Release Notes for the Cisco NetFlow Generation Appliance

Release 1.0 (2)

November 21, 2012, OL-26941-01

This release note includes important information about Cisco NetFlow Generation Appliance (Cisco NGA) Software Release 1.0 (2) and contains the following sections:

- New and Changed Information, page 1
- Cisco NGA New Features, page 2
- Cisco NGA 1.0 (2) Bugs, page 8
- Documentation Updates, page 11
- Product Documentation, page 23
- Obtaining Documentation and Submitting a Service Request, page 24

You can access the most current Cisco NGA documentation, including these release notes, online at the Cisco NetFlow Generation Appliance page on Cisco.com.

New and Changed Information

The following sections describe release information that is pertinent to Cisco NetFlow Generation Appliance Software Release 1.0 (2).

November 21, 2012	Hardware release of Cisco NetFlow Generation Appliance 3240 and software version 1.0 (2), with enhancements and bug fixes and Cisco NGA 3140 software version 1.0 (1) upgrade support.
May 18, 2012	Initial hardware release of Cisco NGA 3140 with software version 1.0 (1).

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco NGA New Features

Cisco NetFlow Generation Appliance (NGA) provides network visibility and establishes a new standard for cross-device flow visibility. It empowers network operations, engineering, and security teams with actionable insight into network traffic for the purpose of resource optimization, application performance improvement, traffic accounting, and security needs.

Cisco NGA 3240 is preinstalled with the Cisco NetFlow Generation Appliance Software Release 1.0 (2). Cisco NGA 3140 users can upgrade to this Cisco NGA software release. For upgrade instructions, see Using Virtual Media to Install or Recover Cisco NGA, page 22 and the *Quick Start Guide for the Cisco NetFlow Generation Appliance*.

The following topics describe new features and enhancements in Cisco NGA 1.0 (2):

- New Device Support, page 2
- Visibility into Switch Interface Data for Managed Device Flows, page 2
- TCP Flags Enhancement, page 2
- Increase Flow Cache Size, page 3
- Session Timeout for TCP, page 3
- Virtual Media Support, page 3

For detailed feature descriptions see the "Key Features" section in the *User Guide for Cisco NetFlow Generation Appliance.*

For the most up-to-date support information and documentation updates, see the online release notes on Cisco.com.

New Device Support

Cisco NGA 1.0 (2) adds support for the Cisco Nexus 3000 Switch device as a Cisco managed device. For details, see Configure Your Traffic Sources, page 13. For version support information, see the *Cisco NetFlow Generation Appliance Compatibility Matrix.*

Visibility into Switch Interface Data for Managed Device Flows

You can now access switch interface information for Cisco Nexus 3000, 5000, and 7000 Series switch flows using the managed device feature. The following switch MIB-2 and IF-MIB objects are mirrored in the Cisco NGA ifTable for the configured managed devices: ifName, ifDescr, ifAlias, ifType, ifMtu, ifSpeed, and ifHighSpeed. This enhancement provides accurate NetFlow interface information without impairing switch performance.

For version support information, see the *Cisco NetFlow Generation Appliance Compatibility Matrix.*

TCP Flags Enhancement

In Cisco NGA 1.0 (1), the bits in the TCP flag field collected were cumulative over the life of a particular flow. To improve security, TCP flag bits are now reset after each flow export so that only the flags that have been observed since the last export are reported. The reporting period is the active timeout interval. This enhancement helps collector applications that are interested in security-oriented data. By clearing the flags after each export, collectors that use NetfFlow to search for network attacks can detect SYN-flood attacks more readily.

Increase Flow Cache Size

The active flow cache size has been increased to 80 million flows.

Session Timeout for TCP

The TCP flows are now reported instantly when they are closed instead of using a fixed delay. This enhancement optimizes the TCP flows to provide more efficient cache management.

Virtual Media Support

The Cisco NGA 3240 hardware release no longer supports a CD/DVD and requires you to use virtual media for installations and upgrades. For instructions on how to use the Cisco NGA built-in management tool to perform various tasks, see Using Virtual Media to Install or Recover Cisco NGA, page 22.

CIMC virtual media support on the Cisco NetFlow Generation Appliance 3140 (as well as the 3240). For details on how to use the CIMC and the specific helper options you should choose, see Using the CIMC, page 21.

Note This software is preinstalled on a UCS C-Series server. Where applicable, documentation may reference the UCS C-Series guides for hardware-specific tasks such as rack mounting and technical specifications. Because Cisco NGA is the only application running on this appliance, it does not require you to perform any maintenance or configuration tasks that may be associated with the UCS C-Series server. We recommend you do not attempt to open the appliance unless directed by a customer support representative.

Device Support

Managed device support now includes the Nexus 3000 Series switches. For details on the list of supported Cisco managed devices and their software versions, see the *Cisco NetFlow Generation Appliance Compatibility Matrix.*

Common Deployment Scenarios

This release note includes the following examples to help illustrate several configuration scenarios for your Cisco NGA.

