Cisco NetFlow Generation Appliance (NGA) User Guide

3140

May 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-26030-01

CONTENTS

About This Guide

This guide describes how to use Cisco NetFlow Generation Appliance. This preface has the following sections:

Audience

This guide is designed for network administrators who are responsible for setting up and configuring the software to monitor NetFlow traffic. As a network administrator, you should be familiar with:

- Basic concepts and terminology used in internetworking.
- Network topology and protocols.
- Basic UNIX commands or basic Windows operations.
- Configuring NetFlow for your Nexus devices and collectors.

Conventions

This document uses the following conventions:

Item	Convention
Commands and keywords	**boldface** font
Variables for which you supply values	*italic* font
Displayed session and system information	`screen` font
Information you enter	**`boldface screen`** `font`
Variables you enter	*`italic screen`* font
Menu items and button names	**boldface** font
Selecting a menu item in paragraphs	**Option > Network Preferences**
Selecting a menu item in tables	Option > Network Preferences

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.

Notices

The *Third Party and Open Source Copyright Notices for Cisco NetFlow Generation Appliance* contains the licenses and notices for open source software used in this product. The appliance includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/). This document is available on www.cisco.com in the technical documentation/support section.

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:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.

CHAPTER 1

Introducing Cisco NetFlow Generation Appliance

The Cisco NetFlow Generation Appliance (NGA) complements best-in-class switching platforms and off loads the NetFlow generation function. It receives packets from up to four 10-Gigabit ports and exports NetFlow data to up to six collectors in NetFlow version 5, 9, and IPFIX format.

You can deploy Cisco NGA at key observation places such as server access layer, fabric path domains, and internet exchange points to help simplify operational manageability. Simple to set up and easy to configure, the appliance is based on the UCS C200 server, so you can specify your specific configuration as needed. To set up your appliance, connect it to your switch devices and collectors, and set up a minimum set of flow components.

You can configure Cisco NGA using the lightweight graphical user interface or a more detailed command line interface.

This chapter contains:

For details on how to use the CLI, see the *Command Reference Guide for Cisco NetFlow Generation Appliance* on Cisco.com.

Key Features

Table 1-1 details the key features of Cisco NetFlow Generation Appliance.

Table 1-1 Key Features

Feature	Function	Benefit
Purpose-built, high-performance form factor	Throughput rate of 32+ Gbps, 64 million simultaneous flows, and more than 10 million new flows per minute.	• Improve performance of forwarding devices by offloading NetFlow generation function. • 100% accuracy with full flow visibility • Cost-effective application and traffic visibility in high-throughput ten-Gigabit networks. • Hop-by-hop flow visibility across multiple network segments.
Four 10G monitoring interfaces, up to four independent flow caches and flow monitors.	Various combinations of data ports, record templates, and export parameters can be associated with each independent flow monitor.	• Independently collected packet streams from up to four switches or tap locations. • Configure different templates, cache, and export parameters for each monitored packet stream.
SPAN and network tap support	Use your switch SPAN function or hardware Ethernet tap to gain access to traffic at various strategic deployment points.	• Improved return on investment (ROI) with flexible deployment choices. • Introduce NetFlow into any environment where it was previously unavailable or impractical.
Multiple collectors (up to six)	Flow replication or weighted round robin to load balance among multiple collectors.	• Efficient use of NetFlow information across multiple management applications for monitoring, troubleshooting, capacity planning, and security. • Avoid overloading any single collector at high traffic and flow rates.
Advanced filters for custom export	Filter on any combination of fields to tailor the data flow for the particular collector application.	• Reduce load on collectors and focus on the most important servers and traffic. • Tailor the flow data for particular types of management applications.
Application awareness	Traffic classification and packet inspection to determine the application associated with each flow.	• Enhanced application recognition; the Cisco NGA recognizes applications on the basis of port, port ranges, and built-in heuristics.

Table 1-1 Key Features (continued)

Feature	Function	Benefit
Embedded GUI and command-line interface (CLI)	Simple embedded web server and command parser for configuration.	• Easy and rapid configuration and deployment. • Reduce learning curve and improve productivity.
NetFlow Data Export (NDE) using version 5, version 9, and/or IPFIX.	Export data in all of the commonly used NetFlow formats.	• Easily integrate with any standard NetFlow collector, including Cisco Prime Assurance Manager and Cisco Prime Network Analysis Module.

Understand the User Interface and Command Line

If you are familiar with advanced features of NetFlow and the use of a command line interface (CLI), you can configure the software using the CLI. For a comparison of what differences exist between the CLI and the user interface, see Table 1-2, "Feature Comparison."

All tasks that are in the graphical user interface can also be completed by using the command line interface (CLI). For example:

- Configuration—Exporter, Monitor, Record, Destination, and Filter.
- Show Commands—Exporter, Monitor, Record, Destination, and Filter.

To view a list of the commands, see the *Command Reference Guide for Cisco NetFlow Generation Appliance*.

Table 1-2 Feature Comparison

Feature	User Interface	Command Line
Manage Device	X	X
Quick Setup of multiple components simultaneously	X	Must configure individual components separately.
Advanced Setup for multiple components	X	X
Filtering	X[1]	X
Administrative Tasks	X	X
Display status and counters		X
Upgrading application software image		X

1. Using Advanced Setup user interface only.

Configuration Overview

Configure the Cisco NetFlow Generation Appliance using the basic workflow in Table 1-3 on page 1-4. You can choose the path you want to take to configure your flow components. This user guide contains quick and advanced workflows and explains why to use each workflow.

- If you decide to configure a single set of flow components quickly using one user interface window, use the Quick Setup. The Quick Setup configuration is described in Chapter 2, "Getting Started" or in the *Quick Start Guide for Cisco NetFlow Generation Appliance*.
- To configure multiple components and set up filters and record parameters, use the Advanced Setup (see Configure Filters, page 3-3).
- To verify that packets are being received at the Cisco NGA data ports, NIC cards, exporters, or collectors, see Verify Flow Records Generated, page 4-1.
- And finally, to configure the Cisco NGA, as well as view system and diagnostic details, use the Administration menus (see Access System Parameters or Diagnostics, page 4-2).

Table 1-3 leads you through the basic configuration steps. These are not necessarily in the order in which you need to perform them. All tasks are required unless designated optional.

Table 1-3 Configuration Overview

Action	Description	Where to Find It?	Comments
Install Cisco NetFlow Generation Appliance (NGA)	Install and connect the Cisco NGA.	See the *Quick Start Guide for Cisco NetFlow Generation Appliance*.	
Configure your switch or router to forward traffic to Cisco NGA	To replicate packets from the switch or router to Cisco NGA, you must configure one of the following: • A Switched Port Analyzer (SPAN) session. • A network tap to replicate a source of packets and send those packets to the appliance.	Action required using switch or router CLI.	See your switch or router user documentation for details on how to configure SPAN or use a network tap.
System administration (Required and optional tasks)	Configure the current system time and SNMP community strings, as well as view current system network parameters (required) and access diagnostic details to assist with troubleshooting (optional).	**Administration > System** • **Resources** • **Network Parameters** • **SNMP Agent** • **System Time** **Administration > Diagnostics** • **Audit Trail** • **Tech Support**	See Access System Parameters or Diagnostics, page 4-2.
Configure the Cisco NetFlow Generation Appliance	Configure Cisco NGA flow components. Configure and activate flow monitor(s) on one or more of the appliance data ports.	**Setup > NetFlow > Quick Setup** **Setup > NetFlow > Advanced Setup**	For Quick Setup, see Configure a Single Set of Components Quickly, page 2-5. For Advanced Setup, see Setting Up Multiple NetFlow Monitor Instances, page 3-1.

Table 1-3 Configuration Overview

Action	Description	Where to Find It?	Comments
Configure the managed device (Optional, for Nexus 5000 and Nexus 7000 Series switches only)	Configure your switch as a managed device so that Cisco NGA uses the switch's interface index values when exporting records.	**Setup > NetFlow > Managed Devices** CLI command: **managed-device**	See Configure Your Traffic Sources, page 2-4.
Verify traffic activity	Verify that packets are being received at the Cisco NGA data ports, NIC cards, exporters, or collectors.	For example, CLI commands: **show dataport statistics cumulative** **show dataport statistics rates**	See Chapter 4, "Verify Flow Records Generated." Detailed command information is not available in the user interface. For commands, see the *Command Reference Guide for Cisco NetFlow Generation Appliance* on Cisco.com.

CHAPTER 2

Getting Started

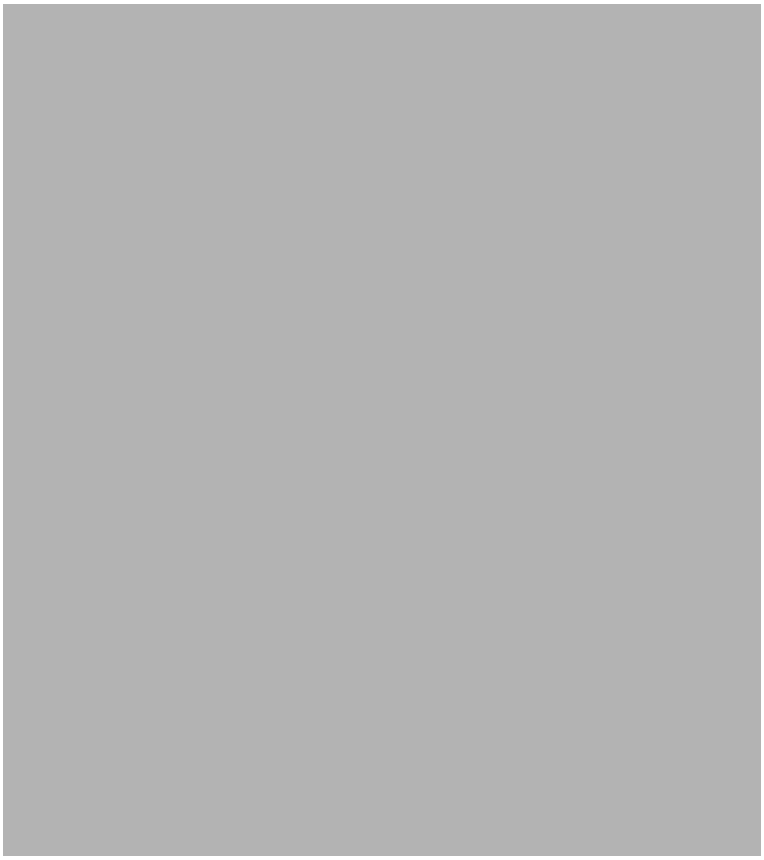
This chapter covers the post-installation configuration of a single NetFlow monitor instance (monitor, exporter, and collector) on one instead of multiple web pages that Cisco NetFlow Generation Appliance uses to export traffic data. Use this chapter to quickly get started with flow component setup. You can set up a single NetFlow monitor instance using the details in this chapter, then move to the next chapter to configure more advanced configurations such as multiple components, filters, and v9 and IPFIX records.

This chapter contains the following sections:

Understand What to Configure

Figure 2-1 depicts an overview of what you need to do to configure a single NetFlow monitor instance on the Cisco NGA using Quick Setup. The flowchart contains links to the various sections in this guide that instruct you on what steps to perform.

Figure 2-1 Quick Start Workflow Overview



The overview steps are described in more details below:

- To set up and log into Cisco NetFlow Generation Appliance (NGA) user interface, follow the steps in the *Quick Start Guide for Cisco NetFlow Generation Appliance.*
- You must configure your traffic sources so that they will forward traffic information to the Cisco NGA. You can optionally configure the IP address of your traffic sources as managed devices in the appliance. For more details, see Configure Your Traffic Sources, page 2-4.
- Configure Cisco NGA flow components. At a minimum, your configuration must include a collector, an exporter, and a monitor. To quickly configure all of these components using one instead of multiple web pages, use the Quick Setup graphical user interface (GUI). For details, see Configure a Single Set of Components Quickly, page 2-5.

