



Cisco Flexible NetFlow Configuration Guide, Cisco IOS XE Release 3SE (Catalyst 3650 Switches)

First Published: October 10, 2013

Last Modified: November 07, 2014

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-29891-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <http://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

© 2013 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface

Preface vii

Document Conventions vii

Related Documentation ix

Obtaining Documentation and Submitting a Service Request ix

CHAPTER 1

Using the Command-Line Interface 1

Information About Using the Command-Line Interface 1

Command Modes 1

Using the Help System 3

Understanding Abbreviated Commands 4

No and Default Forms of Commands 5

CLI Error Messages 5

Configuration Logging 5

How to Use the CLI to Configure Features 6

Configuring the Command History 6

Changing the Command History Buffer Size 6

Recalling Commands 6

Disabling the Command History Feature 7

Enabling and Disabling Editing Features 7

Editing Commands Through Keystrokes 8

Editing Command Lines That Wrap 9

Searching and Filtering Output of show and more Commands 10

Accessing the CLI on a Switch Stack 11

Accessing the CLI Through a Console Connection or Through Telnet 11

CHAPTER 2

Configuring Flexible NetFlow 13

Finding Feature Information 13

Prerequisites	14
Prerequisites for Flexible NetFlow	14
Prerequisites for Wireless Flexible NetFlow	15
Restrictions	15
Restrictions for Flexible NetFlow	15
Restrictions for Wireless Flexible NetFlow	16
Information About NetFlow	17
Flexible NetFlow Overview	18
Wireless Flexible NetFlow Overview	18
Flow Records	19
Flexible NetFlow Match Parameters	20
Flexible NetFlow Collect Parameters	21
Exporters	22
Export Formats	23
Monitors	23
Samplers	24
Supported Flexible NetFlow Fields	24
Default Settings	28
How to Configure Flexible NetFlow	29
Creating a Flow Record	29
Creating a Flow Exporter	31
Creating a Flow Monitor	34
Creating a Sampler	36
Applying a Flow to an Interface	38
Configuring a Bridged NetFlow on a VLAN	39
Configuring Layer 2 NetFlow	40
Configuring WLAN to Apply Flow Monitor in Data Link Input/Output Direction	41
Configuring WLAN to Apply Flow Monitor in IPV4 and IPV6 Input/Output Direction	42
Monitoring Flexible NetFlow	43
Configuration Examples for Flexible NetFlow	44
Example: Configuring a Flow	44
Example: Configuring IPv4 Flexible NetFlow in WLAN (Ingress Direction)	45
Example: Configuring IPv6 and Transport Flag Flexible NetFlow in WLAN (Egress Direction)	45

Example: Configuring IPv6 Flexible NetFlow in WLAN (Both Ingress and Egress
Directions) **46**

Additional References **47**

Feature Information for Flexible NetFlow **48**



Preface

This book describes configuration information and examples for Flexible NetFlow on the switch.

- [Document Conventions, page vii](#)
- [Related Documentation, page ix](#)
- [Obtaining Documentation and Submitting a Service Request, page ix](#)

Document Conventions

This document uses the following conventions:

Convention	Description
<code>^</code> or <code>Ctrl</code>	Both the <code>^</code> symbol and <code>Ctrl</code> represent the Control (<code>Ctrl</code>) key on a keyboard. For example, the key combination <code>^D</code> or <code>Ctrl-D</code> means that you hold down the Control key while you press the <code>D</code> key. (Keys are indicated in capital letters but are not case sensitive.)
bold font	Commands and keywords and user-entered text appear in bold font .
<i>Italic font</i>	Document titles, new or emphasized terms, and arguments for which you supply values are in <i>italic font</i> .
<code>Courier font</code>	Terminal sessions and information the system displays appear in <code>courier font</code> .
Bold Courier font	Bold Courier font indicates text that the user must enter.
[x]	Elements in square brackets are optional.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.

Convention	Description
[x y]	Optional alternative keywords are grouped in brackets and separated by vertical bars.
{x y}	Required alternative keywords are grouped in braces and separated by vertical bars.
[x {y z}]	Nested set of square brackets or braces indicate optional or required choices within optional or required elements. Braces and a vertical bar within square brackets indicate a required choice within an optional element.
string	A nonquoted set of characters. Do not use quotation marks around the string or the string will include the quotation marks.
<>	Nonprinting characters such as passwords are in angle brackets.
[]	Default responses to system prompts are in square brackets.
!, #	An exclamation point (!) or a pound sign (#) at the beginning of a line of code indicates a comment line.