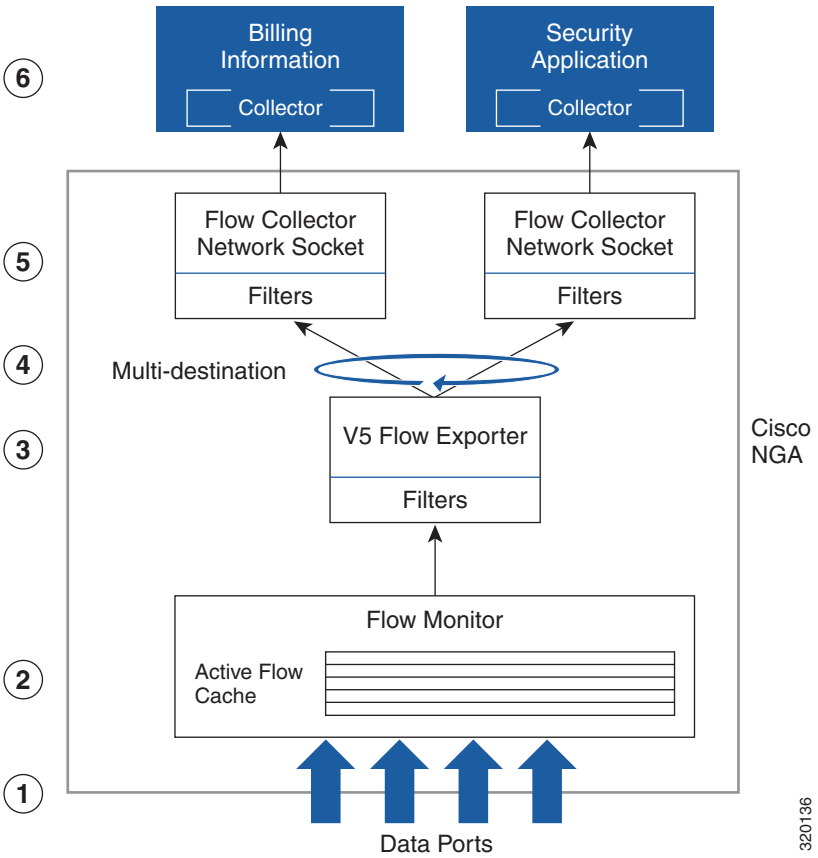
- Single Source of Flow Visibility for Multiple Management Applications, page 4
- Fabric Path Domain Flow Visibility in the Data Center, page 5
- Collect Data Using Various Export Formats to Support Multiple Management Applications, page 7

Single Source of Flow Visibility for Multiple Management Applications

Figure 1 shows a configuration example of the Cisco NGA flow components that use the same traffic flows but allow you to filter flow data about specific applications; for example, if you want to verify application specific flows that enable you to charge a customer for usage, use this type of configuration. The numbered list below the figure corresponds to the callouts in Figure 1 and describes each component in this configuration example.

The quickest way to configure this type of scenario is to use the Quick Setup, then add the second flow collector using the Advanced Setup. For instructions, see the *Quick Start Guide for the Cisco NetFlow Generation Appliance*.

Figure 1 Deployment for Single or Multiple Device Traffic Flows for Multiple Application Data

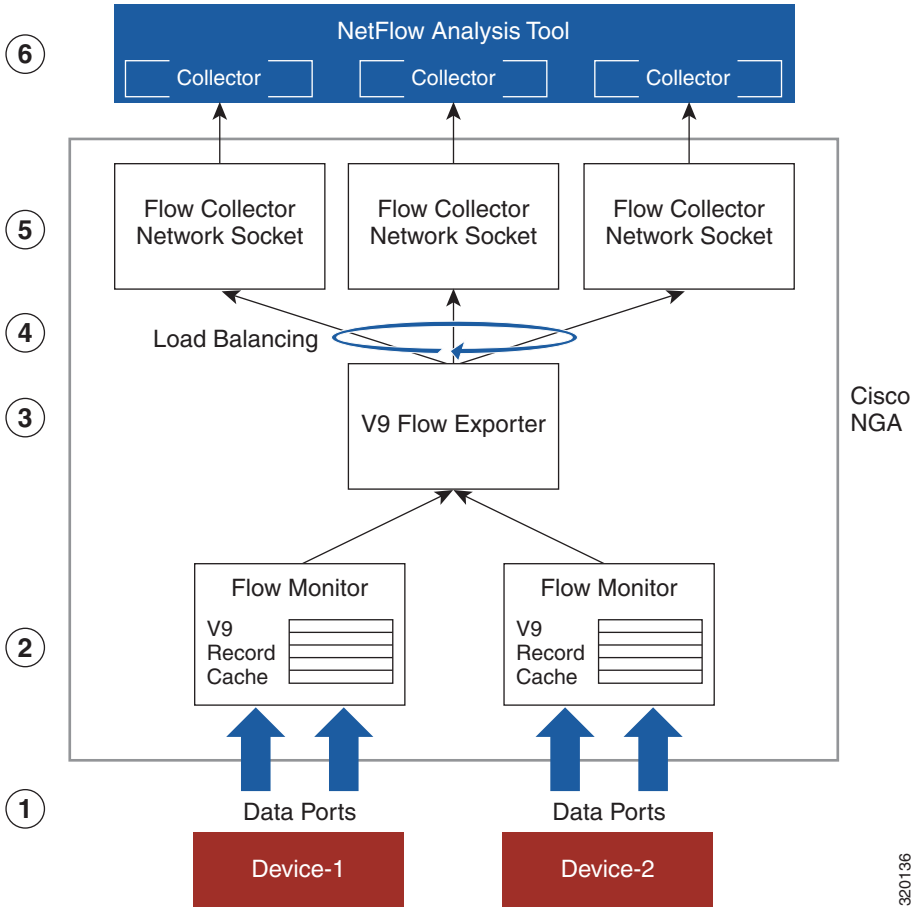


1	Configure traffic from one or more network devices to Cisco NGA using SPAN or a passive network tap. For details on how to configure SPAN or a tap device, see your device documentation.
2	Configure a flow monitor with all four interfaces from your switch (which could be an access or aggregation switch).
3	Configure a single v5 flow exporter to receive traffic on all four data ports. The flow exporter manages the flows with the same filters to support one format; in Figure 1 the exporter supports v5 format.
4	Configure multi-destination policies to replicate the flows across multiple collectors. This enables you to use the same traffic flows across all collectors for the purpose of separate management tasks.
5	Configure a filter for billing purposes by selecting the source IP address and source port number in the Advanced Setup Filter configuration window. Alternately, if you have a v9 flow exporter use the application ID defined in the record, you may filter on the application instead of the port number. For details on configuring the Advanced Setup filters, see the *User Guide for Cisco NetFlow Generation Appliance.*
6	Use your NetFlow collectors to produce reports, graphs, and analysis of the data.

Fabric Path Domain Flow Visibility in the Data Center

Figure 2 shows a configuration example of the Cisco NGA flow components that help you to analyze Layer 2 traffic flows from two or more switches within the data center using load balancing policies; for example, to filter specific flows across all collectors, use this type of configuration. The numbered list below the figure corresponds to the callouts in Figure 2 and describes each component in this configuration example.