  The grey flowchart task in Figure 2-1 indicates that even though you can go directly to the Advanced Setup UI to configure multiple flow components, it is not the quickest way to complete your configuration. To go directly to an overview on how to configure additional components or how to set up multiple components using the GUI, see Advanced Configuration Overview, page 3-1.

- To check your flow component configuration once your configuration is complete, you should verify that flow records are being sent to their destination (see Verify Flow Records Generated, page 4-1).
- To complete your Cisco NGA configuration, you should set your SNMP Agent and system time (see Access System Parameters or Diagnostics, page 4-2).

If you prefer to use the command line to perform set up or configuration tasks on the appliance, see the *Command Reference Guide for Cisco NetFlow Generation Appliance*.

Log In

To log into Cisco NetFlow Generation Appliance from the user interface, open a supported browser and enter the URL: *http://<NetFlow_Gen_IP_address>* or *https://<NetFlow_Gen_IP_address>*.

If you are having problems logging in, do the following:

- Ensure Cisco NGA is configured with an IP address and that ping can be used to reach it from a workstation.
- Use a supported browser that has the appropriate options enabled. See the installation documentation for information on what browsers are supported.
- Clear the browser cache and restart the browser.

To view the full documentation set (including the User Guide and Release Notes) for the software, choose **Network Management and Automation > Switch and Router Management > Cisco NetFlow Generation Appliance** in the Support Technical Documentation area on Cisco.com.

Set System Parameters

Before you begin to configure your traffic sources and flow components, you must set up these system parameters which are required for Cisco NetFlow Generation Appliance.

Procedure

Step 1 Select **Administration > System** to view or configure the following system parameters:

- **Network Parameters**—Allows you to reconfigure the system network parameters including IP address, IP broadcast, subnet mask, IP gateway, hostname, domain name, and optional nameservers. The initial information is prepopulated based on your installation responses.
- **SNMP Agent**—Display and configure the System Group and community strings for the appliance SNMP Agent. Your collectors may use SNMP to poll Cisco NGA, so these community strings are required.
- **System Time**—Synchronize the software clock using a local or a Network Time Protocol (NTP) time server. You must synchronize your clock before use. If you choose **Local**, you must enter the local Region and Zone. If you choose **NTP**, you must enter the NTP Server IP address. Setting the system time ensures accurate time stamps.

For more details on how to configure these parameters, see Set Cisco NGA System Parameters, page 4-2.

Configure Your Traffic Sources

There are two tasks to configuring your traffic sources. The traffic source in Cisco NetFlow Generation Appliance is either a switch or router. The first task is required; the second task is optional.

Perform these tasks to set up your traffic sources, for example a Nexus 5000 or Nexus 7000 Series switch.

1. (Required) Create a Switched Port Analyzer (SPAN) session (also known as port mirroring) on your switch or router using the Nexus supervisor command line interface, or use a tap device to forward traffic to your Cisco NGA. Port mirroring selects network traffic for analysis by a network analyzer.

   Ensure that your traffic sources are connected to the data ports on the appliance with the appropriate 10-Gb Ethernet cable. This guide does not provide details on how to create SPAN sessions or to use a network tap device. See your device documentation for details on how to set up these configurations.

2. (Optional) Configure the IP address of your traffic source in Cisco NGA as a managed device.

   If your traffic source is a Nexus 5000 or Nexus 7000 Series switch and you want the appliance to export flow records with the input and output interface of the device rather than dataport interface index on the appliance, you need to configure the IP address and login credentials of your traffic source as a managed device. For details, see Configure the IP Address of Your Traffic Source, page 2-4.

Configure the IP Address of Your Traffic Source

One of the benefits of configuring the IP address of your Cisco Nexus 5000 or Nexus 7000 Series switches is that when your switch is configured as a managed device, Cisco NetFlow Generation Appliance uses the switch's interface index values when exporting records. This allows you more visibility into the collected data. This is an optional task.

Ensure that your traffic sources are connected to the data ports on the Cisco NGA with the appropriate 10Gb Ethernet cable.

To add, edit, or delete managed devices:

Procedure

Step 1 To configure up to four Nexus 7000 or 5000 Series devices as managed devices in Cisco NGA, choose **Setup > NetFlow > Managed Devices**.

Step 2 Choose one of the following tasks:

- To add managed devices, click **Create** and enter the required information in the Create Managed Device window. See Table 2-1 for field descriptions.
- To edit an existing managed device, select the row, click **Edit**. and enter the device information.
- To delete a managed device, select the row and click **Delete**.

Table 2-1 Managed Devices Table Field Descriptions

Field	Field Description
Address	Device IP address. Use address and not domain name.
Username/Password Verify Password	Enter the managed device (switch) access credentials.
Data Ports	Enter the appliance data ports that are connected to the managed device (for example, the Nexus 5000 or Nexus 7000 Series device) as SPAN destinations. These ports will receive replicated packets for monitoring. Any combination of data ports may be connected to the same managed device. If you connect the appliance to multiple Nexus 5000 or Nexus 7000 Series switches, ensure you define a separate managed device for each switch that specifies the correct data ports that the switch connects to on the appliance.

You can configure up to four managed devices. For each managed device, you can specify which set of data ports are attached to it. Once a data port is assigned to one managed device, you cannot assign it to another managed device.

Step 3 Once you configure the managed device or devices, to configure your Cisco NGA flow components choose **Setup > NetFlow > Quick Setup** or **Setup > NetFlow > Advanced Setup**.

We recommend using the Quick Setup to configure your initial NetFlow monitor instance, then use Advanced Setup if you require additional components or filters. (See Configure a Single Set of Components Quickly, page 2-5 or Advanced Configuration Overview, page 3-1.)

Configure a Single Set of Components Quickly

Cisco NetFlow Generation Appliance requires both hardware and software configuration so that its software can monitor traffic and forward NetFlow records to NetFlow collectors and other consumers that you specify.

To quickly configure a single NetFlow monitor instance to export version 5 or 9 NetFlow Data Export packets from Cisco NGA, use the Quick Setup pane. You can use this interface to configure export to a single collector with no filters.

To configure an environment that requires filters, IPV6 or Layer 2 records, or multiple components, see Configure Filters, page 3-3.

You can also use the command line interface (CLI) to configure the appliance. See the *Command Reference Guide for Cisco NetFlow Generation Appliance* for details.

Once set, you can modify existing configurations using the Advanced Setup user interface.

Before You Begin

You must complete the hardware setup steps in the *Quick Start Guide for Cisco NetFlow Generation Appliance* document before you configure the appliance.

To configure a single NetFlow monitor instance quickly using a single window, the Quick Setup pane:

Procedure

Step 1 To configure Cisco NetFlow Generation Appliance for NetFlow Data Export version 5 or 9, enter the required information in the Quick Setup pane. See Table 2-2 for field descriptions.

Table 2-2 Quick Setup Pane Field Descriptions

Field	Field Description	
Name	Enter a unique name to identify this configuration. Use up to 54 alpha-numeric characters for this field. You can also use the dash (-) or underscore (_).	
Data Port	Check the check box for each appliance data port that will accept incoming packets.	
Collector Address	Enter the IP address for the collector.	
Collector Port (UDP)	Enter the port on which the collector device is listening. This is typically configurable on the collector device. This is a critical step. See your collector device user documentation for configuration details. Ensure the data port configured matches this port number. (for example, UDP port 3000).	
NetFlow Version	Select V5 or V9.[1]	
	V5	Select version 5 to configure the appliance to perform standard NetFlow version 5 monitoring and export. You do not need to select individual record fields since they are predetermined by the NetFlow version 5 standard.
	V9	Select which version 9 fields you want to include in your monitoring/collecting. See Table B-1 on page B-1 for match and collect field descriptions.

1. Quick Setup pane allows configuration for IPv4 records only. To configure IPv6 or Layer 2 records, you must use the Advanced Setup tab or the CLI.

Step 2 Click **Submit**.

The following components are created:

For V5:	For V9:
A collector named *name_collector*	A collector named *name_collector*
An exporter named *name_exporter*	An exporter named *name_exporter*
A monitor named *name_monitor*	A monitor named *name_monitor*
	A record named *name_record*

The Monitor tab appears displaying the newly added *name_monitor*.

Step 3 Select *name_monitor* in the **Monitor** tab and click **Activate/Inactivate** to enable this flow monitor to generate NetFlow information to the collector.

Step 4 To verify flow records have reached their destination, check the collector data by entering both of the following commands:

- **show cache statistics rates** ***monitor_name*** command. Counters begin to increment only after a minute has passed. This command displays the rate of raw traffic being processed and the number of flows being created and forwarded to the exporter engine.
- **show collector statistics** ***collector_name*** command. This displays the information about NetFlow packets being sent to the collector.

You can now add more flow components, add filters or define flow records for IPv6 or Layer 2. See Setting Up Multiple NetFlow Monitor Instances, page 3-1.

CHAPTER 3

Setting Up Multiple NetFlow Monitor Instances

Cisco NetFlow Generation Appliance (NGA) software contains two separate user interfaces that allow you to quickly set up a single NetFlow monitor instance from one window or configure multiple flow monitor instances using several windows, manually associating the components.

This chapter describes how to configure your multiple flow components and associate them to each other in order to allow Cisco NGA to export NetFlow packet information to your collectors.

This chapter contains the following sections:

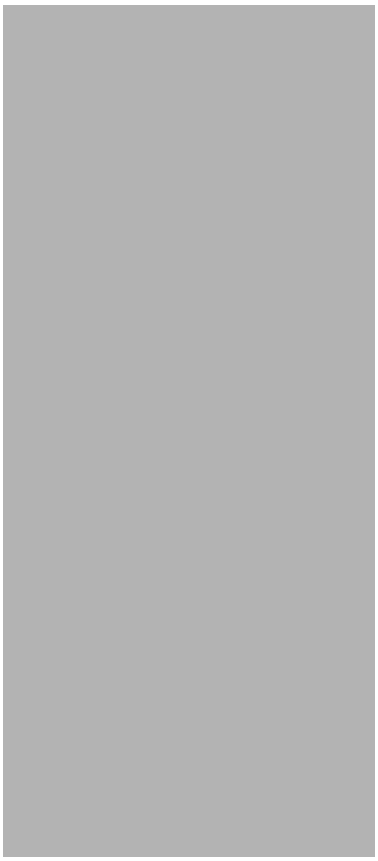
Once the flow component configuration is complete, you should verify that the collectors are receiving the data as well as configure your system parameters.

Advanced Configuration Overview

You must complete the steps in the “Prepare and Install the Cisco NetFlow Generation Appliance” section of the *Quick Start Guide for Cisco NetFlow Generation Appliance* document before you configure Cisco NGA.

Use Figure 3-1 to provide a visual guide to the workflow required to configure Cisco NGA.

Figure 3-1 Configuring Multiple Components Workflow Overview



The complete description of all the tasks required in the appliance configuration are described in Understand What to Configure, page 2-2.

If you want to create more than one instance of a flow monitor or other flow components, you can do so manually using the Advanced Setup UI. Some of the other benefits to using the Advanced Setup UI include creating:

- Up to ten filters—To define which flows are sent to certain collectors. This allows you to use your collector's analysis applications and load balance NetFlow data across collectors.
- Up to four managed devices—To allow you to off load NetFlow data from your Nexus 5000 and 7000 Series switches.
- Up to six collectors—To enable you to load balance NetFlow data export and monitor specific applications in your network.
- Up to four monitors—Up to four independent flow monitors may be active simultaneously. Each monitor supports up to three records. Of those three records, only one IPv4, one IPv6, and one Layer2 record type is supported.