Reader Alert Conventions

This document may use the following conventions for reader alerts:



Note

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



Tip

Means *the following information will help you solve a problem*.



Caution

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



Timesaver

Means *the described action saves time*. You can save time by performing the action described in the paragraph.

**Warning****IMPORTANT SAFETY INSTRUCTIONS**

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Related Documentation

**Note**

Before installing or upgrading the switch, refer to the switch release notes.

- Cisco Catalyst 3650 Switch documentation, located at:
http://www.cisco.com/go/cat3650_docs
- Cisco SFP and SFP+ modules documentation, including compatibility matrixes, located at:
http://www.cisco.com/en/US/products/hw/modules/ps5455/tsd_products_support_series_home.html
- Error Message Decoder, located at:
<https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi>

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/c/en/us/td/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.



Using the Command-Line Interface

- [Information About Using the Command-Line Interface, page 1](#)
- [How to Use the CLI to Configure Features, page 6](#)

Information About Using the Command-Line Interface

Command Modes

The Cisco IOS user interface is divided into many different modes. The commands available to you depend on which mode you are currently in. Enter a question mark (?) at the system prompt to obtain a list of commands available for each command mode.

You can start a CLI session through a console connection, through Telnet, a SSH, or by using the browser.

When you start a session, you begin in user mode, often called user EXEC mode. Only a limited subset of the commands are available in user EXEC mode. For example, most of the user EXEC commands are one-time commands, such as **show** commands, which show the current configuration status, and **clear** commands, which clear counters or interfaces. The user EXEC commands are not saved when the switch reboots.

To have access to all commands, you must enter privileged EXEC mode. Normally, you must enter a password to enter privileged EXEC mode. From this mode, you can enter any privileged EXEC command or enter global configuration mode.

Using the configuration modes (global, interface, and line), you can make changes to the running configuration. If you save the configuration, these commands are stored and used when the switch reboots. To access the various configuration modes, you must start at global configuration mode. From global configuration mode, you can enter interface configuration mode and line configuration mode.

This table describes the main command modes, how to access each one, the prompt you see in that mode, and how to exit the mode.

Table 1: Command Mode Summary

Mode	Access Method	Prompt	Exit Method	About This Mode
User EXEC	Begin a session using Telnet, SSH, or console.	Switch>	Enter logout or quit .	Use this mode to <ul style="list-style-type: none"> • Change terminal settings. • Perform basic tests. • Display system information.
Privileged EXEC	While in user EXEC mode, enter the enable command.	Switch#	Enter disable to exit.	Use this mode to verify commands that you have entered. Use a password to protect access to this mode.
Global configuration	While in privileged EXEC mode, enter the configure command.	Switch(config)#	To exit to privileged EXEC mode, enter exit or end , or press Ctrl-Z .	Use this mode to configure parameters that apply to the entire switch.
VLAN configuration	While in global configuration mode, enter the vlan <i>vlan-id</i> command.	Switch(config-vlan)#	To exit to global configuration mode, enter the exit command. To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure VLAN parameters. When VTP mode is transparent, you can create extended-range VLANs (VLAN IDs greater than 1005) and save configurations in the switch startup configuration file.
Interface configuration	While in global configuration mode, enter the interface command (with a specific interface).	Switch(config-if)#		Use this mode to configure parameters for the Ethernet ports.

Mode	Access Method	Prompt	Exit Method	About This Mode
			To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	
Line configuration	While in global configuration mode, specify a line with the line vty or line console command.	Switch(config-line)#	To exit to global configuration mode, enter exit . To return to privileged EXEC mode, press Ctrl-Z or enter end .	Use this mode to configure parameters for the terminal line.

Using the Help System

You can enter a question mark (?) at the system prompt to display a list of commands available for each command mode. You can also obtain a list of associated keywords and arguments for any command.