Figure 2 Deployment for Fabric Path Domain Flow Visibility in the Data Center



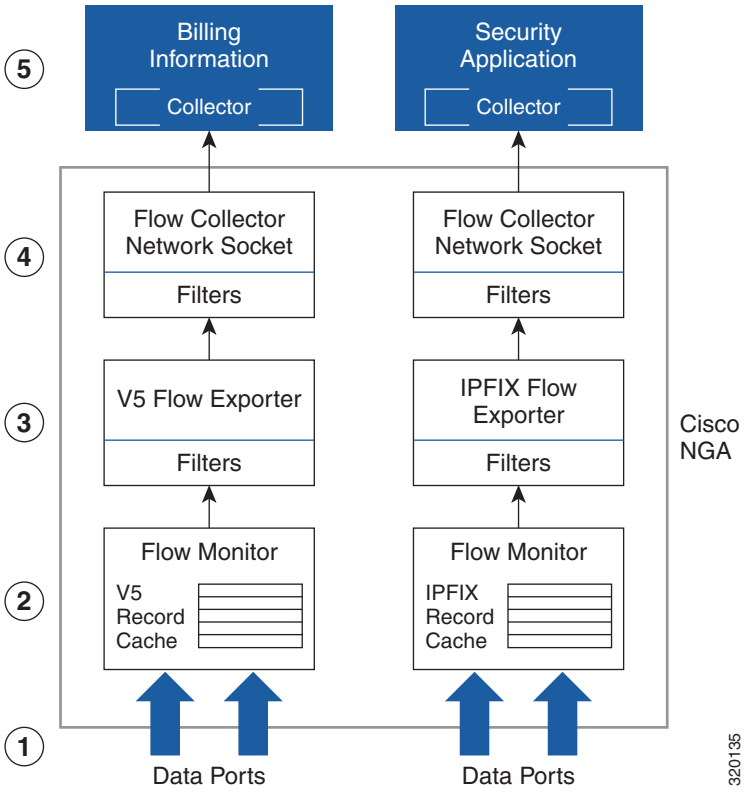
1	Configure traffic from two (or more) network devices in the Fabric Path domain to Cisco NGA using SPAN or a passive network tap. This enables you to analyze Layer 2 traffic flows within the data center. For details on how to configure SPAN or a tap device, see your device documentation.
2	Configure your flow monitors with two interfaces from each device (which could be an access or aggregation switch). For details on configuring the Advanced Setup flow monitors, see the *User Guide for Cisco NetFlow Generation Appliance.*
3	Configure multiple flow exporters to receive traffic from different devices on all four data ports. The flow exporter manages the flows with the same filters to support one format; in Figure 2 the exporter supports v9 format. In this mode, only one level of filters are allowed; the filters that are associated with the flow exporter. Having only a single set of filters applied at the exporter level allows the appliance to accurately honor the round-robin weight assignments.

4	Configure load balancing policies to spread the flows across multiple collectors. This enables you to avoid high traffic flows on any one collector and improve scalability. For details on configuring the Advanced Setup filters, see the *User Guide for Cisco NetFlow Generation Appliance.*
5	When collectors are configured in load-balancing mode you can apply filters at the exporter level only.
6	Use your NetFlow collectors to produce reports, graphs, and analysis of the data.

Collect Data Using Various Export Formats to Support Multiple Management Applications

Figure 3 shows a configuration example of the Cisco NGA flow components that help to gather flow data using different export formats. This scenario supports flow visibility into multiple management applications such as billing (using NetFlow v5 format) and security (using IPFIX format). The numbered list below the figure corresponds to the callouts in Figure 3 and describes each component in this configuration example.

Figure 3 Deployment with Different Export Formats Collecting Multi-Application Data



1	Configure traffic to Cisco NGA using SPAN or a passive network tap. A flow monitor can be configured to listen to up to four data ports. For details on how to configure SPAN or a tap device, see your device documentation.
2	Configure one or more flow monitors to export multiple export formats. Figure 3 depicts v5 and IPFIX exporters. Each exporter can work independently using different traffic input based on the requirements of your management application.
3	Configure multiple flow export filters to funnel application traffic based on specific management applications. For details on configuring the Advanced Setup flow filters, see the *User Guide for Cisco NetFlow Generation Appliance*.
4	Given that filtering has been configured at the flow exporter, no extra filtering is required at the flow collector.
5	Use your NetFlow collectors to produce reports, graphs, and analysis of the data.

Cisco NGA 1.0 (2) Bugs

This section provides information about open and resolved bugs in the Cisco NGA Software Release 1.0 (2) software release.

- Open Bugs in Cisco NGA 1.0 (2), page 8
- Resolved Bugs in Cisco NGA 1.0 (2), page 9
- Using the Bug Tool Kit, page 10

To obtain more information about known problems, access the Cisco Software Bug Toolkit at the following URL:

http://www.cisco.com/cgi-bin/Support/Bugtool/home.pl

Open Bugs in Cisco NGA 1.0 (2)

Table 1 provides a list of open bugs in Cisco NGA Software Release 1.0 (2).

Click on the identifier to view the impact and workaround for the bug. This information is displayed in the Using the Bug Tool Kit, page 10. You can track the status of the open bugs, using the Bug Toolkit.

Table 1 Known Bugs in Cisco NGA 1.0 (2)

Identifier	Description
CSCub92559	wget, wget, cURL and libcURL NTLM Buffer Overflow Vulnerability
CSCub92557	Dojo Toolkit Multiple Cross-Site Scripting Vulnerabilities
CSCub92555	Xinetd TCPMUX Unauthorized Remote Access Vulnerability
CSCub92553	php PHP SQLite open_basedir Protection Security Bypass Vulnerability
CSCtz39289	Application restarts if over 64 million flows terminate simultaneously
CSCtz26355	Linux-2.6.33: Linux Kernel kexec Tool StrictHostKeyChecking Default Configuration Value Remote Man-in-the-middle Vulnerability
CSCtz26351	Linux-2.6.33: Linux Kernel kexec-tools initrd Ramdisk Image File Creation Local Information Disclosure Issue

Table 1 Known Bugs in Cisco NGA 1.0 (2)

Identifier	Description
CSCty55708	Negative value should not be accepted in Flow Filter field
CSCty53026	Inaccurate SNMP community string in Tech Support rpt or show tech CLI
CSCty37106	Login GUI does not remember username
CSCty02430	L2 traffic may not be distributed evenly among the processing threads
CSCtx81861	php P1HP zend_strndup() Denial of Service Vulnerability
CSCtx65963	OpenSSL: OpenSSL ECDSA Private Key Disclosure Vulnerability
CSCtx65951	Linux-2.6.33 Linux Kernel TCP Sequence Number Generator Packet Injection Vulnerability

Resolved Bugs in Cisco NGA 1.0 (2)

Table 2 provides a list of resolved bugs in Cisco NGA Software Release 1.0 (2).