You must also complete the order of component configuration as specified in Understand the Advanced Component Configuration Order, page 3-3. Once you have completed your advanced configuration tasks, remember to verify the exported flow on your collectors and ensure you set up your system parameters,

Understand the Advanced Component Configuration Order

Use the following sequence to configure your flow components. Note that the configuration order matches the order of the tasks located in this guide:

1. Optionally define one or more filters. See Configure Filters, page 3-3.
2. Define one or more collectors. See Configure Collectors, page 3-4.
3. Optionally define one or more records. See Configure Records, page 3-4.
4. Define a flow exporter and associate the collector(s) with it. If you wish to use a v9 or IPFIX exporter, you must also first define one or more records to be used with it, prior to defining a flow exporter. See Configure Exporters, page 3-5.
5. Define a flow monitor and associate the exporter with it. See Configure and Activate Monitors, page 3-6.
6. Activate the flow monitor. See Configure and Activate Monitors, page 3-6.

Configure Filters

You can apply filters globally to a particular exporter, which could have more than one collector. Filter rules in exporter level affect all its collectors.

Cisco NetFlow Generation Appliance is a high-performance device capable of exporting hundreds of thousands of flow records per second. Third-party flow collectors may be unable to process this rate of data and become unresponsive, drop records, or both. In this case, you can use filters to reduce the demand on the collector.

Creating filters is optional, but should be in place before defining collectors and exporters.

You can apply filters to individual collectors in an exporter. You can also apply filters globally to an exporter, and they will apply to all collectors within that exporter.

To define optional filters and describe which flows should be accepted and exported to the collectors:

Procedure

Step 1 Select **Setup > NetFlow > Advanced Setup**.

Step 2 Select the **Filter** tab.

Step 3 Choose one of the following tasks:

- Click **Create** to add a new filter. Continue to step 4.
- Select a row and click **Edit** to change an existing filter.
- Select a row and click **Delete** to remove an existing filter.

Step 4 Enter the information in the Configure Filter window (see Table B-2 on page B-2 for details).

Step 5 Click **Submit**.

Continue to the Collectors tab to configure the flow collector component. See Configure Collectors, page 3-4.

Configure Collectors

Collectors receive flow records from Cisco NGA and interprets those records. Typical collectors summarize and aggregate the data based on user-defined criteria, and store the data in a database or other long-term repository. Collectors typically generate various reports and charts based upon data received over time from the appliance. See your particular collector's user guide for a description of its capabilities and how to use it.

This section describes the steps required to define one or more collectors and allow the appliance to transmit flow records to them.

Before You Begin

Configure a SPAN session or TAP device to one of the collector data ports. This enables the appliance to receive network traffic.

To add one or more collectors to your NetFlow environment:

Procedure

Step 1 Select **Setup > NetFlow > Advanced Setup**.

Step 2 Select the **Collector** tab.

Step 3 Choose one of the following tasks:

- Click **Create** to add a new collector. Continue to step 4.
- Select a row and click **Edit** to change an existing collector.
- Select a row and click **Delete** to remove an existing collector.

Step 4 Enter the following information in the Configure Collector window (see Table B-4 on page B-4 for details).

Step 5 Click **Submit**.

Continue to the Records tab to configure the flow record component. See Configure Records, page 3-4.

Configure Records

A flow record is the basic unit of information exported by the Cisco NetFlow Generation Appliance to collectors. Each flow record describes a sequence of packets sent from one host to another host which is monitored at one of the appliance data ports.

The flow record consists of a set of match fields and a set of collect fields. The match fields are keys which are used to uniquely distinguish different flows from each other. They do not change for the entire lifetime of the flow. Typical examples of match fields are source and destination IP addresses, since it is important to keep separate statistics for different IP addresses.

The collect fields are the statistics that are accumulated and reported once the flow has been selected by the match fields. Typical examples of collect fields are packet count and byte count. These fields are not useful for distinguishing unique flows from each other, but instead provide the desired information to be tracked for each flow.

The value of the collect fields change throughout the lifetime of a flow. For example, we expect the packet count field to continually increase during the life of a flow until that flow is expired and flushed.

If you are using NetFlow version 5, you do not need to explicitly define your own records. The NetFlow version 5 standard defines all the match and collect fields and permits no variation.

NetFlow version 9 and IPFIX, on the other hand, are considered forms of flexible NetFlow. The match and collect fields are not predefined, so you can customize these fields within certain restrictions. The primary restriction is that each individual field may only be used either as a match field or a collect field. For example, the source IP address may only be used as a match field, never as a collect field. Similarly, the packet count may only be used as a collect field and not a match field. For more details on filter field options, see The window field description tables for the following are included in this section:, page B-1.

To define a record when using flexible NetFlow such as version 9 or IPFIX:

Procedure

Step 1 Select **Setup > NetFlow > Advanced Setup**.

Step 2 Select the **Record** tab.

Step 3 Choose one of the following tasks:

- Click **Create** to add a new record. Continue to step 4.
- Select a record and click **Edit** to change an existing record.
- Select a record and click **Delete.**

Step 4 Enter the required information (see Table B-3 on page B-3 for details).

Step 5 Click **Submit**.

Continue to the Exporter tab to configure the exporter flow component. See Configure Exporters, page 3-5.

Configure Exporters

The exporter configuration defines a group of one or more collectors, the load-balancing policy to be used with multiple collectors, and allows filters to limit which flows are sent to which collectors. An exporter is a required configuration item for the Cisco NGA to function.

An exporter must be defined prior to creating a monitor. If the exporter is configured with v9 or IPFIX, at least one record must be defined.

To configure exporters:

Procedure

Step 1 Use **Setup > NetFlow > Advanced Setup > Exporter** to configure your exporters.

Step 2 Enter the required information in the Configure Exporter window (see Table B-5 on page B-5 for details).

Step 3 Click **Submit**.

Note You can use the same collector in more than one exporter.

Continue to the Monitor tab to configure the monitor flow component. See Configure and Activate Monitors, page 3-6.

Configure and Activate Monitors

A flow monitor represents one instance of the complete functionality of the Cisco NGA. You must create at least one active flow monitor so that the appliance can export NetFlow records. Up to four independent flow monitors may be active simultaneously.

A monitor supports up to three records. Of those three records, only one IPv4, one IPv6, and one Layer2 record type is supported.

Before You Begin

Before you can activate a flow monitor, you must ensure the other components have been successfully configured. See Understand the Advanced Component Configuration Order before you activate your monitor.

To create, edit, delete and make a flow monitor active or inactive:

Procedure

Step 1 Select **Setup > NetFlow > Advanced Setup**.

Step 2 Select the **Monitor** tab.

Step 3 Choose one of the following tasks:

- Click **Create** to add a new monitor. Continue to step 4.
- Select a row and click **Edit** to change an existing monitor.
- Select a row and click **Delete** to remove an existing monitor.

Step 4 Enter the required information in the Configure Monitor window (see Table B-6 on page B-5 for details).

Step 5 Click **Submit**.

Step 6 Choose the monitor name you want to make active or inactive and click **Activate/Inactivate**. For more details, see Activate/Inactivate Monitors, page 3-7.

Continue to the next step, to verify that the collector data is successful (see Verify Flow Records Generated, page 4-1).

Activate/Inactivate Monitors

You must activate a monitor to start exporting records. and at most four monitors may be active at the same time. If you already have four active monitors and want to make another monitor active, you must choose a monitor that is already active to inactivate it, then click the **Activate/Inactivate** button to allow the cache memory resources to be freed for use.

When a monitor is in Active state, configuration of all components that are being used by the monitor cannot be modified. To modify, you must first inactivate the monitor.

CHAPTER 4

Performing Administrative and Maintenance Tasks

Cisco NetFlow Generation Appliance (NGA) contains several administrative and maintenance tasks. The graphical user interface (GUI) also provides some diagnostics tools for you to collect or view system data.

This chapter contains information on the following administrative and maintenance tasks including:

Once you complete the setup, configuration, and administrative tasks you may leave the Cisco NGA to its monitoring duties and view and analyze your data from the collectors.

Verify Flow Records Generated

After you complete Cisco NetFlow Generation Appliance configuration tasks described in the previous chapters, you should verify that the configurations you made are successful.

To verify flow records are being sent to their destination, check the collector data by entering both of the following commands at the appliance command line interface (CLI):

- **show cache statistics rates** ***monitor_name*** command. Counters begin to increment only after a minute has passed. This command displays the rate of raw traffic being processed and the rate of flows being created and forwarded to the export engine.
- **show collector statistics** ***collector_name*** command. This displays the information about NetFlow packets being sent to the collector.

After you successfully verify your collectors are receiving data, you can periodically check audit trail or collect troubleshooting information as needed.

Access System Parameters or Diagnostics

To set your network parameters, SNMP Agent, and system time, use the Administration menu. You can also get details about several system preferences and view diagnostic details about Cisco NGA. Table 4-1 contains detailed descriptions of the tasks you can perform. All tasks are required, unless otherwise noted.

Table 4-1 Administrative Tasks

Tasks	Benefit
Resources—Displays an overview of the system, including CPU and memory utilization. (Optional)	Gives you insight into the appliance system load details.
Network Parameters—Display and configure the network parameters such as IP Address.	Enables you to check that you have parameters set correctly.
SNMP Agent—Display and configure the System Group and community strings for the server SNMP agent.	Some collectors will use SNMP to poll MIB variables on the appliance. This page allows you to synchronize the community string on the appliance with your collector or collectors to allow this SNMP communication. See SNMP Agent, page 4-3.
System Time—Configure server system time to use either the local server clock or synchronize with up to two external NTP servers.	Allows the system to generate accurate timestamps for diagnostic log messages and audit trail events. See System Time, page 4-3.
Audit Trail—Displays a listing of recent critical CLI activities from a syslog log file. (Optional)	Provides visibility into user login and configuration activity.
Tech Support—Provides troubleshooting information (similar to the **show tech** command). (Optional)	For troubleshooting purposes, this page allows you to view and download support data into a zip file. Should you need technical support for the product you may be asked to use your browser to download this file and send it to a Cisco support representative.

Set Cisco NGA System Parameters

There are three system administrative tasks you must perform to ensure Cisco NGA performs successfully. These settings should be in place before NetFlow generation takes place. Use the **Administration > System** menu to configure, reconfigure, or view these settings:

- Network Parameters, page 4-2
- SNMP Agent, page 4-3
- System Time, page 4-3

Network Parameters

The initial Network Parameter information is prepopulated based on your responses during the installation. If you must reconfigure the system network parameters, you can do so from this window.

SNMP Agent

An SNMP Agent is a network management software module that resides in a device, in this case, Cisco NetFlow Generation Appliance. It has local knowledge of management information and translates that information into a form compatible with SNMP.

The SNMP Agent on the Cisco NGA allows the collectors or other applications to use SNMP and a community string to send SNMP get and set requests to the appliance.You can manage the appliance with SNMPv2 and SNMPv1.

For security purposes, the community string is associated with the Cisco NGA IP address only, and no other SNMP application can use this community string to communicate with the appliance. For more information about community strings, see Working with Cisco NGA Community Strings, page 4-3.

Also, to further alleviate any security concerns, the SNMP exchanges between Cisco NGA and the collectors take place on an internal backplane bus. These SNMP packets are not visible on any network, nor any interface outside of the appliance. It is a completely secure out-of-band channel inside the appliance.

