode. If a managed device with the address already exists, the existing managed device will be edited. Available subcommands are as follows:

- **dataport ports**: Use this command to set the data ports where NGA is receiving network traffic from the managed device. `ports` is a comma-separated string, e.g. 2,3 for data port 2 and data port 3.

- **password**: Use this command to set the password that NGA uses for telnet/ssh session to the managed device. This password is the password for the username defined below.

- **username**: Use this command to set the user name that NAM uses for telnet/ssh session to the managed device.

- **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the command mode.

- **cancel**: Use this command to cancel the setting and exit the subcommand mode. You will be brought back to the command mode. Configuration does not change.

Use the no form of the command, `no managed-device netconf address v4-address`, to delete a managed device. You can only delete 1 managed device at a time.

**Defaults**

This command has no default settings.
**Command Modes**

Command mode

**Examples**

This example shows how to configure a managed device in the Cisco NGA:

```
root@nga-ucs.cisco.com# managed-device netconf address 1.1.1.1
```

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

```
root@nga-ucs.cisco.com(sub-mgd-device)# username example
root@nga-ucs.cisco.com(sub-mgd-device)# password
Enter password:
Confirm password:
```

Successfully created managed device 1.1.1.1.
```
root@nga-ucs.cisco.com# show managed-device
```

<table>
<thead>
<tr>
<th>Managed Device:</th>
<th>1.1.1.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID:</td>
<td>1</td>
</tr>
<tr>
<td>Username:</td>
<td>example</td>
</tr>
<tr>
<td>Dataport:</td>
<td>2,4</td>
</tr>
</tbody>
</table>

```
root@nga-ucs.cisco.com#
```

**Related Commands**

*show managed-device*
This command is the negate form of various commands. See each command for more detail information. As a summary, the following commands can be negated by preceding with the **no** keyword:

- no audit-trail enable
- no flow collector name
- no flow exporter name
- no flow filter name
- no flow monitor name
- no flow record name
- no flow sampling
- no login banner
- no managed-device netconf address v4-address
- no password strong-policy

**Defaults**
This command has no default settings.

**Command Modes**
Command and sub-command mode

**Examples**
This example shows how to delete a managed device.

```
root@nga-ucs.cisco.com# no managed-device netconf address 1.1.1.1
Successfully deleted managed-device 1.1.1.1.
root@nga-ucs.cisco.com#
```
**nslookup**

This command is used to resolve a hostname to an address. You must first provide a Domain Name Server (DNS) address to NGA via command `ip nameserver name-server-v4-address`. As an alternative, you could use a different DNS address from the command.

```
nslookup hostname [server]
```

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to perform name server queries:

```
root@nga-ucs.cisco.com# nslookup www.cisco.com
Name:   origin-www.cisco.com
Address: 198.133.219.25
root@nga-ucs.cisco.com#
```
password root
Use this command to change the CLI root user account password.

password root

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to change the password

root@nga-ucs.cisco.com# password root
Enter new password:
Confirm new password:
Successfully changed password for user 'root'
root@nga-ucs.cisco.com

password strong-policy
To enable strong password policy for user names, use the password strong-policy command. To disable this option, use the no form of this command. When password strong policy is enabled, root user account password must contain at least 3 of the 4 following:

- Lower case letters
- Upper case letters
- Digits
- Special characters

password strong-policy
no password strong-policy

Defaults
This command has no default settings.
**Command Modes**
Command mode

**Examples**
This example shows how to configure strong password enforcement policy:

```
root@localhost.cisco.com# password strong-policy
Strong password policy is enabled.
```
patch
To download and install a software patch, use the patch command.

```
patch ftp://user:passwd@host/full-path/filename
```

**Syntax Description**

- `ftp://user:passwd@host/full-path/filename`
  - Provides the full path of the patch file to be downloaded and installed. Note that you may omit the `user:passwd` portion of the URL if the FTP server supports anonymous login. Also, you may omit just the `passwd` portion, if you would prefer to be prompted for your password so it will not be echoed to the screen.