Table 2 Resolved Bugs in Cisco NGA 1.0 (2)

Identifier	Description
CSCtz26358	Linux-2.6.33: Linux Kernel CIFS Mount is_path_accessible Validation Check Processing Remote Denial of Service Vulnerability
CSCtz26356	Linux-2.6.33: Linux Kernel Network Drivers Priority Tagged Data Frames Processing Remote Denial of Service Vulnerability
CSCtz26348	OpenSSL: OpenSSL ASN.1 Parser Incorrect S/MIME Header Processing Denial of Service Vulnerability
CSCty99097	OpenSSL: CMS, PKCS #7, or S/MIME Decryption Routines MMA Security Bypass Vulnerability
CSCty67785	Using Microsoft Internet Explorer version 9, the GUI may not display some configuration check boxes.
CSCty65650	Using the GUI to set local time synchronization does not work properly.
CSCty55686	Undefined error message is displayed when the Delete button is pressed.
CSCty04438	php: PHP magic_quote_gpc Security Bypass Remote SQL Injection Vulnerability
CSCtx81870	OpenSSL: OpenSSL SSL_CTX_new Uninitialized Buffer Remote Information Disclosure Vulnerability
CSCtx81860	OpenSSL: OpenSSL SSL3_FLAGS_SGC_RESTART_DONE Flag SGC Handshake Restart Denial of Service Vulnerability
CSCtx81859	OpenSSL: OpenSSL Datagram Transport Layer Security Plaintext Recovery Issue
CSCtx81858	OpenSSL: OpenSSL X509_V_FLAG_POLICY_CHECK Denial of Service Vulnerability
CSCtx65965	OpenSSL: OpenSSL Elliptic Curve Diffie-Hellman Ciphersuite Denial of Service Vulnerability
CSCtx65961	Linux-2.6.33: Linux Kernel l2cap_config_req() Function Integer Underflow Remote Denial of Service Vulnerability
CSCtx65957	Linux-2.6.33: Linux Kernel Generic Receive Offload Denial of Service Vulnerability
CSCtx65955	Linux-2.6.33: Linux Kernel nfs-util Remote Unauthorized Access Vulnerability
CSCtx20018	php: Multiple Products Hash Collisions Denial of Service Vulnerability

Using the Bug Tool Kit

This section explains how to use the Bug Toolkit to search for a specific bug or to search for all bugs in a release.

Step 1 Go to http://tools.cisco.com/Support/BugToolKit.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Toolkit page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, click the Search Bugs tab, enter the bug ID in the Search for Bug ID field, and click **Go**.

Step 4 To search for bugs in the current release, click the Search Bugs tab and specify the following criteria:

- Select Product Category—Network Management and Automation.
- Select Products—[Product Name].
- Software Version—[Product Version].
- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.
- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, click Use custom settings for severity, status, and others and specify the following information:
  - Severity—Choose the severity level.
  - Status—Choose Terminated, Open, or Fixed.

    Choose Terminated to view terminated bugs. To filter terminated bugs, uncheck the Terminated check box and select the appropriate suboption (Closed, Junked, or Unreproducible) that appears below the Terminated check box. Select multiple options as required.

    Choose Open to view all open bugs. To filter the open bugs, uncheck the Open check box and select the appropriate suboptions that appear below the Open check box. For example, if you want to view only new bugs in Prime Optical 9.5, choose only New.

    Choose Fixed to view fixed bugs. To filter fixed bugs, uncheck the Fixed check box and select the appropriate suboption (Resolved or Verified) that appears below the Fixed check box.
  - Advanced—Check the Show only bugs containing bug details check box to view only those bugs that contain detailed information, such as symptoms and workarounds.
  - Modified Date—Choose this option to filter bugs based on the date when the bugs were last modified.
  - Results Displayed Per Page—Specify the number of bugs to display per page.

Step 5 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Step 6 To export the results to a spreadsheet:

a. In the Search Bugs tab, click **Export All to Spreadsheet**.

b. Specify the filename and location at which to save the spreadsheet.

c. Click **Save**. All bugs retrieved by the search are exported.

If you cannot export the spreadsheet, log into the Technical Support website at http://www.cisco.com or contact the Cisco Technical Assistance Center (TAC).

Documentation Updates

This section contains information about errors, omissions, and changes for Cisco NetFlow Generation Appliance 1.0 documentation and online help.

The following information is more recent than the existing Cisco.com documentation and online help:

- Updates for Quick Start Guide, page 11
- Updates for User Guide, page 16

Updates for Quick Start Guide

The following sections in the *Quick Start Guide for the Cisco NetFlow Generation Appliance* are updated below for release 1.0 (2) as follows:

- Requirements and Restrictions, page 11
- Rear Panel for Cisco NGA 3240, page 11
- Front Panel for Cisco NGA 3240, page 12
- Supported Upgrade Path, page 13
- Configure Your Traffic Sources, page 13
- Field Replaceable Units (FRU) Components, page 20
- Cisco NGA 3240 Technical Specifications, page 15

We recommend you review the *Quick Start Guide for the Cisco NetFlow Generation Appliance 3240* and refer back to the release notes for recently updated details.

Requirements and Restrictions

Browser support includes the following tested browsers:

- Mozilla Firefox ESR 10
- Microsoft Internet Explorer 9

For additional compatibility information, see the *Cisco NetFlow Generation Appliance Compatibility Matrix*.

Rear Panel for Cisco NGA 3240

The rear panel for the Cisco NGA 3240 is described in Figure 4. Cisco NGA software comes preinstalled on the UCS 220 M3 server and is referred to in the product documentation as the Cisco NetFlow Generation Appliance, or the appliance.