Working with Cisco NGA Community Strings

You use community strings so that other applications, such as collectors, can send SNMP get and set requests to the Cisco NGA, set up collections, poll data, and so on.

To create the Cisco NGA community strings:

Procedure

Step 1 Select **Administration > System > SNMP Agent**.

At the bottom of the window, the Community Strings Dialog Box displays.

Step 2 Click **Create**.

The SNMP Agent Dialog Box displays.

Step 3 Enter the community string (use a meaningful name).

Step 4 Enter the community string again in the Verify Community field.

Step 5 Assign read-only or read-write permissions using the following criteria:

- Read-only allows only read access to SNMP MIB variables (get).
- Read-write allows full read and write access to SNMP MIB variables (get and set).

Step 6 Do one of the following:

- To make the changes, click **Submit**.
- To cancel, click **Cancel**.
- To clear the fields, click **Reset**.

System Time

Synchronizes the software clock using a local or a Network Time Protocol (NTP) time server. If you choose **Local**, you must enter the appliance Region and Zone. If you choose **NTP**, you must enter a NTP Server IP address. You can enter up to two NTP server IP addresses (a primary and secondary).

Access Diagnostics Tools

There are two diagnostic tools you can use to collect diagnostic information from Cisco NGA. Use the **Administration > System** menu to access these tasks:

- Audit Trail
- Tech Support

Audit Trail

The Audit Trail option displays a listing of recent critical CLI activities from a syslog log file. Use this tool when you need visibility into user login and configuration activity.

The following user activities are logged in the audit trail:

- All CLI commands
- User logins (including failed attempts)
- Unauthorized access attempts
- SPAN changes
- NDE data source changes
- Enabling and disabling data collections
- Starting and stopping captures
- Adding and deleting users

Each log entry will contain the following:

- User ID
- Time stamp
- IP address (in case of remote web access)
- Activity description

To access the audit trail window:

Step 1 Select **Administration > Diagnostics > Audit Trail**.

The Audit Trail Window displays.

The Audit Trail window provides a way to view the user access log and filter entries based on time, user, (IP address) from or activity. The internal log files are rotated after reaching a certain size limit.

Tech Support

Provides troubleshooting information (similar to the **show tech** command). Use this tool to view and download support data into a zip file.

The Cisco NGA syslog records appliance system alerts that contain event descriptions and date and time stamps, indicating unexpected or potentially noteworthy conditions. This feature generates a potentially extensive display of the results of various internal system troubleshooting commands and system logs.

This information is unlikely to be meaningful to the average user. It is intended to be used by the Cisco TAC or your support team for debugging purposes. You are not expected to understand this information; instead, you should save the information and attach it to an email message to the support team.

Note You can also view this information from the CLI. For information on using the CLI, see the *Command Reference Guide for Cisco NetFlow Generation Appliance*.

To view tech support:

Step 1 Select **Administration > Diagnostics > Tech Support**.

After a few minutes, extensive diagnostic information is generated and displayed in the Diagnostics Tech Support Window.

Step 2 To save the information, either choose **File>Save As...** from the browser menu, or scroll to the bottom, click on techsupport-logs.tar.bz2, and save it to your local PC.

Maintain Your Appliance

This section covers details on maintenance tasks you may need to perform to replace faulty hardware in your appliance, as well as perform preventative procedures.

Required Equipment

The following equipment is used to perform the procedures in this chapter:

- Number 2 Phillips-head screwdriver
- Electrostatic discharge (ESD) strap or other grounding equipment such as a grounded mat

Tip You do not have to remove the cover to replace hard drives or power supplies.

Install or Replace Server Components

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Warning **Class 1 laser product.**
Statement 1008

Caution When handling server components, wear an ESD strap to avoid damage.

Tip You can press the Identification button on the front panel or rear panel to turn on a flashing Identification LED on the front and rear panels of the server. This allows you to locate the specific server that you are servicing when you go to the opposite side of the rack. You can also activate these LEDs remotely by using the CIMC interface.For LED information, see the *Quick Start Guide for Cisco NetFlow Generation Appliance*.

This section describes how to install and replace server components, and it includes the following topics:

- Replace Hard Drives, page 4-6
- Replace Your Power Supply, page 4-7

Replace Hard Drives

If for some reason you must replace a faulty hard disk drive, use the instructions in this section to perform the replacement.

Drive Population Guidelines

The drive-bay numbering is shown in Figure 4-1. Cisco NGA uses only the first two hard disk bays.

Figure 4-1 Hard Disk Drive Numbering

HDD1	HDD2	HDD3	HDD4

Observe these drive population guidelines for optimum performance:

- When populating drives, add drives to the lowest-numbered bays first.
- Keep an empty drive blanking tray in any unused bays to ensure proper air flow.

To replace or install a hot-pluggable hard drive:

Tip You do not have to shut down or power off the server to replace hard drives because they are hot-pluggable.

Step 1 Remove the drive that you are replacing or remove a blank drive tray from the bay:

a. Press the release button on the face of the drive tray. See Figure 4-2.

b. Grasp and open the ejector lever and then pull the drive tray out of the slot.

c. If you are replacing an existing drive, remove the four drive-tray screws that secure the drive to the tray and then lift the drive out of the tray.

Step 2 Install a new drive:

a. Place a new drive in the empty drive tray and install the four drive-tray screws.

b. With the ejector lever on the drive tray open, insert the drive tray into the empty drive bay.

c. Push the tray into the slot until it touches the backplane, then close the ejector lever to lock the drive in place.

Figure 4-2 Replacing Hard Drives

1	Release button	**3**	Hard drive sled, bottom view
2	Ejector level	**4**	Securing screws (four)

Replace Your Power Supply

The Cisco NetFlow Generation Appliance has one power supply. For more information about the power supply specifications and LEDs, see *Quick Start Guide for Cisco NetFlow Generation Appliance*.

Note Shut down and power off the Cisco NetFlow Generation Appliance using the **shutdown** command in the CLI. Do not use the Cisco NGA Power button unless the **shutdown** command is unsuccessful.

To replace or install a power supply, follow these steps:

Step 1 To remove the power supply that you are replacing or a blank panel from an empty bay (see Figure 4-3) do the following:

a. Remove the power cord from the power supply that you are replacing.

b. Grasp the power supply handle while pinching the release lever towards the handle.

c. Pull the power supply out of the bay.

Step 2 Install a new power supply:

a. Grasp the power supply handle and insert the new power supply into the empty bay.

b. Push the power supply into the bay until the release lever locks.

c. Connect the power cord to the new power supply.

d. Press the **Power** button to return the appliance to main power mode.

Figure 4-3 Removing and Replacing Power Supplies

1	Power supply handle	**2**	Power supply release lever

Maintain Your Site Environment

The following sections discuss various environmental factors that can adversely affect appliance performance and longevity.

Your Cisco NetFlow Generation Appliance is configured to your order and is ready for installation and startup when it leaves the factory. After you install and configure your appliance, you might have to perform specific maintenance procedures and operations to ensure that the appliance is operating properly.

Following these preventive maintenance procedures can keep your appliance in top operating condition and minimize the need for costly, time-consuming service procedures:

- General Exterior Cleaning and Inspection, page 4-9
- Cooling, page 4-10
- Temperature, page 4-10
- Humidity, page 4-11
- Altitude, page 4-11
- Electrostatic Discharge, page 4-11

Caution To help prevent problems, before performing any procedures in this chapter, review the *Regulatory Compliance and Safety Information* documentation and the "Safety Guidelines" section on page 2-2.

General Exterior Cleaning and Inspection

This section details the cleaning requirements for exterior surfaces of the appliance and the inspection of cables and adapter cards.

Caution Never spray cleaning solution on the surfaces of the appliance. Overspray can penetrate into the appliance and cause electrical problems and corrosion.

Appliance

Use a lint-free, nonabrasive cloth to perform cleaning. *Do not* use a solvent, abrasive cleaning agents, or tissue paper. If the appliance is dirty (for example, with thick dust), use a soft damp cloth and wipe the surface of the appliance gently.

Immediately wipe off any water or liquid from the appliance.

Dust and Particles

A clean operating environment can greatly reduce the negative effects of dust and other particles, which act as insulators and interfere with the operation of an appliance's mechanical components. In addition to regular cleaning, you should follow these guidelines to deter contamination of the appliance:

- Do not permit smoking anywhere near the appliance.
- Do not permit food or drink near the appliance.

Cables and Connectors

Inspect cables and connectors to and from your appliance periodically to see if they are worn out or loose.

Adapter Cards

Check the connections on the adapter cards. Be sure they are secured to the appliance and have not been jarred loose or mechanically damaged.

Corrosion

The oil from a person's fingers or prolonged exposure to high temperature or humidity can corrode the gold-plated edge connectors and pin connectors on adapter cards in the appliance. This corrosion on adapter card connectors is a gradual process that can eventually lead to intermittent failures of electrical circuits.

To prevent corrosion, you should avoid touching contacts on adapter cards. Protecting the appliance from corrosive elements is especially important in moist and salty environments, which tend to promote corrosion. Also, as a further deterrent to corrosion, the appliance should not be used in extreme temperatures, as explained in the "Temperature" section on page 4-10.

Cooling

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Exhaust fans in the power supply and in the appliance itself cool the power supply and the appliance by drawing air in through various openings in the front of the appliance and blowing it out the back. However, the fans also draw dust and other particles into the appliance, causing contaminant buildup, which results in an increase in the appliance's internal temperature and interferes with the operation of various appliance components.

To avoid these conditions, we recommend keeping your work environment clean to reduce the amount of dust and dirt around the appliance, thereby reducing the amount of contaminants drawn into the appliance by the fans.

Temperature

Temperature extremes can cause a variety of problems, including premature aging and failure of chips or mechanical failure of devices. Extreme temperature fluctuations can cause chips to become loose in their sockets and can cause expansion and contraction of disk drive platters, resulting in read or write data errors.

To minimize the negative effects of temperature on appliance performance, follow these guidelines:

- Ensure that the appliance is operated in an environment no colder than 50°F (10°C) or hotter than 95°F (35°C).
- Ensure that the appliance has adequate ventilation. Do not place it within a closed-in wall unit or on top of cloth, which can act as insulation. Do not place it where it will receive direct sunlight, particularly in the afternoon. Do not place it next to a heat source of any kind, including heating vents during winter.

Adequate ventilation is particularly important at high altitudes. Appliance performance might not be optimum when the appliance is operating at high temperatures as well as high altitudes.

- Make sure that all slots and openings on the appliance remain unobstructed, especially the fan vents on the back of the appliance.
- Clean the appliance at regular intervals to avoid any buildup of dust and debris, which can cause an appliance to overheat.
- If the appliance has been exposed to abnormally cold temperatures, allow a 2-hour warm-up period to bring it up to normal operating temperature before turning it on. Failure to do so might cause damage to internal components, particularly the hard disk drive.

Humidity

High-humidity conditions can cause moisture migration and penetration into the appliance. This moisture can cause corrosion of internal components and degradation of properties, such as electrical resistance, thermal conductivity, physical strength, and size. Extreme moisture buildup inside the appliance can result in electrical shorts, which can cause serious damage to the appliance.

Each appliance is rated to operate at 8 to 80 percent relative humidity, with a humidity gradation of 10 percent per hour. Buildings in which climate is controlled by air conditioning in the warmer months and by heat during the colder months usually maintain an acceptable level of humidity for appliances. However, if an appliance is located in an unusually humid location, a dehumidifier can be used to maintain the humidity within an acceptable range.

Altitude

Operating an appliance at high altitude (low pressure) reduces the efficiency of forced, convection cooling and can result in electrical problems related to arcing and corona effects. This condition can also cause sealed components with internal pressure, such as electrolytic capacitors, to fail or perform at reduced efficiency.