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

**Related Commands**

- show patches
- show version
ping
To check connectivity to a network device, use the ping command.

```
  ping [-n | -v] [-c count] [-i wait] [-p pattern] [-s packetsize] hostname | IP address
```

**Syntax Description**

- `-n` (Optional) Displays the network addresses as numbers.
- `-v` (Optional) Specifies verbose output.
- `-c count` (Optional) Stops the ping after sending the count of ECHO_REQUEST packets.
- `-i wait` (Optional) Specifies the time interval in seconds between sending each packet.
- `-p pattern` (Optional) Specifies the pad bytes to fill out packets sent in the ping. You may specify up to 16 pad bytes to fill out packets being sent.
- `-s packetsize` (Optional) Specifies the number of data bytes to be sent. The default is 56, which translates into 64 ICMP data bytes when combined with the 8 bytes of ICMP header data.

**Hostname**
Sets the hostname of the network device to ping.

**IP address**
Specifies the IP address of the network device to ping.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode
Examples
This example shows how to check the connectivity of a network device with ping:

root@localhost# ping -n -v ralph 100.20.19.23
root@localhost#
reboot
To shut down and then restart NGA, use the reboot command. By default, NGA will boot to its application image if there is not any interruption. You could boot NGA to its helper image by providing the option as in reboot –helper.

    reboot
    reboot –helper

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to reboot the NGA:

root@nga-ucs.cisco.com# reboot
Reboot the NGA? (Y/N) [N]: y
System reboot in process...

Broadcast message from root (pts/1) (Wed Apr 11 12:25:24 2012):

(more messages after this point. If you are not in console, you will be log out.)
rmwebusers

To remove the user from the local WEB user database, use the `rmwebusers` command. NGA supports only one WEB user. If the password of the WEB user is forgotten, use this command to delete the existing WEB user. The HTTP and/or HTTPS server will be disabled after the `rmwebusers` command. When the HTTP or HTTPS server is enabled (`ip http server enable` or `ip http secure server enable`), you will be prompt to enter the WEB user account name and password.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to remove web users from the local web user database:

```
root@nga-ucs.cisco.com# rmwebusers
WARNING: Doing this will stop the web server and remove all locally defined web users from web user database.
Are you sure you want to continue (y/n) [n]? y
Stopping httpd
All locally defined web users have been removed from web user database.

root@nga-ucs.cisco.com# ip http server enable
No web users are configured.
Please enter a web administrator user name [admin]:
New password:
Confirm password:
User admin added.
Enabling web server...
Successfully enabled web server.
root@nga-ucs.cisco.com#
```
Related Commands

- show ip
- ip http server enable
- ip http secure server enable
show

Show commands show what have been configured in the NGA system. There are many show commands. A few of them are for debugging purpose. A list of show commands follows:

- **show audit-trail**: This command shows the status of audit-trail
- **show cache statistics cumulative monitor-name**: This command is for troubleshooting. It shows stats information at the internal cache level. Flow information in the cache is derived from processing network traffic received at NGA data ports.
- **show cache statistics rates monitor-name**: This command is for troubleshooting. It shows flow stats information at the internal cache level with rate derived from the last minute.
- **show cdp settings**: This command shows CDP settings.
- **show clock details**: This command shows the local clock.
- **show collector statistics collector-name**: This command is for troubleshooting. It shows flow statistics at the flow collector level, both cumulative and last minute rates. This displays how many packets, flows, etc. have been sent to each collector.
- **show configuration**: This command shows the current configuration of the system.
- **show dataport statistics cumulative**: This command is for troubleshooting. It shows statistics at the data port level where network traffic arrives at NGA for processing.
- **show dataport statistics rates**: This command is for troubleshooting. It shows statistics at the data port level with rates computed for the last minute.
- **show dataport statistics rates queues**: This command is for troubleshooting. It shows how balanced packets are at each data port queues. In general, queues at the data ports should be fairly balanced for the best performance.
- **show date**: This command show the current date from the system clock.
- **show debug log-levels**: This command shows debug log level of all features. This command is primarily for troubleshooting.
- **show debug messages**: This command shows debug messages logged in the debug log file. The content of the debug log file is also included in the output of `show tech-support` command.

- **show exporter statistics exporter-name**: This command is for troubleshooting. It shows flow statistics at the flow exporter level. Flow exporter receives flow information from the internal cache.

- **show flow collector [collector-name]**: This command shows all flow collectors configured in the system. You may view a specific collector by providing the collector name.

- **show flow exporter [exporter-name]**: This command shows all flow exporters configured in the system. You may show a specific exporter by providing the exporter name at the end of the command.

- **show flow filter [filter-name]**: This command shows all flow filters configured in the system. You may view a specific filter by providing the filter name.