SUMMARY STEPS

1. **help**
2. *abbreviated-command-entry ?*
3. *abbreviated-command-entry <Tab>*
4. **?**
5. *command ?*
6. *command keyword ?*

DETAILED STEPS

	Command or Action	Purpose
Step 1	help Example: Switch# help	Obtains a brief description of the help system in any command mode.
Step 2	<i>abbreviated-command-entry ?</i> Example: Switch# di? dir disable disconnect	Obtains a list of commands that begin with a particular character string.
Step 3	<i>abbreviated-command-entry <Tab></i> Example: Switch# sh conf<tab> Switch# show configuration	Completes a partial command name.
Step 4	? Example: Switch> ?	Lists all commands available for a particular command mode.
Step 5	<i>command ?</i> Example: Switch> show ?	Lists the associated keywords for a command.
Step 6	<i>command keyword ?</i> Example: Switch(config)# cdp holdtime ? <10-255> Length of time (in sec) that receiver must keep this packet	Lists the associated arguments for a keyword.

Understanding Abbreviated Commands

You need to enter only enough characters for the switch to recognize the command as unique.

This example shows how to enter the **show configuration** privileged EXEC command in an abbreviated form:

```
Switch# show conf
```

No and Default Forms of Commands

Almost every configuration command also has a **no** form. In general, use the **no** form to disable a feature or function or reverse the action of a command. For example, the **no shutdown** interface configuration command reverses the shutdown of an interface. Use the command without the keyword **no** to reenable a disabled feature or to enable a feature that is disabled by default.

Configuration commands can also have a **default** form. The **default** form of a command returns the command setting to its default. Most commands are disabled by default, so the **default** form is the same as the **no** form. However, some commands are enabled by default and have variables set to certain default values. In these cases, the **default** command enables the command and sets variables to their default values.

CLI Error Messages

This table lists some error messages that you might encounter while using the CLI to configure your switch.

Table 2: Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for your switch to recognize the command.	Reenter the command followed by a question mark (?) without any space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Incomplete command.	You did not enter all of the keywords or values required by this command.	Reenter the command followed by a question mark (?) with a space between the command and the question mark. The possible keywords that you can enter with the command appear.
% Invalid input detected at '^' marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all of the commands that are available in this command mode. The possible keywords that you can enter with the command appear.

Configuration Logging

You can log and view changes to the switch configuration. You can use the Configuration Change Logging and Notification feature to track changes on a per-session and per-user basis. The logger tracks each configuration command that is applied, the user who entered the command, the time that the command was entered, and the parser return code for the command. This feature includes a mechanism for asynchronous

notification to registered applications whenever the configuration changes. You can choose to have the notifications sent to the syslog.



Note Only CLI or HTTP changes are logged.

How to Use the CLI to Configure Features

Configuring the Command History

The software provides a history or record of commands that you have entered. The command history feature is particularly useful for recalling long or complex commands or entries, including access lists. You can customize this feature to suit your needs.

Changing the Command History Buffer Size

By default, the switch records ten command lines in its history buffer. You can alter this number for a current terminal session or for all sessions on a particular line. This procedure is optional.

SUMMARY STEPS

1. `terminal history [size number-of-lines]`

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal history [size number-of-lines] Example: Switch# <code>terminal history size 200</code>	Changes the number of command lines that the switch records during the current terminal session in privileged EXEC mode. You can configure the size from 0 to 256.

Recalling Commands

To recall commands from the history buffer, perform one of the actions listed in this table. These actions are optional.



Note The arrow keys function only on ANSI-compatible terminals such as VT100s.

SUMMARY STEPS

1. **Ctrl-P** or use the **up arrow** key
2. **Ctrl-N** or use the **down arrow** key
3. **show history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	Ctrl-P or use the up arrow key	Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
Step 2	Ctrl-N or use the down arrow key	Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.
Step 3	show history Example: Switch# show history	Lists the last several commands that you just entered in privileged EXEC mode. The number of commands that appear is controlled by the setting of the terminal history global configuration command and the history line configuration command.

Disabling the Command History Feature

The command history feature is automatically enabled. You can disable it for the current terminal session or for the command line. This procedure is optional.

SUMMARY STEPS

1. **terminal no history**

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal no history Example: Switch# terminal no history	Disables the feature during the current terminal session in privileged EXEC mode.

Enabling and Disabling Editing Features

Although enhanced editing mode is automatically enabled, you can disable it and reenble it.

SUMMARY STEPS

1. terminal editing
2. terminal no editing

DETAILED STEPS

	Command or Action	Purpose
Step 1	terminal editing Example: Switch# <code>terminal editing</code>	Reenables the enhanced editing mode for the current terminal session in privileged EXEC mode.
Step 2	terminal no editing Example: Switch# <code>terminal no editing</code>	Disables the enhanced editing mode for the current terminal session in privileged EXEC mode.