Electrostatic Discharge

Electrostatic discharge (ESD) results from the buildup of static electricity on the human body and certain other objects. This static electricity is often produced by simple movements, such as walking across a carpet. ESD is a discharge of a static electrical charge that occurs when a person whose body contains such a charge touches a component in the appliance. This static discharge can cause components, especially chips, to fail. ESD is a problem particularly in dry environments where the relative humidity is below 50 percent.

To reduce the effects of ESD, you should observe the following guidelines:

- Wear a grounding wrist strap. If a grounding wrist strap is unavailable, touch an unpainted metal surface on the appliance chassis periodically to neutralize any static charge.
- Keep components in their antistatic packaging until they are installed.
- Avoid wearing clothing made of wool or synthetic materials.

Electromagnetic and Radio Frequency Interference

Warning **Blank faceplates and cover panels serve three important functions: they prevent exposure to hazardous voltages and currents inside the chassis; they contain electromagnetic interference (EMI) that might disrupt other equipment; and they direct the flow of cooling air through the chassis. Do not operate the system unless all cards, faceplates, front covers, and rear covers are in place.** Statement 1029

Electromagnetic interference (EMI) and radio frequency interference (RFI) from an appliance can adversely affect devices, such as radio and television (TV) receivers operating near the appliance. Radio frequencies emanating from an appliance can also interfere with cordless and low-power telephones.

RFI is defined as any EMI with a frequency above 10 kilohertz (kHz). This type of interference can travel from the appliance to other devices through the power cable and power source or through the air like transmitted radio waves. The Federal Communications Commission (FCC) publishes specific regulations to limit the amount of EMI and RFI emitted by computing equipment. Each appliance meets these FCC regulations.

To reduce the possibility of EMI and RFI, follow these guidelines:

- Operate the appliance only with the appliance cover installed.
- Ensure that the screws on all peripheral cable connectors are securely fastened to their corresponding connectors on the back of the appliance.

Magnetism

Because they store data magnetically, hard disk drives are susceptible to the effects of magnetism. Hard disk drives should never be stored near magnetic sources such as the following:

- Monitors
- Printers
- Telephones with real bells
- Fluorescent lights

Power Source Interruptions

Appliances are especially sensitive to variations in voltage supplied by the AC power source. Overvoltage, undervoltage, and transients (or spikes) can erase data from the memory or even cause components to fail. To protect against these types of problems, power cables should always be properly grounded and one or both of the following methods should be used:

- Place the appliance on a dedicated power circuit (rather than sharing a circuit with other electrical equipment). In general, do not allow the appliance to share a circuit with any of the following:
  - Copier machines
  - Teletype machines
  - Laser printers
  - Facsimile machines
  - Any other motorized equipment

Besides the above equipment, the greatest threats to an appliance's supply of power are surges or blackouts caused by electrical storms.

If a blackout occurs—even a temporary one—while the appliance is turned on, turn off the appliance immediately and disconnect it from the electrical outlet. Leaving the appliance on might cause problems when the power is restored.

CHAPTER 5

Upgrade the Software

The Cisco NetFlow Generation Appliance is shipped with the software image installed; however, to obtain future release versions, a software upgrade is required.

Before the upgrade procedure, you may wish to back up your current configuration. From the command line enter a **config upload** command such the following:

config upload ftp://server/path [*filename*]

The config upload command sends a copy of the appliance running configuration to the destination you specify. For details on restoring your back up configuration, see the **config restore** command in the *Command Reference Guide for Cisco NetFlow Generation Appliance*.

To upgrade the software:

Step 1 Download the image from Cisco.com Software Download.

Step 2 Log in using your Cisco.com ID and enter **Cisco NetFlow Generation Appliance** software to search for images.

Step 3 Copy the software image to a directory accessible to FTP.

Step 4 If a README is available, follow the README or text file on the Cisco download site.

Step 5 Log into the appliance through the console port or through a Telnet session.

Step 6 Upgrade the software as follows:

```
root@localhost# upgrade ftp-url
```

where *ftp-url* is the FTP location and name of the software image file.

Note If the FTP server does not allow anonymous users, use the following syntax for the *ftp-url* value: *ftp://user:password@host//absolute-path/filename*. Enter your password when prompted.

As in the following example:

```
upgrade ftp://admin:secret@172.20.104.11//archive/nga_software/
nga-app-x86_64.1-0-1-10.bin.gz
```

Step 7 Follow the screen prompts during the upgrade.

Step 8 After completing the upgrade, the appliance reboots and then prompts you to log in.

CHAPTER 6

Using the Recovery CD and Helper Utility

You can use the recovery CD to reinstall the software on your Cisco NetFlow Generation Appliance if your appliance should suffer a catastrophic event, such as a hard disk crash, and you can no longer boot the appliance. The recovery CD is part of the Cisco NGA software kit.

After you use the recovery CD to reinstall the Cisco NGA image, you can use the command-line interface (CLI) to restore the most recent configuration file to the appliance if you have stored a configuration file at an accessible location.

This chapter contains:

For information on how to prepare to recover from a catastrophic event, see Booting the Recovery CD, page 6-1 or Using the Helper Utility, page 6-2. We recommend you use the helper utility only if you want to reformat the disk.

Booting the Recovery CD

When you boot the Cisco NetFlow Generation Appliance (NGA) from the recovery CD, the console will temporarily display the bootloader window. After this window displays for ten seconds, the appliance will automatically boot the appliance application software.

When using the recovery CD, choose **helper** and press **Enter** within that 10 second interval to get to the helper utility Menu. Otherwise, you might have to reboot the appliance again.

To use the recovery CD:

Step 1 Insert the Cisco NGA Software Recovery CD-ROM into the DVD-ROM drive on the front panel of the appliance.

Step 2 From the console or command line, enter the **reboot** command.

The Cisco NGA performs a reset and launches the GNU GRUB boot loader and displays the window shown in Figure 6-1. This window displays for about ten seconds enabling you to select to boot the **helper utility** instead of the appliance application software.

Per the instructions, use the **^** and **v** keys to select which entry is highlighted. Press **Enter** to boot the selected OS, '**e**' to edit the commands before booting or '**c**' for a GNU command-line.

Step 3 Use the "**v**" key to select **helper**, and press **Enter**.

The helper utility menu displays as shown in Figure 6-1.

Figure 6-1 Helper Utility Menu

```
================================================================================
     Cisco Systems, Inc.
     NetFlow Generation Appliance helper utility
     Version 1.0

     -----
     Main menu
     1 - Download application image and write to HDD
     2 - Download application image and reformat HDD
     3 - Install application image from CD
     4 - Display software versions
     5 - Reset application image CLI passwords to default
     6 - Change file transfer method (currently ftp/http)
     7 - Send Ping
     n - Configure network
     r - Exit and reset Services Engine
     h - Exit and shutdown Services Engine

     Selection [1234567dnfrh]:
```

See the next section, Using the Helper Utility, for more information about the options.

Using the Helper Utility

This section describes the Helper Utility Menu, what each option does, and any requirements for using a particular option. We recommend you use the helper utility only if you want to reformat the disk. Otherwise, you should use the recovery CD or upgrade software instructions.

Note Before you can use menu items 1 and 2, you must first use menu item **n** to configure network parameters for the appliance.

Possible selections for the top level of the helper utility menu are **1, 2, 3, 4, 5, 6, 7, n, r,** and **h**.

- Option n - Configure Network, page 6-3
- Option 1 - Download Application Image and Write to HDD, page 6-4
- Option 2 - Download Application Image and Reformat HDD, page 6-4
- Option 3 - Install Application Image from CD, page 6-4
- Option 4 - Display Software Versions, page 6-4
- Option 5 - Reset Application Image CLI Passwords to Default, page 6-4
- Option 6 - Change File Transfer Method, page 6-5
- Option 7- Send Ping, page 6-5
- Option r- Exit and Reset Services Engine, page 6-5
- Option h- Exit and Shutdown Services Engine, page 6-5

Option n - Configure Network

Use **Option n** to configure the network parameters for the appliance.

Step 1 When the Configure Network Interface menu displays, enter **2** to configure manually.

```
-----
Configure Network interface:
1 - Use application image configuration
2 - Configure manually
3 - Show config
r - return to main menu

Selection [123r]: 2
```

Step 2 The utility prompts you for the IP address, netmask, and default gateway for the appliance.

```
Enter IP configuration:
IP address []: 172.20.122.93
netmask []: 255.255.255.128
default gateway []: 172.20.122.1

-----
Configure Network interface:
1 - Use application image configuration
2 - Configure manually
3 - Show config
r - return to main menu

Selection [123r]
```

Step 3 Check your network configuration using Configure Network menu option 3.

```
Selection [123r]: 3

eth0      Link encap:Ethernet  HWaddr 00:0E:0C:EE:50:3E
          inet addr:172.20.122.93  Bcast:172.20.122.127  Mask:255.255.255.128
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:210 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:13632 (13.3 KiB)  TX bytes:0 (0.0 b)

Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref     Use Iface
172.20.122.0     0.0.0.0        255.255.255.128 U       0      0      0 eth0
0.0.0.0          172.20.122.1    0.0.0.0      UG   0     0      0 eth0
-----
Configure Network interface:
1 - Use application image configuration
2 - Configure manually
3 - Show config
r - return to main menu

Selection [123r]:
```

Option 1 - Download Application Image and Write to HDD

Prior to using **Option 1**, first use **Option n** to configure the network.

Use **Option 1** to download a version of the application image from an FTP server location and write the image to the hard disk drive. This option requires network connectivity and that network parameters be configured for the appliance using helper menu item **n**.

This option enables you to download an image you might have stored at an FTP location or at a location you can access using **http**. You can download the latest version of software from the following URL:

http://www.cisco.com/cgi-bin/tablebuild.pl/nga-appl

This URL requires you to have a Cisco service agreement and access to the internet to download the zipped software.

Option 2 - Download Application Image and Reformat HDD

Prior to using **Option 2**, first use **Option n** to configure the network.

Use **Option 2** to download the application image and write the image to the hard disk drive. This option downloads a version of the application image from an FTP server location or at a location you can access using **http**.

Using this option reformats the hard disk drives before writing the application image and will destroy all data such as reports or data captures.

You can also download the latest version from Cisco.com.

Option 3 - Install Application Image from CD

Use **Option 3** to install the application image from the recovery CD. This option might be necessary if you are unable to connect to your network and download a version of software you archived earlier.

Note The version of software available on the recovery CD is the first release of the software and has no patches or upgrades.

This option reformats the hard disk drives before writing the application image and will destroy all data such as reports or data captures.

Option 4 - Display Software Versions

Use **Option 4** to display the current application image version stored on your hard disk.

```
Selection [123456789dnfrh]:5

-----
NGA application version: 1.0

Selection [123456789dnfrh]:
```

Option 5 - Reset Application Image CLI Passwords to Default

Use **Option 5** to reset the password for users root and admin to their default values.

Option 6 - Change File Transfer Method

Use **Option 6** to change the file transfer method. This option is only necessary if you change the file transfer method by mistake. Only **FTP** and **http** are supported.

```
Selection [123456789dnfrh]: 7
-----
Change file transfer method menu
The current file transfer method is ftp/http.
1 - Change to FTP/HTTP
r - return to main menu
```

Option 7- Send Ping

Use **Option 7** to send a ping to determine if network connectivity exists. When prompted, enter the IP address or full domain name of the location to send the ping.

```
IP address to ping []: 172.20.122.91

Sending 5 ICPM ECHO_REQUEST packets to 172.20.122.91.
PING 172.20.122.91 (172.20.122.91) 56(84) bytes of data.
64 bytes from 172.20.122.91: icmp_seq=1 ttl=64 time=0.151 ms
64 bytes from 172.20.122.91: icmp_seq=2 ttl=64 time=0.153 ms
64 bytes from 172.20.122.91: icmp_seq=3 ttl=64 time=0.125 ms
64 bytes from 172.20.122.91: icmp_seq=4 ttl=64 time=0.102 ms
64 bytes from 172.20.122.91: icmp_seq=5 ttl=64 time=0.166 ms

--- 172.20.122.91 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4000ms
rtt min/avg/max/mdev = 0.102/0.139/0.166/0.025 ms
```

Option r- Exit and Reset Services Engine

Use **Option r** to reset the appliance prior to rebooting the newly installed application image.