- **show flow monitor [monitor-name]**: This command shows all flow monitors configured in the system. You may view a specific monitor by providing the monitor name.

- **show flow record [record-name]**: This command shows all flow records configured in the system. You may view a specific flow record by providing the record name.

- **show flow sampling**: This command shows flow sampling settings configured in the system.

- **show inventory**: This command shows the product ID and serial number of NGA device.

- **show ip**: This command shows IP network settings.

- **show log config**: This command shows logging of configuration done via `config network ftp-url` command.

- **show log patch**: This command shows logging results from `patch` commands.

- **show log upgrade**: This command shows logging results from `upgrade` commands.

- **show login banner**: This command shows the login banner string configured in the system.

- **show managed-device**: This command shows all managed devices configured in the system.

- **show password strong-policy**: This command shows the status of password policy. A strong policy requires minimum certain combinations of characters in the password string.
- **show patches**: This command shows all patches that have been installed in the system.
- **show snmp**: This command shows SNMP settings in the system.
- **show tech-support**: This command is for troubleshooting. It gathers and generates all necessary configuration as well as logging information for support.
- **show time**: This command shows time sync and time zone settings configured in the system.
- **show version**: This command shows image version information.

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows all the flow collectors configured in the system:

```
root@NGA.cisco.com# show flow collector

Collector name: kluuQuickSetup_collector
Description:  
IP address: 172.20.98.171
DSCP value: 0
Transport: UDP
Port number: 3000

Collector name: example-collector
Description:  
IP address: 1.2.3.4
DSCP value: 0
Transport: UDP
Port number: 3000
```

root@nga-ucs.cisco.com#
**shutdown**
To shut down the Cisco NGA, use the **shutdown** command.

```
  shutdown
```

**Defaults**
This command has no default settings.

**Command Modes**
Command mode

**Examples**
This example shows how to shut down the appliance:

```
Root@localhost# shutdown
Shut down the NGA? (y/n) [n]: n
```

**Related Commands**
- exit
- logout
To configure Cisco NGA system MIB objects, use the `snmp` command.

```
  snmp community community-string { ro | rw }
  snmp delete community community-string
  snmp contact contact-string
  snmp location location-string
  snmp name name-string
```

**Syntax Description**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>`community community-string ro</td>
<td>rw`</td>
</tr>
<tr>
<td><code>delete community-string</code></td>
<td>Deletes a device community string.</td>
</tr>
<tr>
<td><code>contact contact-string</code></td>
<td>Sets the device’s contact string.</td>
</tr>
<tr>
<td><code>Location location-string</code></td>
<td>Sets the device’s location string.</td>
</tr>
<tr>
<td><code>name name-string</code></td>
<td>Sets the device’s name string.</td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to configure a read-only SNMP community string:

```
Root@localhost# snmp community public ro
```
Related Commands
Error! Reference source not found.
terminal
To set the number of lines per screen for your CLI session, use the terminal command.

    terminal editor [enable | disable]
    terminal length length
    terminal mode { 0 | 1}

Syntax Description

<table>
<thead>
<tr>
<th>Syntax</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>editor</td>
<td>(Optional) Enables or disables the NGA CLI command editing.</td>
</tr>
<tr>
<td>length</td>
<td>Sets the number of lines per screen for a session.</td>
</tr>
<tr>
<td>mode</td>
<td>Sets the terminal mode.</td>
</tr>
</tbody>
</table>

Defaults
This command has no default settings.

Command Modes
Command mode

Examples
This example shows how to set the number of lines on a session’s screen:

    root@localhost# terminal length 24
    Terminal length for this session set to 24.

Related Commands
config clear
time

To enter the time configuration subcommand mode, and then configure NGA system time settings, use the time command. NGA supports time sync via NTP or using the local clock only. Following are the subcommands:

- **sync ntp ntp-server**: Use this subcommand to sync NGA system time with NTP server. You could provide up to 2 NTP servers separated by a space.
- **sync local**: use this command to sync system time with the local clock.

  **Note** NGA could either sync its system time to local clock or NTP server, not both at the same time.

- **zone region [zone-name]**: Use this command to set the NGA time zone.
- **exit**: Use this command to apply the settings and exit the subcommand mode. You will be brought back to the command mode.
- **cancel**: Use this command to cancel the setting and exit the subcommand mode. You will be brought back to the command mode. Configuration does not change.