Note Rear panel port numbers mirror the location numbers in Figure 4. They are unlike standard port numbers, so take special note.

Figure 4 Cisco NGA 3240 Rear Panel

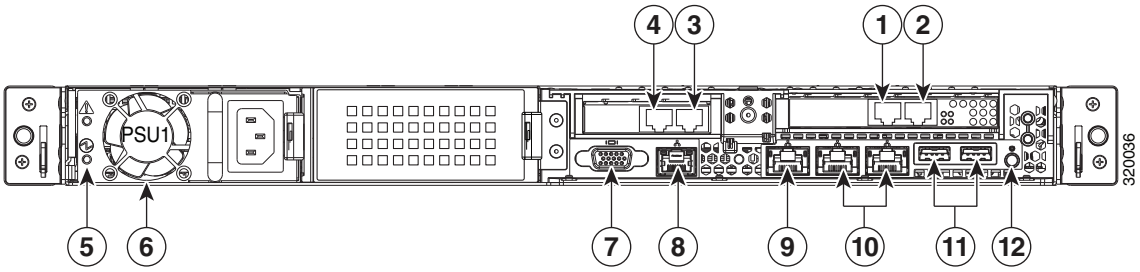


Table 3 Rear Panel Location Numbers

1	Data port #1	**7**	VGA video connector
2	Data port #2	**8**	Serial port (RJ-45 connector)[1]
3	Data port #3	**9**	CIMC Ethernet port (RJ45)[2]
4	Data port #4	**10**	Dual 1-Gb Ethernet ports (LAN1 and LAN2)[3]
5	Power supply LED	**11**	USB ports
6	Power supply	**12**	Rear Identification button/LED

1. Connect to local terminal server
2. Required only if you plan to use the UCS management center software
3. Only one port is used as a management port for Cisco NGA (LAN1); additional port is reserved for future use

Front Panel for Cisco NGA 3240

The front panel for the Cisco NGA 3240 is described in Figure 5. Cisco NGA software comes preinstalled on the UCS 220 M3 server.

Figure 5 Cisco NGA Front Panel

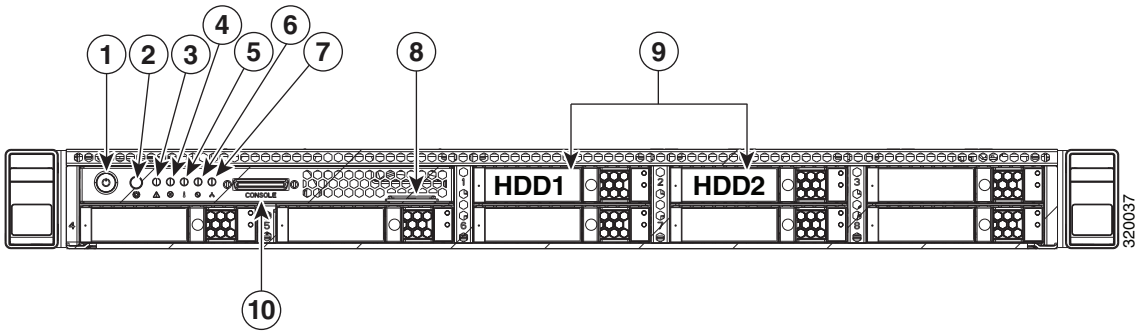


Table 4 Cisco NGA 3240 Front Panel

1	Power button/Power status LED[1]	**6**	Power supply status LED
2	Identification locator button/Locator LED	**7**	Network link activity LED

Table 4 Cisco NGA 3240 Front Panel (continued)

3	System status LED	**8**	Pull-out asset tag
4	Fan status LED	**9**	Hard disk drives (2)
5	Temperature status LED	**10**	KVM console port[2]

1. Use only when a forced shutdown is necessary. Hold down for several seconds until light is no longer lit with a green color.
2. Use with KVM cable that provides two USB, one VGA, and one serial connector. You can connect to an optional keyboard and VGA monitor.

Supported Upgrade Path

Table 5 provides details on the commands to use for Cisco NGA backup, upgrade, and restore tasks.

Table 5 Backup, Upgrade, and Restore Information

Task	Preferred Method	Command
Back up Cisco NGA version 1.0 (1) or 1.0 (2)	CLI	**config upload**
Upgrade Cisco NGA 3140, v 1.0 (1) to 1.0 (2)	CLI	**upgrade ftp**
Restore configuration v 1.0 (1) or 1.0 (2)	CLI	**config network**
Recovery (only when catastrophic event occurs)	CIMC	power cycle server or use helper utility

Configure Your Traffic Sources

This section includes updates to the existing product documentation which now includes the Cisco Nexus 3000 Series switch as a managed device.

Cisco NGA supports network devices that can direct traffic to Cisco NGA using standard SPAN. For traffic sources that are supported Cisco managed devices, you can also collect interface information for the traffic sources. For specific Cisco managed device support versions, see the marketing documentation on Cisco.com.

There are two tasks to configuring your traffic sources. The traffic source in Cisco NetFlow Generation Appliance can be 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 3000, Nexus 5000, or Nexus 7000 Series switch. For a list of supported platforms, see the *Cisco NetFlow Generation Appliance Compatibility Matrix*.

1. (Required) Create a Switched Port Analyzer (SPAN) session (also known as port mirroring) on your switch or router using the 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 document does not provide details on how to create SPAN sessions or to use a network tap device. For details on how to set up these configurations, see your device documentation.

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

If your traffic source is one of the supported Cisco switches or routers and you want the appliance to export flow records with the input and output interface of the device rather than data port 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 14.

One of the benefits of configuring a managed device on the Cisco NGA allows the appliance to gather the interface index from the device. Cisco NGA populates exported NetFlow records with the interface (ifIndex) values from the device that is being monitored, rather than the interface values from the appliance itself.

For example, in a scenario when a flow enters a Cisco Nexus switch on interface 50 and leaves on interface 60, and it is also being replicated (through SPAN) to interface 2 of the appliance, if the Cisco Nexus switch is configured as the managed device, Cisco NGA can report input interface 50 and output interface 60 for the flow. Otherwise, it will report interface 2 for both input and output, as this is the Cisco NGA interface on which a copy of the flow is received. Note that the managed device feature support is limited to platforms indicated in the *Cisco NetFlow Generation Appliance Compatibility Matrix.*

Note SSH must be enabled on the remote Nexus device in order for Cisco NGA to access interface information. For details on how to enable SSH on the Nexus OS, see the device documentation.