Editing Commands Through Keystrokes

The keystrokes help you to edit the command lines. These keystrokes are optional.

**Note**

The arrow keys function only on ANSI-compatible terminals such as VT100s.

Table 3: Editing Commands

Editing Commands	Description
Ctrl-B or use the left arrow key	Moves the cursor back one character.
Ctrl-F or use the right arrow key	Moves the cursor forward one character.
Ctrl-A	Moves the cursor to the beginning of the command line.
Ctrl-E	Moves the cursor to the end of the command line.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

Delete or Backspace key	Erases the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-U or Ctrl-X	Deletes all characters from the cursor to the beginning of the command line.
Ctrl-W	Deletes the word to the left of the cursor.
Esc D	Deletes from the cursor to the end of the word.
Esc C	Capitalizes at the cursor.
Esc L	Changes the word at the cursor to lowercase.
Esc U	Capitalizes letters from the cursor to the end of the word.
Ctrl-V or Esc Q	Designates a particular keystroke as an executable command, perhaps as a shortcut.
Return key	Scrolls down a line or screen on displays that are longer than the terminal screen can display. Note The More prompt is used for any output that has more lines than can be displayed on the terminal screen, including show command output. You can use the Return and Space bar keystrokes whenever you see the More prompt.
Space bar	Scrolls down one screen.
Ctrl-L or Ctrl-R	Redisplays the current command line if the switch suddenly sends a message to your screen.

Editing Command Lines That Wrap

You can use a wraparound feature for commands that extend beyond a single line on the screen. When the cursor reaches the right margin, the command line shifts ten spaces to the left. You cannot see the first ten characters of the line, but you can scroll back and check the syntax at the beginning of the command. The keystroke actions are optional.

To scroll back to the beginning of the command entry, press **Ctrl-B** or the left arrow key repeatedly. You can also press **Ctrl-A** to immediately move to the beginning of the line.

**Note**

The arrow keys function only on ANSI-compatible terminals such as VT100s.

The following example shows how to wrap a command line that extends beyond a single line on the screen.

SUMMARY STEPS

1. **access-list**
2. **Ctrl-A**
3. **Return** key

DETAILED STEPS

	Command or Action	Purpose
Step 1	access-list Example: <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 Switch(config)# \$ 101 permit tcp 10.15.22.25 255.255.255.0 10.15.22.35 255.25 Switch(config)# \$t tcp 10.15.22.25 255.255.255.0 131.108.1.20 255.255.255.0 eq Switch(config)# \$15.22.25 255.255.255.0 10.15.22.35 255.255.255.0 eq 45</pre>	Displays the global configuration command entry that extends beyond one line. When the cursor first reaches the end of the line, the line is shifted ten spaces to the left and redisplayed. The dollar sign (\$) shows that the line has been scrolled to the left. Each time the cursor reaches the end of the line, the line is again shifted ten spaces to the left.
Step 2	Ctrl-A Example: <pre>Switch(config)# access-list 101 permit tcp 10.15.22.25 255.255.255.0 10.15.25\$</pre>	Checks the complete syntax. The dollar sign (\$) appears at the end of the line to show that the line has been scrolled to the right.
Step 3	Return key	Execute the commands. The software assumes that you have a terminal screen that is 80 columns wide. If you have a different width, use the terminal width privileged EXEC command to set the width of your terminal. Use line wrapping with the command history feature to recall and modify previous complex command entries.

Searching and Filtering Output of show and more Commands

You can search and filter the output for **show** and **more** commands. This is useful when you need to sort through large amounts of output or if you want to exclude output that you do not need to see. Using these commands is optional.

SUMMARY STEPS

1. `{show | more} command | {begin | include | exclude} regular-expression`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>{show more} command {begin include exclude} regular-expression</code> Example: <pre>Switch# show interfaces include protocol Vlan1 is up, line protocol is up Vlan10 is up, line protocol is down GigabitEthernet1/0/1 is up, line protocol is down GigabitEthernet1/0/2 is up, line protocol is up</pre>	Searches and filters the output. Expressions are case sensitive. For example, if you enter <code> exclude output</code> , the lines that contain output are not displayed, but the lines that contain output appear.

Accessing the CLI on a Switch Stack

You can access the CLI through a console connection, through Telnet, a SSH, or by using the browser.