Before using **Option r**, remove the recovery CD from the CD drive to enable the appliance to boot the application image.

Option h- Exit and Shutdown Services Engine

Use **Option h** to reset and shut down the appliance.

```
------------------------------------------------------------------------
Option h for recovery CD
Selection [123456789dnfrh]: h
About to exit and reset NGA.
Are you sure? [y/N] :y
Stopping internet superserver: inetd.
Stopping OpenBSD Secure Shell server: sshd.
Stopping internet superserver: xinetd.
Stopping internet superserver: xinetd-ipv4.
: done.
Shutting down NGA, part 1:
Stopping klogd . . .
Stopping syslogd . . .
Sending all processes the TERM signal... done.
Sending all processes the KILL signal... done.
```

```
Unmounting remote filesystems... done.
Deactivating swap...done.
Unmounting local filesystems...done.
Starting halt command: halt
md: stopping all md devices.
Synchronizing SCSI cache for disk sdb:
FAILED
  status = 1, message = 00, host = 0, driver = 08
  <6>sd: Current: sense key=0x5
    ASC=0x20 ASCQ=0x0
Synchronizing SCSI cache for disk sda:
FAILED
  status = 1, message = 00, host = 0, driver = 08
  <6>sd: Current: sense key=0x5
    ASC=0x20 ASCQ=0x0
ACPI: PCI interrupt for device 0000:07:00.1 disabled
ACPI: PCI interrupt for device 0000:07:00.0 disabled
Power down.
acpi_power_off called
--------------------------------------------------------------------------------------------
```

APPENDIX A

Troubleshooting

This appendix includes

Table A-1 Troubleshooting Tips

Problem Description	What to Check?	What Should You Do?
Cisco NetFlow Generation Appliance does not appear in your collectors list of NetFlow devices.	Is the SNMP community string configured to the same value on both the collector and Cisco NGA?	Check your collector documentation to find out what community string it is using. Choose **Administration > System > SNMP Agent** to set the same community string (or use the CLI command **snmp community <***string***> ro|rw**).
Cannot enable flow monitor.	Are there error messages indicating any missing components?	Execute the command **show debug messages** and look for diagnostic messages. Ensure you configure the missing component and include it in the flow monitor configuration using **Advanced Setup** or CLI.
	Are there any other flow monitors active in the system?	Enter **show flow monitor** and check the cache size assigned to the already activated monitors. Ensure the total cache size is less than 100%.
	Are there already four flow monitors activated?	Deactivate one of the flow monitors to allow a new one to become active.
User interface layout behaves strangely, or content does not change when navigating to a different menu area.	Are you using a supported browser and version?	Ensure that your browser version is supported.
	Has your browser session timed out?	Click your browser's **Refresh** button and log in again if prompted to do so.
	Is stale data cached in your browser?	Clear your browser cache and restart the browser.

Table A-1 Troubleshooting Tips (continued)

Problem Description	What to Check?	What Should You Do?
No NetFlow data is reaching the collector (collector side).	Is the Cisco NGA sending data on the same UDP port that the collector is listening on?	Consult your collector documentation to determine which UDP port it is listening on. Use the GUI or CLI to modify the collector configuration with the same UDP port number. By default, the value is 3000 on Cisco NGA. Third party collectors may listen on a different UDP port.
	Was the collector application properly installed and configured?	Check your collector and see your collector user documentation for verification. Check the collector configuration to ensure it is accurate.
	Is Cisco NGA reachable from the collector server?	Use **ping** to ensure the collector and IP addresses successfully reach each other. If they are unreachable, check your network connection and configuration.
	Does SPAN traffic forward to the switch ports that are connected to the data ports?	On the Nexus switch console, check the SPAN configuration. Read the interface counters and ensure traffic is being forwarding to the collector.
	Is the collector reachable from the appliance?	Use **ping** to check the collector IP address. If ping does not work, check your network connectivity and configuration.
	Is the collector listening to the correct UDP port?	Ensure the collector is listening to the same UDP port that is configured in the flow collector.
	Is SPAN traffic received by the appliance?	On the console, run **show dataport statistics rate** and ensure there is sufficient traffic arriving at the connected data ports. If not, check the traffic source on the switch side (SPAN configuration, physical network connections between the switch and device. Run **show dataport statistics cumulative** and check for packet drops. If there are many namelookup connection issue messages, disable name resolution from the UI, clear the browser cache, and see what is the result for the span page.
	Does traffic get passed to the cache engine?	On the console, run **show cache statistics rate** ***monitor_name*** and ensure the cache engine is processing traffic. You can run **show cache statistics cumulative** ***monitor_name*** to check for packet drops. If the **Packet Dropped (no record)** counter is high and continues to increase, ensure the defined flow record type is compatible with the incoming traffic type.
	Does the exporter export NetFlow data?	On the console, run **show collector statistics** ***collector_name*** and ensure no flow traffic was dropped and that flow rates are sufficient.

Table A-1 Troubleshooting Tips (continued)

Problem Description	What to Check?	What Should You Do?
The power LED on the front panel is not on.	Is the AC power cord connected properly?	If the power LED is still off, the problem might be a power supply failure.
The appliance shuts down after being on for only a short time.	• Check for an environmentally induced shutdown (see the "Reading the LEDs" section on page A-4). • Check the fans. If the fans are not working, the appliance will overheat and shut itself down. • Ensure that the appliance intake and exhaust vents are clear.	• If the fans are not working, you might need to check the power supply connections to the fans. • Check the environmental site requirements in the "Maintain Your Appliance" section on page 4-5.
The appliance partially boots, but the LEDs do not light.	Check for a power supply failure by inspecting the power LED on the front panel of the appliance. If the LED is on, the power supply is functional.	If the LED is off, refer to the *Cisco Information Packet* for warranty information or contact your customer service representative.
Power supply shuts down or latches off.	Check to see if the fan has failed, the air conditioning in the room has failed or airflow is blocked to cooling vents.	Take steps to correct the problem. For information about environmental operating conditions, see Cooling, page 4-10.
Adapter card is not recognized by the appliance.	• Make sure that the adapter card is firmly seated in its slot. • Check the LEDs on the adapter card. Each adapter card has its own set of LEDs. For information on these LEDs, see the "Reading the LEDs" section on page A-4. • Make sure that you have a version of software that supports the adapter card.	For information, see the documentation that was included with your adapter card.
Adapter card is recognized, but interface ports do not initialize.	• Make sure that the adapter card is firmly seated in its slot. • Check external cable connections. • Make sure that you have a version of software that supports the adapter card. Refer to the documentation that was included with your adapter card.	For information, see the documentation that was included with your adapter card.
The appliance does not boot properly, or it constantly or intermittently reboots.	• Make sure that the adapter card is firmly seated in its slot. • Check the appliance chassis or the application software.	• For information, see the documentation that was included with your adapter card. • For warranty information, see the *Cisco Information Packet* publication that shipped with your appliance or contact your customer service representative.

Table A-1 Troubleshooting Tips (continued)

Problem Description	What to Check?	What Should You Do?
If you are using the console port with a terminal, and the appliance boots but the console screen is frozen.	• Check the external console connection. • Verify that the parameters for your terminal are set as follows: (a) The terminal should have the same data rate that the appliance has (9600 bps is the default). (b) 8 data bits. (c) No parity generated or checked. (d) 1 stop bit.	
The appliance powers up and boots only when an adapter card is removed.	• Check the adapter card. There might be a problem with the adapter card. Refer to the documentation that was included with your adapter card.	For warranty information, refer to the *Cisco Information Packet* publication that shipped with your appliance or contact your customer service representative.
The Cisco NAM appliance powers up and boots only when a particular cable is disconnected.	There might be a problem with the cable.	For warranty information, see the *Cisco Information Packet* publication that shipped with your appliance or contact your customer service representative.
Cannot locate the product serial ID on the Cisco NGA.	Before you submit a request for service online or by phone, use the CPI tool to locate your product serial number. This tool offers three search options: • Search by product ID or model name • Browse for Cisco model • Copy and paste the output of the **show** command to identify the product	On the Cisco NAM appliance, the serial number label is located on the right-hand corner above the RJ-45 serial connector on the front of the appliance.

Reading the LEDs

The Cisco NetFlow Generation Appliance LEDs serve the following purposes:

- Indicate that basic power is available to the appliance
- Guide you to a broken adapter card, or to one that has failed its diagnostics
- Give an indication that traffic is flowing through the adapter card to the appliance

The LEDs on the front panel of the Cisco NAM appliance and corresponding adapter card are aids for determining appliance and adapter performance and operation.

This section contains:

Front-Panel LEDs

Figure 1 depicts the Cisco NGA front panel. Table 2 describes the appliance LEDs.

Figure 1 Front Panel Cisco NGA

3	Operations panel LEDs, left to right: System status LED Fan status LED Temperature status LED Power supply status LED Network activity LED	**5**	Power button/LED. Use only when a forced shutdown is necessary. Hold down for several seconds until light is no longer lit with a green color.
4	Identification button/LED		

Table 2 Front-Panel LEDs

LED	Color	State	Description
Operations panel LEDs, left to right (location 3): System status LED Fan status LED Temperature status LED Power supply status LED Network activity LED	Green	On	Standby or ready for operation
	Green	Blinking	Traffic occurring
	Amber	On	One or more critical fault conditions
	Amber	Blinking	One or more noncritical fault conditions
Appliance Status (location 4)	Green	On	Standby or ready for operation
	Green	Blinking	Traffic occurring
	Amber	On	One or more critical fault conditions
	Amber	Blinking	One or more noncritical fault conditions
Appliance Power (location 5)	Green	On	Power on
	Off	Off	Power off

Built-In NIC LEDs

Figure 2 shows the NIC 1 and NIC 2 LEDs located on the rear of the appliance. These LEDs indicate the connection activity and speed of the NIC ports. Table 3 describes the activity and connection speed associated with each LED state.

Figure 2 NIC 1 and NIC 2 LEDs

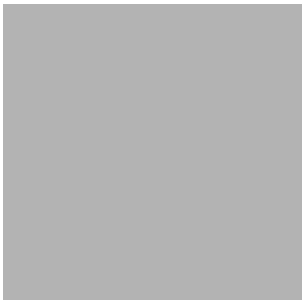


Table 3 NIC 1 and NIC 2 LED Descriptions

LED	Color	State	Description
Left (location 1)		Off	No network connection
	Green	Solid	Network connection
	Green	Blinking	Transmit/receive activity
Right (location 2)		Off	10-Mb/s connection (if left LED is on or blinking)
	Green	Solid	100-Mb/s connection
	Amber	Solid	1000-Mb/s (or 1-Gb/s) connection

APPENDIX B

Software Field Description Tables

The window field description tables for the following are included in this section:

Table B-1 lists the match and collect field descriptions for IPv4, IPv6, and Layer 2 flow records in the user interface, as well as the CLI.