Configure the IP Address of Your Traffic Source

One of the benefits of configuring the IP address of your supported Nexus 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:

Step 1 To configure up to four Nexus Series switch 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 1-6 for field descriptions.
- To edit an existing managed device, select the row, click **Edit** then enter the device information.
- To delete a managed device, select the row and click **Delete**.

Table 1-6 Managed Devices Table Field Descriptions

Field	Field Description
Address	Device IP address. Use the IP address and not the domain name.
Username/Password Verify Password	Enter the managed device (switch or router) access credentials.
Data Ports	Enter the appliance data ports that are connected to the managed device (for example, the Nexus 3000, 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 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*. A NetFlow monitor instance consists of a flow monitor, collector, and exporter for v5 and a flow monitor, collector, exporter, and record name for v9. Then use Advanced Setup if you require additional flow components or filters.

Cisco NGA 3240 Technical Specifications

The following table contains links to the technical specifications for the Cisco NetFlow Generation Appliance 3240. Cisco NGA is an integrated hardware platform that is preinstalled with the Cisco NetFlow Generation Appliance Software Release 1.0 (2) on the UCS C220 M3 server.

Specification	See...
Physical	The *Physical Specifications* section in the *Cisco UCS C220 Server Installation and Service Guide*.
Environmental	The *Environmental Specifications* section in the *Cisco UCS C220 Server Installation and Service Guide*.
Power	The *Power Specifications* section in the *Cisco UCS C220 Server Installation and Service Guide*. Cisco NGA ships with a 650W power supply.

For more information about the Cisco UCS C220 server, see the *Cisco UCS C220 Server Installation and Service Guide*.

Updates for User Guide

Several updates did not make it into to the *User Guide for Cisco NetFlow Generation Appliance* after the release was published. To view the latest product information, review the updates in this section. For the product documentation set, see Cisco.com.

The following sections are new or replace existing content in the user guide for release 1.0 (2):

- Overview of Cisco NGA Flow Components, page 16
- Examples of Deployment Scenarios, page 20
- Miscellaneous Updates, page 21
- Using Virtual Media to Install or Recover Cisco NGA, page 22

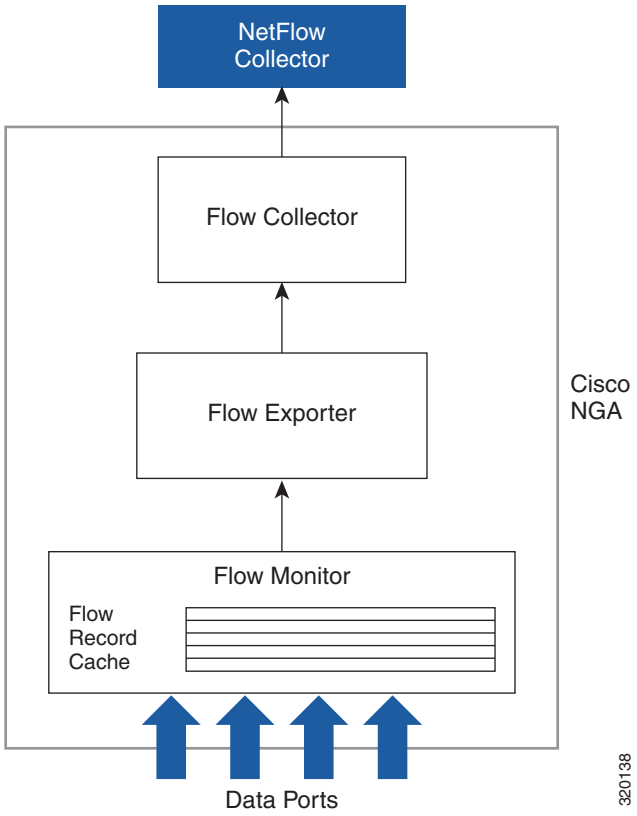
Overview of Cisco NGA Flow Components

Cisco NGA uses flow components, or standard NetFlow configurations, to customize the traffic analysis parameters for your specific requirements. You can quickly set up a single NetFlow *monitoring instance* which is the minimum set of flow components required using the Quick Start workflow.

For advanced configurations where multiple NetFlow monitoring instances are desired or advanced features such as filters and customizing v9 and IPFIX record parameters are needed, you can use the Advanced Setup workflow.

Figure 6 depicts the simplest deployment scenario. It is an example of a Cisco NGA *monitoring instance*. Each monitoring instance contains a variable set of flow components based on your configuration. This is the minimum set of flow components that you must configure in the appliance to export NetFlow v5 data. For NetFlow v9 data export, the monitoring instance may contain any combination of the following: a flow monitor, exporter, collector, and record name. Configure this setup using the Advanced Setup menu. For definitions of Cisco NGA flow components, see Table 7.

Figure 6 Quick Setup Diagram of Cisco NGA Flow Components



You can connect up to four routers or switches to the appliance using the four data ports configured with SPAN sessions as described in Examples of Deployment Scenarios, page 20. Other configurations are also possible using a network tap device. For additional scenarios, see Common Deployment Scenarios, page 4. For an installation and configuration overview, see the *Quick Start Guide for Cisco NetFlow Generation Appliance*.

Table 7 defines each flow component and provides examples of how to configure them. Flow components can be combined to create various monitoring instances to address specific deployment needs. For details on the deployment methods you can choose for device support, see Examples of Deployment Scenarios, page 20.