You manage the switch stack and the stack member interfaces through the active switch. You cannot manage stack members on an individual switch basis. You can connect to the active switch through the console port or the Ethernet management port of one or more stack members. Be careful with using multiple CLI sessions on the active switch. Commands that you enter in one session are not displayed in the other sessions. Therefore, it is possible to lose track of the session from which you entered commands.



Note

We recommend using one CLI session when managing the switch stack.

If you want to configure a specific stack member port, you must include the stack member number in the CLI command interface notation.

Accessing the CLI Through a Console Connection or Through Telnet

Before you can access the CLI, you must connect a terminal or a PC to the switch console or connect a PC to the Ethernet management port and then power on the switch, as described in the hardware installation guide that shipped with your switch.

If your switch is already configured, you can access the CLI through a local console connection or through a remote Telnet session, but your switch must first be configured for this type of access.

You can use one of these methods to establish a connection with the switch:

- Connect the switch console port to a management station or dial-up modem, or connect the Ethernet management port to a PC. For information about connecting to the console or Ethernet management port, see the switch hardware installation guide.

- Use any Telnet TCP/IP or encrypted Secure Shell (SSH) package from a remote management station. The switch must have network connectivity with the Telnet or SSH client, and the switch must have an enable secret password configured.
 - The switch supports up to 16 simultaneous Telnet sessions. Changes made by one Telnet user are reflected in all other Telnet sessions.
 - The switch supports up to five simultaneous secure SSH sessions.

After you connect through the console port, through the Ethernet management port, through a Telnet session or through an SSH session, the user EXEC prompt appears on the management station.



CHAPTER 2

Configuring Flexible NetFlow

- [Finding Feature Information, page 13](#)
- [Prerequisites, page 14](#)
- [Restrictions, page 15](#)
- [Restrictions for Flexible NetFlow, page 15](#)
- [Restrictions for Wireless Flexible NetFlow, page 16](#)
- [Information About NetFlow, page 17](#)
- [How to Configure Flexible NetFlow, page 29](#)
- [Monitoring Flexible NetFlow, page 43](#)
- [Configuration Examples for Flexible NetFlow, page 44](#)
- [Additional References, page 47](#)
- [Feature Information for Flexible NetFlow, page 48](#)

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

Prerequisites

Prerequisites for Flexible NetFlow

The following are prerequisites for your Flexible NetFlow configuration:

- You must configure a source interface. If you do not configure a source interface, the exporter will remain in a disabled state.
- You must configure a valid record name for every flow monitor.
- You must enable IPv6 routing to export the flow records to an IPv6 destination server.
- You must configure IPFIX export protocol for the flow exporter to export netflow records in IPFIX format.
- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands in the Cisco IOS Flexible NetFlow Command Reference :
 - **match datalink**—Datalink (layer2) fields
 - **match flow**—Flow identifying fields
 - **match interface**—Interface fields
 - **match ipv4**—IPv4 fields
 - **match ipv6**—IPv6 fields
 - **match transport**—Transport layer fields
 - **match wireless**—Wireless fields
- You are familiar with the Flexible NetFlow non key fields as they are defined in the following commands in the Cisco IOS Flexible NetFlow Command Reference :
 - **collect counter**—Counter fields
 - **collect flow**—Flow identifying fields
 - **collect interface**—Interface fields
 - **collect timestamp**—Timestamp fields
 - **collect transport**—Transport layer fields
 - **collect wireless**—Wireless fields

IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding or distributed Cisco Express Forwarding.

IPv6 Traffic

- The networking device must be configured for IPv6 routing.
- One of the following must be enabled on your router and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 or distributed Cisco Express Forwarding.

Prerequisites for Wireless Flexible NetFlow

The following are the prerequisites for wireless Flexible NetFlow:

- Ensure that the networking device is running a Cisco release that supports wireless Flexible NetFlow.
- Ensure that the target is connected to a WLAN.
- The networking device must be configured to support protocol types such as IP, IPv6, and datalink.
- Valid flow record and monitor are required before generating the flow.