  **Note** Upon applying the settings via subcommand **exit**, A few internal processes will be restarted.

**Defaults**
This command has no default settings.

**Command Types**
Switch command

**Examples**
This example shows how to configure system time settings on the NGA to synchronize the time with an NTP server.

```
root@nga-ucs.cisco.com# time
```

Entering into subcommand mode for this command.
Type 'exit' to apply changes and come out of this mode.
Type 'cancel' to discard changes and come out of this mode.

root@nga-ucs.cisco.com(sub-time)# sync ntp 171.68.10.80
root@nga-ucs.cisco.com(sub-time)# zone US/Pacific
root@nga-ucs.cisco.com(sub-time)# exit
Stopping klogd . . .
Stopping syslogd . . .
Starting syslogd . . .
Starting klogd . . .
Restarting periodic command scheduler: cron.
Shutting down NGA monitor daemons
Shutting down watchdog
Stopping httpd
Shutting down RMON daemon
Starting NGA monitor daemons:
Starting RMON daemon
Starting netconfd
Starting watchdog
Starting httpd
Successfully updated NGA system time settings.

root@nga-ucs.cisco.com# show time
NGA synchronize time to: NTP
NTP server1: 171.68.10.80
NGA time zone: US/Pacific

Related Commands

Error! Reference source not found.
traceroute
To trace the route to a network device, use the traceroute command.

```
traceroute [-I | n | v] [-f first_ttl] [-m max_ttl] [-p port] [-s src_addr] [-t tos] [-w waittime] destination host name | IP address [packetlen]
```

**Syntax Description**

- **-I** (Optional) Specifies that ICMP ECHO is used instead of UDP datagrams.
- **-n** (Optional) Prints hop addresses numerically.
- **-v** (Optional) Sets the output to verbose.
- **-f first_ttl** (Optional) Sets the initial time-to-live used in the first outgoing packet.
- **-m max_ttl** (Optional) Sets the maximum time-to-live (max number of hops) used.
- **-p port** (Optional) Sets the base UDP port number used in probes.
- **-s src_addr** (Optional) Forces the source address to be an address other than the IP address of the interface the packet is sent on.
- **-t tos** (Optional) Sets the type-of-service in packets to the following value.
- **-w waittime** (Optional) Sets the time (in seconds) to wait for a response to a probe.

**destination** Sets the packet destination.

**host** Sets the host.

**name** Sets the hostname.

**IP address** Sets the IP address.

**packetlen** (Optional) Set the length of the packet.

**Defaults**
This command has no default settings.
**Command Modes**

Command mode

**Examples**

This example shows how to trace a route to a network device:

```
root@nga-ucs.cisco.com# traceroute 172.20.98.174
traceroute to 172.20.98.174 (172.20.98.174), 30 hops max, 46 byte packets
1  172.20.103.1 (172.20.103.1)  0.370 ms  0.251 ms  0.228 ms
2  nlab-125-dist-96 (172.20.96.3)  0.451 ms  0.322 ms  0.321 ms
3  namlab-tb (172.20.57.2)  3.557 ms  1.410 ms  2.014 ms
4  namlab-pc7 (172.20.98.174)  0.419 ms  0.380 ms  0.388 ms
root@nga-ucs.cisco.com#
```
**upgrade**

To download and install a new application image on the NGA, use the **upgrade** command.

```
upgrade ftp://user:passwd@host/full-path/filename
```

This command is the easiest way to upgrade application image on NGA. Upon entering the command, NGA will be automatically rebooted twice: the first time to its helper image, and the second time back to the new application image. If disk reformat is desired, you need to boot the NGA to its helper image (command **reboot –helper**), and use helper menu item 2 to install the application.

<table>
<thead>
<tr>
<th>Syntax Description</th>
<th>Provides the full path of the image file to be downloaded and installed. Note that you may omit the <code>user:passwd</code> portion of the URL if the FTP server supports anonymous login. Also, you may omit just the <code>passwd</code> portion, if you would prefer to be prompted for your password so it will not be echoed to the screen.</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>ftp://user:passwd@host/full-path/filename</code></td>
<td></td>
</tr>
</tbody>
</table>

**Defaults**

This command has no default settings.

**Command Modes**

Command mode

**Examples**

This example shows how to download and install a new image:

```
Root@localhost# upgrade ftp://<username>@1.1.1.1/<path>/<image-name>
```

Root@localhost#
Related Commands
Error! Reference source not found.
Error! Reference source not found.