Table B-1 Flow Record Match and Collect Field Descriptions

Match Fields (keys of the flow record)	GUI and CLI		
	IPv4	IPv6	Layer 2
CoS	X	X	X
Ethertype	X	X	X
Input SNMP Interface	X	X	X
IP Protocol	X	X	
IPv4 Destination Address	X		
IPv4 Source Address	X		
IPv4 TOS	X		
IPv4 TTL	X		
IPv6 Destination Address		X	
IPv6 Hop Limit		X	
IPv6 Source Address		X	
IPv6 Traffic Class		X	
Layer 4 Destination Port	X	X	
Layer 4 Source Port	X	X	
MAC Destination Address	X	X	X

Table B-1 Flow Record Match and Collect Field Descriptions (continued)

Match Fields (keys of the flow record)	GUI and CLI		
	IPv4	IPv6	Layer 2
MAC Source Address	X	X	X
MPLS Label	X	X	X
Output SNMP Interface	X	X	X
VLAN ID	X	X	X
Collect Fields			
Application ID[1]	X	X	X
Byte Count	X	X	X
First Timestamp	X	X	X
Flow Label		X	
IPv4 ICMP Code	X		
IPv4 ICMP Type	X		
IPv6 ICMP Code		X	
IPv6 ICMP Type		X	
Last Timestamp	X	X	X
Network Encapsulation	X	X	X
Packet Count	X	X	X
TCP Header Flags	X	X	X

1. See Table B-7 on page B-6 for a list of Application ID values.

Table B-2 lists the field descriptions for the Configure Filter window.

Table B-2 Configure Filter Window Fields

Field[1]	Description
Application ID	Application ID [0]. See Table B-7 on page B-6 for a list of values.
CoS	802.1q priority field value [0-7].
Description	Provide a description for the flow filter.
Destination IP Address	Destination IP address, or address/prefix value. Either an IPv4 or IPv6 address can be typed into this field.
Destination Layer 4 Ports	Layer 4 destination port number [0-65535].
Destination MAC Address	Destination MAC address or MAC address/prefix (for example: EE:EE:EE:EE:EE:EE or EE:EE:EE:EE:EE:EE/xx).
Ethertype	Ethertype value [0x0000-0xFFFF/0000-FFFF].
Input SNMP If-Index	Input SNMP If-Index value [0-2147483647].
IP Protocol	IP protocol number [0-255].
IPv4 ICMP Code	ICMP code for IPv4 [0-255].
IPv4 ICMP Type	ICMP type for IPv4 [0-255].

Table B-2 Configure Filter Window Fields (continued)

Field[1]	Description
IPv6 Flow Label	Flow label value for IPv6 traffic [0-1048575].
IPv6 ICMP Code	ICMP code for IPv6 [0-255].
IPv6 ICMP Type	ICMP type for IPv6 [0-255].
MPLS Label	Top-most MPLS label [0-1048575].
Name	Enter a unique name to identify this filter configuration. Use up to 63 alpha-numeric characters.
Network Encapsulation	Network encapsulation value [1-7].
Output SNMP If-Index	Output SNMP If-Index value [0-2147483647].
Source IP Address	Source IP address, or address/prefix value. Either an IPv4 or IPv6 address can be typed into this field.
Source Layer 4 Ports	Layer 4 source port number [0-65535].
Source MAC Address	Source MAC address or MAC address/prefix (for example: EE:EE:EE:EE:EE:EE or EE:EE:EE:EE:EE:EE/xx).
TCP Header Flags	TCP flags [0-255].
TOS	Type of Service for IPv4 traffic [0-255].
TTL	Time to Live for IPv4 traffic [0-255].
VLAN ID	VLAN identifier [0-4095].

1. In general, filtering on address (IPv4, IPv6, or MAC) supports address mask. Other non-address field filtering supports a comma-separated list of single and value ranges (e.g 1, 3, 9-12).

Table B-3 lists the field descriptions for the Configure Records window.

Table B-3 Configure Records Window Fields

Field	Field Description		
Name	Enter a unique name to identify this configuration. Use up to 63 alpha-numeric characters.		
Description	Enter information about this record.		
Type	IPv4	IPv6	Layer 2

Table B-3 Configure Records Window Fields (continued)

Field	Field Description		
Match Fields	CoS	CoS	CoS
	Ethertype	Ethertype	Ethertype
	Input SNMP Interface	Input SNMP Interface	Input SNMP Interface
	IP Protocol	IP Protocol	MAC Destination Address
	IPv4 Destination Address	IPv6 Destination Address	MAC Source Address
	IPv4 Source Address	IPv6 Hop Limit	MPLS Label
	IPv4 TOS	IPv6 Source Address	Output SNMP Interface
	IPv4 TTL	IPv6 Traffic Class	VLAN ID
	Layer 4 Destination Port	Layer 4 Destination Port	
	Layer 4 Source Port	Layer 4 Source Port	
	MAC Destination Address	MAC Destination Address	
	MAC Source Address	MAC Source Address	
	MPLS Label	MPLS Label	
	Output SNMP Interface	Output SNMP Interface	
	VLAN ID	VLAN ID	
Collect Fields	Application ID	Application ID	Application ID
	Byte Count	Byte Count	Byte Count
	First Timestamp	First Timestamp	First Timestamp
	IPv4 ICMP Code	Flow Label	Last Timestamp
	IPv4 ICMP Type	IPv6 ICMP Code	Network Encapsulation
	Last Timestamp	IPv6 ICMP Type	Packet Count
	Network Encapsulation	Last Timestamp	
	Packet Count	Network Encapsulation	
	TCP Header Flag	Packet Count	
		TCP Header Flag	

Table B-4 lists the field descriptions for the Configure Collector window.

Table B-4 Configure Collector Window Fields

Field	Field Description
Name	A unique name to identify this configuration. Use up to 63 alpha-numeric characters.
Description	Provide unique description.
IP Address	IPv4 address of NetFlow collector. Cannot use a domain name.

Table B-4 Configure Collector Window Fields (continued)

Field	Field Description
UDP Port	UDP port at which the NetFlow collector device is receiving NetFlow packets from Cisco NGA.
DSCP	The Differentiated Services CodePoint (DSCP) priority value that Cisco NGA uses when it sends flow records to this collector. This value is related to the quality of service (QOS) policy in use on your network. The default value is 0 and in most cases will not need to be changed.

Table B-5 lists the field descriptions for the Configure Exporter window.

Table B-5 Configure Exporter Window Fields

Field	Field Description
Name	Enter a unique name to identify this configuration. Use up to 63 alpha-numeric characters.
Description	Up to 120 character description.
NetFlow Version	V5, V9, or IPFIX
Timeout Template/Options	Configures how often data templates and options templates will be sent to the collectors. For more information about data and options templates, see the *NetFlow Version 9 Flow-Record Format* white paper.
Policy	Select multi-destination or round-robin policy.
Export Filters	Select one or more filters that you have already created to be applied to this exporter. Exporter filters selected at this level apply to all collectors in the exporter.
Collector Name	Collector name that you have defined using the steps outlined in Configure Collectors, page 3-4.
Filter	Select filter or filters to be applied to this particular collector only. Filters specified here at the destination are only applicable if you have selected the policy **multi-destination**.
Weight	If a round-robin policy has been chosen to load balance among a group of multiple collectors, this parameter specifies the weight of this individual collector among the group. The number you enter here is the number of NetFlow packets that will be sent to this collector before moving on to start sending to the next collector. For example, if two collectors are associated with this exporter using a round-robin policy, and the weight of collector A is 3 and the weight of collector B is 1, then 3 NetFlow packets will be sent to collector A for every 1 packet that is sent to collector B.

Table B-6 lists the field descriptions for the Configure Monitor window.

Table B-6 Configure Monitor Window Fields

Field	Field Description
Name	Enter a unique name to identify this configuration. Use up to 63 alpha-numeric characters.
Description	Enter any information to identify this monitor.
Export Name	Enter the exporter name to which this monitor is associated.
Data Port	Select the data ports on which raw network traffic enter into this monitor.

Table B-6 Configure Monitor Window Fields (continued)

Field	Field Description
Tunnel Mode	Select either **inner** or **outer** tunnel mode. The default value is inner (which is desired in most cases). This parameter determines which IP addresses are used for flows which are tunneled. For example, when there is more than one IP layer present in the packets, such as IPv6 encapsulated within IPv4.
Cache Type	Select either **standard** or **permanent** cache type. The default value is standard (which is desired in most cases). For a standard flow cache, flows expire from the cache according to the setting of the inactive timeout. For a permanent cache, flows never expire from the cache once they are created. This mode is only recommended for deployments where very few flows are expected and you want to ensure that those flows are never flushed from the cache. This is a very rare deployment scenario.
Cache Size (%)	Enter the cache size for this flow monitor as a percentage of the total cache memory available for the entire Cisco NGA. In many cases, only one flow monitor is activated, and in those cases the value should be set to 100%. If more than one flow monitor is activated, then you may want to choose to customize the memory resources used for each monitor. The default value is 25%, which provides enough storage for at least 16 million simultaneous flows.
Cache Timeout (sec) Active/Inactive	Enter the values for the active timeout and inactive timeout (in seconds). The inactive timeout determines when a flow will be flushed from the cache when packets are no longer observed. The active timeout determines how often the appliance exports records for continuously active flows.
Record Name	When you configure an exporter for V9 or IPFIX, at least one record is required. You can select up to three records, one of each type (IPv4, IPv6, Layer2). When an IPv4 packet is received by the monitor, it is matched with the IPv4 record if one has been configured; otherwise it is matched to a Layer2 record. If no Layer2 record has been configured, the packet is dropped. When an IPv6 packet is received by the monitor, it is matched with the IPv6 record if one has been configured; otherwise it is matched to a Layer2 record. If no Layer2 record has been configured, the packet is dropped. When a packet is received by the monitor that is neither IPv4 nor IPv6, it is matched to the Layer2 record. If no Layer2 record has been configured, it is dropped. Any packets dropped cause a counter to increment which can be shown using the CLI command **show cache statistics cumulative** <*monitor-name*>. It appears on the row labeled **Packets Dropped (no record)**. For more information, refer to the *Command Reference Guide for Cisco NetFlow Generation Appliance*.

Table B-7 lists the possible Application ID and Name details for the Application ID Collect field.