Restrictions**Restrictions for Flexible NetFlow**

The following are restrictions for Flexible NetFlow:

- Traditional NetFlow (TNF) accounting is not supported.
- Flexible NetFlow version 9 and version 10 export formats are supported. However, if you have not configured the export protocol, version 9 export format is applied by default.
- Microflow policing feature shares the NetFlow hardware resource with FNF.
- Only one flow monitor per interface and per direction is supported .
- Layer 2, IPv4, and IPv6 traffic types are supported; however, the switch can apply a flow monitor to only one of these types at a time for a given direction and interface.
- Layer 2, VLAN, WLAN and Layer 3 interfaces are supported, but the switch does not support SVI and tunnels.
- The following NetFlow table sizes are supported:

Trim Level	Ingress NetFlow Table	Egress NetFlow Table
LAN Base	Not supported	Not supported
IP Base	8 K	16 K
IP Services	8 K	16 K

- Depending on the switch type, a switch will have one or two forwarding ASICs. The capacities listed in the above table are on a per-ASIC basis.
- The switch can support either one or two ASICs. Each ASIC has 8K ingress and 16 K egress entries, whereas each TCAM can handle up to 6K ingress and 12K egress entries.
- The NetFlow tables are on separate compartments and cannot be combined. Depending on which ASIC processed the packet, the flows will be created in the table in the corresponding ASIC.
- NetFlow hardware implementation supports four hardware samplers. You can select a sampler rate from 1 out of 2 to 1 out of 1024. Only random sampling mode is supported.
- With the microflow policing feature (which is enabled only for wireless implementation), NetFlow can and should be used only in full flow mode i.e. NetFlow policing cannot be used. For wireless traffic, applying a sampler is not permitted, as it hinders microflow QoS.
- Only full flow accounting is supported for wireless traffic.
- NetFlow hardware uses hash tables internally. Hash collisions can occur in the hardware. Therefore, in spite of the internal overflow Content Addressable Memory (CAM), the actual NetFlow table utilization could be about 80 percent.
- Depending on the fields that are used for the flow, a single flow could take two consecutive entries. IPv6 flows also take two entries. In these situations, the effective usage of NetFlow entries is half the table size, which is separate from the above hash collision limitation.
- The switch supports up to 63 flow monitors.
- SSID-based NetFlow accounting is supported. SSID is treated in a manner similar to an interface. However, certain fields are not supported such as user ID .
- The NetFlow software implementation supports distributed NetFlow export, so the flows are exported from the same switch in which the flow was created.
- Ingress flows are present in the ASIC that first received the packets for the flow. Egress flows are present in the ASIC from which the packets actually left the switch set up.
- The reported value for the bytes count field (called “bytes long”) is Layer-2-packet-size—18 bytes. For classic Ethernet traffic (802.3), this will be accurate. For all other Ethernet types, this field will not be accurate. Use the "bytes layer2" field, which always reports the accurate Layer 2 packet size. For information about supported Flexible NetFlow fields, see [Supported Flexible NetFlow Fields, on page 24](#).
- Configuration of IPFIX exporter on an AVC flow monitor is not supported.
- Flexible NetFlow export is not supported on the Ethernet management port, Gi0/0.

Restrictions for Wireless Flexible NetFlow

- Supports up to 24 K NetFlow per ASIC.
- Supports one policy per direction (input and output) per WLAN, which is at the most two monitors per WLAN.
- Supports only Flexible NetFlow v9 export format.
- The wireless client QoS policy feature shares the NetFlow hardware resource with Flexible NetFlow.

- Use NetFlow only in full flow mode with the QoS policy feature.
- Supports only one flow monitor per interface, per direction.
- Supports Layer 2, IPv4, and IPv6 traffic types. Allows you to apply flow monitor to only one of these types at a time for a given direction and interface.
- Supports only full flow accounting.
- NetFlow tables cannot be combined because they are on separate compartments. Depending on which ASIC processed the packet, the flows will be created in the table in the corresponding ASIC.
- Hash collisions occur in the Flexible NetFlow hardware. In spite of the internal overflow CAM, the actual NetFlow table utilization is about 80 percent.
- Depending on the fields that are used for the flow, a single flow takes two consecutive entries. IPv6 flows also take two entries. So, the effective usage of NetFlow entries is half the table size. This is apart from the hash collision limitation.
- Supports up to 63 flow monitors. QoS policy uses a separate set of flow monitors.
- The Flexible NetFlow software implementation supports distributed NetFlow export. The flows are exported from the same switch in which the flow was created.
- Ingress flows are present in the ASIC that received the packets first for the flow. Egress flows are present in the ASIC from which the packets actually left the switch setup.
- The reported value for the bytes count field (IN_BYTES) is (layer-2-packet-size - 18 bytes). This field will be accurate only for classic Ethernet traffic. Use the bytes layer2 field, which will always report the accurate Layer 2 packet size.
- The controller supports three ASICs.
- Supports SSID-based NetFlow accounting.
- For IOS XE release 3E, it is not recommended to use IPFIX IPv4 exporting on the Cisco 5700 Series Wireless LAN Controller.
- For IOS XE release 3E, following are the limitations on WLAN configurations of egress wireless traffic:
 - 1 If all or some of the WLANs have egress flow monitor configured, then there is no egress microflow QoS on any WLAN.
 - 2 If all or some of the WLANs have egress microflow QoS defined, then there is no egress flow monitor configured on any WLAN.
- For IOS XE release 3E, there is support for one WLAN that has egress netflow and egress WQoS enabled simultaneously.