Table 7 Cisco NGA Flow Components and Terms

Component[1]	Description	Uses/Importance
Flow monitor	A flow monitor is required to export flow cache data. You must create and activate at least one flow monitor for the system to begin exporting flows. You can create more than one flow monitor to monitor different sets of data ports and use different cache parameters. One data port can be used by one active monitor at any given time.	The flow monitor designates which data ports are monitored by the the appliance and specifies parameters for the flow cache operation. You can custom the following parameters: • The size of the cache • Timeout values and behavior • Which flow records are to be associated with the flow monitor When you use multiple flow monitors you can associate different data ports with each monitor. You can also associate different exporters with each monitor, and by doing so associate different collectors with each monitor. For example, you can attach four different switches to the appliance, so that you send the data from each switch to a different collector. In this case, you must create four distinct flow monitors, each one configured with the data port that is connected to the corresponding switch. Each flow monitor has its own flow exporter (so you can vary them to use either v5 or v9), and each of those exporters can be associated with a different collector.
Flow collector	Each flow collector within the Cisco NGA represents a construct (which may have associated filters). That internal construct, represented in the figure as a flow collector socket, is what you must explicitly configure. The NetFlow collector is an external device, separate from the Cisco NGA, to which the appliance can export flow records. Most collectors will store the flow data in a database and then produce reports, graphs, and analysis of the data. Use the Cisco NGA's flow collector configuration to specify the IP address and UDP port of your collectors.	A collector may specialize in traffic accounting, billing, monitoring traffic patterns on your network, or detecting potential security threats. Flow records exported by the Cisco NGA provide the necessary data to produce these reports. You may configure multiple collectors and the Cisco NGA exports data to each of them, either alternating between them in a round robin fashion, or replicating the same flow data to each collector. In this way you can deploy multiple collectors for different purposes. You can also spread the load across multiple collectors if one collector cannot keep up with the data rate exported by the Cisco NGA.

Table 7 Cisco NGA Flow Components and Terms (continued)

Component[1]	Description	Uses/Importance
Flow exporter	The flow exporter specifies which version of NetFlow Data Export format should be exported by the Cisco NGA. The flow exporter is also used to designate other parameters such as how often the Cisco NGA sends out NetFlow template updates, and which policy should be used if there are multiple collectors (replicate the same to data to each, or load balance among them). You may define filters in the flow exporter to specify exactly which flows are to be sent to each collector.	Ensure you choose a NetFlow Data Export format that is supported by your collectors. **Note** Cisco NGA is capable of generating a large amount of data. If necessary, use filters to reduce the load on your collector, or use multiple collectors in round robin load balancing mode.
Flow Filters (optional)	There are two configurable filter levels in Cisco NGA: one filter that defines which device record data to collect (collector) and one that defines what data to export to the NetFlow collectors (exporter). You can use filters to match specific fields within each flow record before it is exported. You can also reduce the demand on your collector by applying filters to reduce the number of flows that are actually exported by the appliance. You may apply specific filters to individual collectors, or you may apply filters globally in the flow exporter definition and they will apply to all collectors in that exporter.	The primary use of filters is to lighten the load on collectors that may not be able to keep up with a high export rate. Alternately, you may only be interested in flow data for a particular host, or set of hosts, or a particular application, and so on. In these cases, you can use filters to limit the data to only those flows that are of interest. Filters are not applicable for round robin export policy.
Flow Record (configurable in v9 and IPFIX)	A flow record is a basic unit of information exported by the Cisco NGA to collectors. Use the record configuration to specify which fields are used to uniquely identify a flow, and to specify which counters and information elements are to be exported for each flow.	The **Match** fields are treated as keys and are used to uniquely identify each flow. For example, you may want a particular flow to be identified by five parameters such as source IP address, destination IP address, source port number, destination port number, and IP protocol value. Or to effectively aggregate several flows together you can select fewer **Match** fields. For example by selecting only the source and destination IP address. In that case, several connections which use different port numbers are aggregated into a single flow record for export. The **Collect** fields collect additional data in the flow that you can specify; such as packet count, byte count, TCP flags, and so on.

Table 7 Cisco NGA Flow Components and Terms (continued)

Component[1]	Description	Uses/Importance
Managed Device	A supported Cisco switch or router that is configured so that the Cisco NGA can gather NetFlow data such as interface details. For specific Cisco switch and router platform support, see the *Cisco NetFlow Generation Appliance Compatibility Matrix.*	One of the benefits of configuring a managed device on the Cisco NGA is that it allows the appliance to gather the interface index from the device as well as the interface name. Cisco NGA populates exported NetFlow records with the interface (ifIndex) values (ifName, ifDescr, ifAlias, ifType, ifMtu, ifSpeed, and ifHighSpeed) from the device that is being monitored, rather than the interface values from the appliance itself.

1.For details on how to configure these components, see the *Quick Start Guide for Cisco NetFlow Generation Appliance* or the *User Guide for Cisco NetFlow Generation Appliance.*

Examples of Deployment Scenarios

The following content clarifies the deployment methods, or scenarios, that Cisco NGAsupports.

You can direct packets to the Cisco NGA using either or both of the following deployment scenarios:

- A Switched Port Analyzer (SPAN) session (also known as port mirroring) from the network device that supports this method. Port mirroring selects network traffic for analysis by a network analyzer. This is a low-cost alternative to network taps.

  You can choose to use SPAN, remote SPAN (RSPAN), or SPAN with port channels to monitor your traffic. To configure one of these SPAN methods on your Cisco Nexus or Catalyst devices to send traffic to the Cisco NGA, use the Nexus supervisor or the Catalyst IOS CLI. Using local SPAN uses four data ports, thus four routers or switches.

- A network tap. A network tap is a hardware device which provides a copy of the data that flows across a network link. By setting up a network tap using remote SPAN or Remote (RSPAN), you are able to monitor more than the four routers or switches you are limited to using local SPAN.

To understand how SPAN, RSPAN, and port channelling work on Cisco routers and switches and how to configure your network devices using standard SPAN, see your router and switch software configuration documentation.

Field Replaceable Units (FRU) Components

This section details links to manage the Cisco NGA Field Replaceable Units (FRUs):

- Removing and Replacing a Hard Disk Drive

  For information about replacing hard disk drives in the appliance, see the Replacing Hard Drives or Solid State Drives section in the *Cisco UCS C220 Server Installation and Service Guide*.