Table B-7 Application ID Collect Field Information

Application ID	Application Name
16777217	icmp
16777218	igmp
16777219	ggp
16777220	ip4inip
16777222	tcp
16777224	egp

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
16777225	igp
16777232	chaos
16777233	udp
16777238	xns-idp
16777243	rdp
16777244	irtp
16777245	iso-tp4
16777246	netblt
16777249	dccp
16777251	idpr
16777254	idpr-cmtp
16777257	ipv6inip
16777258	sdrp
16777259	ipv6-route
16777260	ipv6-frag
16777261	idrp
16777262	rsvp
16777263	gre
16777264	dsr
16777266	esp
16777267	ah
16777270	narp
16777271	mobile
16777274	ipv6-icmp
16777275	ipv6-nonxt
16777276	ipv6-opts
16777296	iso-ip
16777299	vines
16777304	eigrp
16777305	ospfigp
16777308	mtp
16777309	ax-25
16777310	ipip
16777311	micpa
16777313	etherip
16777314	encap

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
16777318	pnni
16777319	pim
16777324	ipcomp
16777328	vrrp
16777348	sctp
16777349	fc
16777350	rsvp-e2e-ignore
16777351	mobility-header
16777352	udplite
16777353	mpls-in-ip
16777354	manet
16777355	hip
16777356	shim6
50331655	echo
50331657	discard
50331659	systat
50331661	daytime
50331665	qotd
50331667	chargen
50331668	ftp-data
50331669	ftp
50331670	ssh
50331671	telnet
50331673	smtp
50331685	time
50331686	rap
50331688	rlp
50331690	nameserver
50331691	nicname
50331697	tacacs
50331698	re-mail-ck
50331700	xns-time
50331701	dns
50331702	xns-ch
50331703	isi-gl
50331704	xns-auth

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50331706	xns-mail
50331711	whois++
50331713	tacacs-ds
50331714	sql*net
50331715	bootps
50331716	bootpc
50331717	tftp
50331718	gopher
50331727	finger
50331728	http
50331736	kerberos
50331740	npp
50331742	objcall
50331749	hostname
50331750	iso-tsap
50331752	acr-nema
50331753	cso
50331757	pop2
50331758	pop3
50331759	sunrpc
50331761	auth
50331763	sftp
50331765	uucp-path
50331766	sqlserv
50331767	nntp
50331771	ntp
50331776	gss-xlicen
50331777	pwdgen
50331778	cisco-fna
50331779	cisco-tna
50331780	cisco-sys
50331782	ingres-net
50331783	epmap
50331791	imap
50331794	iso-tp0
50331795	iso-tp0

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50331798	sql-net
50331800	bftp
50331801	sgmp
50331804	sqlsrv
50331806	pcmail-srv
50331808	sgmp-traps
50331809	snmp
50331810	snmptrap
50331811	cmip-man
50331812	cmip-agent
50331813	xns-courier
50331818	print-srv
50331821	xyplex-mux
50331825	xdmcp
50331826	nextstep
50331827	bgp
50331833	remote-kis
50331834	remote-kis
50331842	irc
50331847	smux
50331849	at-rtmp
50331850	at-nbp
50331852	at-echo
50331854	at-zis
50331857	qmtp
50331858.50	z39.50
50331861	ipx
50331865	dbase
50331866	mpp
50331868	imap3
50331912	bgmp
50331967	ptp
50332001	ndsauth
50332019	clearcase
50332037	ldap
50332044	netware-ip

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50332055	timbuktu
50332075	svrloc
50332082	mobileip-agent
50332083	mobilip-mn
50332091	https
50332092	snpp
50332106	appleqtc
50332112	kpasswd
50332117	rcp
50332144	pim-rp-disc
50332148	isakmp
50332150	asa-appl-proto
50332160	exec
50332161	login
50332162	cmd
50332163	printer
50332164	videotex
50332165	talk
50332166	ntalk
50332167	utime
50332168	router
50332169	ripng
50332171	ibm-db2
50332172	ncp
50332173	timed
50332188	uucp
50332191	klogin
50332192	kshell
50332194	dhcpv6-client
50332195	dhcpv6-server
50332196	afpovertcp
50332202	rtsp
50332211	nntps
50332212	9pfs
50332221	banyan-vip
50332235	submission

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50332262	sshell
50332279	ipp
50332284	ldaps
50332287	msdp
50332294	ldp
50332302	aodv
50332314	doom
50332322	acap
50332331	corba-iiop
50332332	corba-iiop-ssl
50332346	olsr
50332348	epp
50332349	lmp
50332353	agentx
50332359	cisco-tdp
50332377	netviewdm
50332397	kerberos-adm
50332398	kerberos-iv
50332402	tell
50332477	pkix-3-ca-ra
50332508	iscsi
50332521	rsync
50332558	kink
50332637	ftps-data
50332638	ftps
50332640	telnets
50332641	imaps
50332642	ircs
50332643	pop3s
50332700	ddt
50332728	socks
50332747	rmiregistry
50332831	llsurfup-http
50332832	llsurfup-https
50332842	openvpn
50332862	kazaa

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50332915	epc
50332948	h323hostcallsc
50332992	icap
50333000	lotusnote
50333065	timbuktu-srv
50333081	ms-sql-s
50333082	ms-sql-m
50333137	dmdocbroker
50333142	ica
50333146	sybase-sqlany
50333160	wins
50333173	orasrv
50333195	laplink
50333206	xingmpeg
50333252	icabrowser
50333275	t128-gateway
50333325	groupwise
50333349	l2tp
50333366	h323gatedisc
50333367	h323gatestat
50333368	h323hostcall
50333371	pptp
50333389	cisco-net-mgmt
50333393	remote-winsock
50333396	oracle-em1
50333403	ms-streaming
50333449	msmq
50333460	radius
50333461	radius
50333511	msnp
50333548	ssdp
50333571	pkt-krb-ipsec
50333620	intersys-cache
50333621	dcap
50333626	unisql
50333633	hsrp

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50333641	cisco-snmp-tcp-port
50333645	gdp-port
50333646	x25-svc-port
50333647	cisco-ident-port
50333648	cisco-sccp
50333689	interbase
50333697	nfs
50333713	dlsrpn
50333715	dlswpn
50333754	mzap
50333771	gtp-control
50333800	gtp-user
50333838	tivoconnect
50333868	netiq
50333870	ethernet_ip
50333894	pc-mta-addrmap
50333961	iapp
50334030	ms-olap3
50334031	ms-olap4
50334049	cvspserver
50334052	iec-104
50334075	mgcp-gateway
50334140	groove
50334160	citrixima
50334161	citrixadmin
50334192	novell-zen
50334235	masc
50334246	citriximaclient
50334276	dict
50334375	mgcp-callagent
50334423	smpp
50334535	wlccp
50334552	m2ua
50334553	m3ua
50334592	megaco-h248
50334615	ssc-agent

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50334662	broker_service
50334664	notify_srvr
50334666	srvc_registry
50334667	resource_mgr
50334698	gds_db
50334778	icpv2
50334793	csi-lfap
50334853	isns
50334873	fcip
50334912	ccmail
50334916	msft-gc
50334917	msft-gc-ssl
50334931	net-assistant
50334936	cops
50334954	mysql
50335000	ssql
50335005	adtech-test
50335020	tip2
50335034	gprs-data
50335037	ms-wbt-server
50335044	printer_agent
50335068	ifcp
50335126	stun
50335131	slim-devices
50335151	lsp-ping
50335192	teredo
50335198	ssmpp
50335213	m2pa
50335280	distcc
50335307	apple-sasl
50335361	tftps
50335432	bfd-control
50335511	asap
50335516	diameter
50335969	rwhois
50336148	ipsec-nat-t

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50336217	iax
50336387	ipfix
50336388	ipfixs
50336547	radmin-port
50336650	rfe
50336708	sip
50336709	sip-tls
50336714	stanag-5066
50336798	atmp
50336838	aol
50336870	xmpp-client
50336894	capwap-control
50336895	capwap-data
50336917	xmpp-server
50337080	postgresql
50337279	pcanywheredata
50337280	pcanywherestat
50337326	rrac
50337361	proshare
50337377	openmail
50337548	vnc
50337635	wbem
50337648	x11
50337771	backup-express
50337991	sflow
50337994	gnutella
50338313	ircu
50338648	afs3
50338921	oma-rlp
50338923	oma-ulp
50338924	oma-ilp
50339275	soap-http
50339296	cuseeme
50339748	xprint-server
50339764	cp-cluster
50340091	pcsync-https

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
50340092	pcsync-http
50340736	sqlexec
50340748	up-bdl.-detester
50340848	wap-wsp
50340849	wap-wsp-wtp
50340850	wap-wsp-s
50340851	wap-wsp-wtp-s
50340852	wap-vcard
50340853	wap-vcal
50340854	wap-vcard-s
50340855	wap-vcal-s
50341523	sapv1
50341548	iua
50341648	ndmp
50341728	amanda
50341936	blocks
50345649	sua
50348032	connected
50351648	dnp
50353493	webphone
50357648	quake
50357909	ezmeeting
50364416	filenet
50379456	bacnet
201326593	ipv4
201326594	arp
201326595	ipv6
201326596	ether2
201326597	llc
201326598	snap
201326600	chaosnet
201326601	wol
201326603	vecho
201326604	dec
201326605	mop
201326606	drp

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
201326607	lat
201326608	dec-diag
201326609	lavc
201326610	apollo
201326611	rarp
201326612	dstp
201326613	atalk
201326614	aarp
201326615	vlan
201326616	mac-ctrl
201326617	ppp
201326618	gsmp
201326619	mpls
201326620	pppoe
201326621	ans
201326622	3gpp2-a10
201326623	eapol
201326624	hyperscsi
201326625	aoe
201326626	802-1ad
201326627	ieee-802a
201326628	erspan
201326629	rsn-preauth
201326630	tipc
201326631	lldp
201326632	lltd
201326633	802-1ah
201326634	cfm
201326635	fcoe
201326636	sia
201326637	loopback
201326638	sna-th
201326639	stp
201326640	netbeui
201326641	osi
201326642	cisco-snap

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
201326643	tagswitch
201326644	vsi
201326645	pagp
201326646	cipc
201326647	sstb
201326648	cstb
201326649	l2rly
201326650	udld
201326651	rbcp
201326652	cdp
201326653	cgmp
201326654	vtp
201326655	disl
201326656	ieee-slow-protocols
201326657	mac-sec
201326658	boardwalk
201326659	mdshdr
201326660	goose
201326661	ieee802-15-4
218103808	unclassified
218103809	unknown
218103834	netbios
218103849	syslog
218103855	novadigm
218103869	rtp
218103874	rtcp
218103875	edonkey
218103876	winmx
218103877	bittorrent
218103878	directconnect
218103885	yahoo-messenger
218103886	mapi
218103888	cifs
218103892	sap
218103918	tzsp
218104064	biff

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
218104065	who
218104066	asf-rmcp
218104073	hotline
218104074	manolito
218104075	soulseek
218104076	napster
218104077	icq
218104078	uma
218104079	quake3
218104140	dce-rpc
218104141	smtps
218104142	mtp3
218104143	sccp
218104144	tup
218104145	isup
218104146	isup-b
218104147	isup-s
218104148	alcap
218104149	bicc
218104150	h245
218104151	portmapper
218104152	rstat
218104153	nis
218104154	mount
218104155	rwall
218104156	yppasswd
218104157	spray
218104158	nlm
218104159	bootparams
218104160	ypxfr
218104161	nfsacl
218104162	nfsauth
218104163	nisplus
218104164	nisplus-cb
218104165	ms-exch-nspi
218104166	ms-frs

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
218104167	ms-frsapi
218104168	ms-ad-rep
218104169	ms-rfr
218104171	wccp
218104172	quake2
218104173	netflow
218104174	cisco-q931-backhaul
218104175	sametime
218104176	saa-rtr
218104177	cisco-callmanager
218104178	vt-advantage
218104179	3gpp2-a11
218104180	imode
218104181	openft
218104182	zebra
218104183	netsync
218104184	ajp13
218104185	tpcp
218104186	lwapp
218104187	synergy
218104188	lwres
218104189	oicq
218104190	commvault
218104191	ibm-tsm
218104192	legato-networker
218104193	legato-replistor
218104194	veritas-backupexec
218104195	veritas-netbackup
218104196	ms-netmeeting
218104197	vocaltec
218104198	siebel
218104199	apple-ichat
218104200	grouper
218104201	laplink-sharedirect
218104202	qnext
218104203	altiris-carboncopy

Table B-7 Application ID Collect Field Information (continued)

Application ID	Application Name
218104204	controlit
218104205	danware-netop
218104206	remote-anything
218104207	vmware-vmconsole
218104208	ms-content-repl-srv
218104209	netapp-snapmirror
218104210	pervasive-sql
218104211	liquid-audio
218104212	bmc-patrol
218104213	hp-openview
218104214	ibm-tivoli
218104215	landesk
218104216	netopia-netoctopus
218104217	flowmonitor
218104218	double-take
218104219	netlogon

INDEX

A

B

C

D

E

F

G

H

I

L

M

N

O

P

Q

R

S

T

U

V