Information About NetFlow

NetFlow is a Cisco technology that provides statistics on packets flowing through the switch. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to enable network and security monitoring, network planning, traffic analysis, and IP accounting. Flexible NetFlow improves on original NetFlow by adding the capability to customize the traffic analysis parameters for your specific requirements. Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

Flexible NetFlow Overview

Flexible NetFlow uses flows to provide statistics for accounting, network monitoring, and network planning.

A flow is a unidirectional stream of packets that arrives on a source interface and has the same values for the keys. A key is an identified value for a field within the packet. You create a flow using a flow record to define the unique keys for your flow.

The switch supports the Flexible NetFlow feature that enables enhanced network anomalies and security detection. Flexible NetFlow allows you to define an optimal flow record for a particular application by selecting the keys from a large collection of predefined fields.

All key values must match for the packet to count in a given flow. A flow might gather other fields of interest, depending on the export record version that you configure. Flows are stored in the Flexible NetFlow cache.

You can export the data that Flexible NetFlow gathers for your flow by using an exporter and export this data to a remote system such as a Flexible NetFlow collector. The Flexible NetFlow collector can use an IPv4 or IPv6 address.

You define the size of the data that you want to collect for a flow using a monitor. The monitor combines the flow record and exporter with the Flexible NetFlow cache information.

Wireless Flexible NetFlow Overview

The wireless Flexible NetFlow infrastructure supports the following:

- Flexible NetFlow Version 9.0
- User-based rate limiting
- Microflow policing
- Voice and video flow monitoring
- Reflexive access control list (ACL)

Microflow Policing and User-Based Rate Limiting

Microflow policing associates a 2-color 1-rate policer and related drop statistics to each flow present in the NetFlow table. When the flow mask comprises all packet fields, this functionality is known as microflow policing. When the flow mask comprises either source or destination only, this functionality is known as user-based rate limiting.

Voice and Video Flow Monitoring

Voice and video flows are full flow mask-based entries. The ASIC provides the flexibility to program the policer parameters, share policers across multiple flows and rewrite the IP address and Layer 4 port numbers of these flows.

**Note**

For dynamic entries, the NetFlow engine will use the policer parameters that are derived for the flow based on the policy (ACL/QoS-based policies). Dynamic entries cannot share policer across multiple flows.

Reflexive ACL

Reflexive ACLs allow IP packets to be filtered based on upper-layer session information. The ACLs allow outbound traffic and limit inbound traffic in response to the sessions that originate inside the trusted network. The reflexive ACLs are transparent to the filtering mechanism until a data packet that matches the reflexive entry activates it. At this time, a temporary ACL entry is created and added to the IP-named access lists. The information obtained from the data packet to generate the reflexive ACL entry is permit/deny bit, the source IP address and port, the destination IP address, port, and the protocol type. During reflexive ACL entry evaluation, if the protocol type is either TCP or UDP, then the port information must match exactly. For other protocols, there is no port information to match. After this ACL is installed, the firewall is then opened for the reply packets to pass through. At this time, a potential hacker could have access to the network behind the firewall. To narrow this window, an idle timeout period can be defined. However, in the case of TCP, if two FIN bits or an RST is detected, the ACL entry can be removed.