- Installing or Replacing a Power Supply

  For information about replacing power supplies, see the Replacing Power Supplies section in the *Cisco UCS C220 Server Installation and Service Guide.*

Miscellaneous Updates

The following details will be added to the user guide during the next release update:

- You must define a NetFlow v9 record counter field (such as packets or bytes) or no NetFlow data generates (since there is no data to collect).
- The v9 record name of an existing flow monitor may still be displayed after the particular flow monitor being edited and changed to exported NetFlow v5 type. The workaround is, while in flow monitor editing mode, use the backspace key to delete the Exporter name then un-select the v9 Record Name when this field becomes editable. Reselect the Exporter then save.
- When you use the CLI, if you have multiple existing filters and attempt to add another filter you must reenter all the filter names in order to add any new filters. We recommend you use commas with no spaces to separate the filters.
- Cisco NGA is now recovered using virtual media if necessary. The CD/DVD is no longer shipped. See Using Virtual Media to Install or Recover Cisco NGA, page 22 for instructions.
- Table 8 lists the ports used by the Cisco NGA for network communication.

Table 8 Ports Used by Cisco NGA in Network Deployments

Port	Description
TCP (22)	SSH—The port that Cisco NGA uses to collect configuration information from managed devices. **Note** SSH must be enabled on the remote Nexus device in order for Cisco NGA to access interface information. For details on how to enable SSH on the Nexus OS, see the device documentation.
TCP (23)	Telnet—Port used for Telnet.
TCP (80)	HTTP—Default port if Cisco NGA is configured for access using HTTP.
UDP (161)	SNMP—The port used to communicate with the Cisco NGA's SNMP Agent.
TCP (443)	HTTPS—Default port if Cisco NGA is configured for access using HTTPS.

Using the CIMC

The CIMC is a built-in management service provided with the Cisco NGA. CIMC provides a web-based GUI that enables you to perform tasks including:

- Manage remote presence with KVM console. The console is an interface accessible from CIMC and emulates a direct keyboard, video, and mouse (KVM) connection to the appliance. The KVM console allows you to connect to the appliance from a remote location. It also provides the "Virtual Media" feature used for recovery/ISO install. (See Using the KVM Console, page 22.)
- Power on, power off, power cycle, reset and shut down the appliance
- Toggle the locator LED to locate the appliance with blinking blue LED

For instructions on how to use the Cisco NGA built-in management tool to perform various tasks, see Using Virtual Media to Install or Recover Cisco NGA, page 22.

Using the KVM Console

The KVM console is an interface accessible from the Cisco NGA that emulates a direct KVM connection. The KVM console allows you to view the serial console remotely without any connection to a terminal server. It also provides the Virtual Media feature used for recovery/ISO install.

If you want to use the KVM console to access the appliance, you must ensure that either the appliance or the service profile associated with the appliance is configured with a CIMC IP address. The KVM console uses the CIMC IP address assigned to an appliance or a service profile to identify and connect with the correct appliance.

- If the management subnet you are connected to has a DHCP server deployed, the CIMC will automatically receive an IP address. This address will be displayed during initial bootup and can be seen from a serial console connection or a VGA screen.
- If the management subnet you are connected to does not have a DHCP server, you must enter a static IP address by entering the CIMC configuration setup during bootup. To do this, press <F8> during initial bootup. After the address is set, the CIMC GUI and ssh connections will be available.

For more information about the KVM console, see the "Starting the KVM Console" section in the *Cisco UCS Manager GUI Configuration Guide*.

Using Virtual Media to Install or Recover Cisco NGA

To upgrade or recover Cisco NGA you can use the Cisco Image Management Controller to map the Cisco NGA ISO file to the virtual media CD. No CD/DVD is shipped with the product. You must log in with user or admin privileges to perform this task.

Step 1 Download the ISO file from Cisco.com (where the Cisco NGA images are located).

Step 2 Log into web interface (default: admin/password) using your web browser.

For more information about configuring virtual media using the CIMC, see Set up CIMC for the UCS C-Series Server.

Step 3 Click Launch KVM Console (requires Java).

Step 4 In the Java applet, click the Virtual Media tab.

Step 5 Click **Add Image** and select the ISO file.

Step 6 Check Mapped in Client View for the newly created drive.

Step 7 Log into web interface, click **Power Cycle Server**.

The appliance will boot up from the mapped ISO image and will stop at the Helper Utility menu.

Step 8 Click the KVM tab in the Java applet.

Step 9 Choose one of these options:

a. Option 3 to install the image bundled in the ISO.	You must use Option 3 when upgrading from Cisco NGA 3140, software release 1.0.1 to 1.0.2. This option ensures the helper image is updated.
b. Option 2 to install a new image from the network and reformat the disk.	
c. Option 1 to upgrade NGA to a new image from the network.	

For details on how to set up virtual media for this product (which is preinstalled on a UCS server), see "Configuring Virtual Media" in *Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide* at http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/gui/config/guide/1.4.1/b_Cisco_UCS_C-Series_GUI_Configuration_Guide_141_chapter_0110.html#topic_04C1A0A98E0841D797DBD5D4149607F9.

Reference Appendix Updates

The Cisco NGA does not have support for certain NetFlow v5 fields. It will export a value of zero for these fields. In Table B-3, Configure Records Window Fields, the following routing features are not supported in Cisco NGA:

- SRC_AS, DST_AS
- BGP_NEXT_HOP
- SRC_MASK, DST_MASK

Product Documentation

The Cisco NetFlow Generation Appliance product documentation supports Hardware Releases 3140 and 3240.

Note We sometimes update the documentation after original publication. Therefore, you should review the documentation on Cisco.com for any updates.

You can view the marketing and user documents for Cisco NGA 1.0 (2) at: http://www.cisco.com/go/nga

The following document lists the documents available for Cisco NGA 1.0 (2): http://www.cisco.com/en/US/products/ps12508/products_documentation_roadmaps_list.html

Related Documentation

This section provides information about other documentation related to the Cisco NetFlow Generation Appliance.

Cisco Nexus 7000 Series Switch

- *Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 5.x*
- *SPAN Configuration on a Nexus 7000 Series Switches*

Cisco Nexus 5000 Series Switch

- *Cisco Nexus 5000 Series NX-OS Software Configuration Guide*

Cisco Nexus 3000 Series Switch

- *Cisco Nexus 3000 Series NX-OS Fundamentals Configuration Guide* (for SPAN configuration details)

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 the following URL:

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

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