Related Topics

[Configuring WLAN to Apply Flow Monitor in IPv4 and IPv6 Input/Output Direction](#), on page 42

[Example: Configuring IPv4 Flexible NetFlow in WLAN \(Ingress Direction\)](#), on page 45

[Example: Configuring IPv6 and Transport Flag Flexible NetFlow in WLAN \(Egress Direction\)](#), on page 45

[Example: Configuring IPv6 Flexible NetFlow in WLAN \(Both Ingress and Egress Directions\)](#), on page 46

Flow Records

In Flexible NetFlow a combination of key and nonkey fields is called a record. Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data. Flexible NetFlow includes several predefined records that can help you get started using Flexible NetFlow.

A flow record defines the keys that Flexible NetFlow uses to identify packets in the flow, as well as other fields of interest that Flexible NetFlow gathers for the flow. You can define a flow record with any combination of keys and fields of interest. The switch supports a rich set of keys. A flow record also defines the types of counters gathered per flow. You can configure 64-bit packet or byte counters. The switch enables the following match fields as the defaults when you create a flow record:

- match datalink—Layer 2 attributes
- match flow direction — Specifies a match to the fields identifying the direction of flow.
- match interface—Interface attributes
- match ipv4—IPv4 attributes
- match ipv6—IPv6 attributes
- match transport—Transport layer fields
- match wireless—Wireless fields

Related Topics

[Creating a Flow Record](#), on page 29

Flexible NetFlow Match Parameters

The following table describes Flexible NetFlow match parameters. You must configure at least one of the following match parameters for the flow records.

Table 4: Match Parameters

Command	Purpose
match datalink {dot1q ethertype mac vlan }	Specifies a match to datalink or Layer 2 fields. The following command options are available: <ul style="list-style-type: none"> • dot1q—Matches to the dot1q field. • ethertype—Matches to the ethertype of the packet. • mac—Matches the source or destination MAC fields. • vlan—Matches to the VLAN that the packet is located on (input or output).
match flow direction	Specifies a match to the flow identifying fields.
match interface {input output}	Specifies a match to the interface fields. The following command options are available: <ul style="list-style-type: none"> • input—Matches to the input interface. • output—Matches to the output interface.
match ipv4 {destination protocol source tos ttl version}	Specifies a match to the IPv4 fields. The following command options are available: <ul style="list-style-type: none"> • destination—Matches to the IPv4 destination address-based fields. • protocol—Matches to the IPv4 protocols. • source—Matches to the IPv4 source address based fields. • tos—Matches to the IPv4 Type of Service fields. • ttl—Matches to the IPv4 Time To Live fields. • version—Matches to the IP version from the IPv4 header.

Command	Purpose
match ipv6 { destination hop-limit protocol source traffic-class version }	<p>Specifies a match to the IPv6 fields. The following command options are available:</p> <ul style="list-style-type: none"> • destination—Matches to the IPv6 destination address-based fields. • hop-limit—Matches to the IPv6 hop limit fields. • protocol—Matches to the IPv6 payload protocol fields. • source—Matches to the IPv6 source address based fields. • traffic-class—Matches to the IPv6 traffic class. • version—Matches to the IP version from the IPv6 header.
match transport { destination-port igmp icmp source-port }	<p>Specifies a match to the Transport Layer fields. The following command options are available:</p> <ul style="list-style-type: none"> • destination-port—Matches to the transport destination port. • icmp—Matches to ICMP fields, including ICMP IPv4 and IPv6 fields. • igmp—Matches to IGMP fields. • source-port—Matches to the transport source port.

Flexible NetFlow Collect Parameters

The following table describes the Flexible NetFlow collect parameters.

Table 5: Collect Parameters

Command	Purpose
collect counter { bytes { layer2 { long } long } packets { long } }	Collects the counter fields total bytes and total packets.
collect interface { input output }	Collects the fields from the input or output interface.
collect timestamp absolute { first last }	Collects the fields for the absolute time the first packet was seen or the absolute time the most recent packet was last seen (in milliseconds).

Command	Purpose
collect transport tcp flags	<p>Collects the following transport TCP flags:</p> <ul style="list-style-type: none"> • ack—TCP acknowledgement flag • cwr—TCP congestion window reduced flag • ece—TCP ECN echo flag • fin—TCP finish flag • psh—TCP push flag • rst—TCP reset flag • syn—TCP synchronize flag • urg—TCP urgent flag <p>Note On the switch, you cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags. All TCP flags will be collected with this command.</p>

Exporters

An exporter contains network layer and transport layer details for the Flexible NetFlow export packet. The following table lists the configuration options for an exporter.

Table 6: Flexible NetFlow Exporter Configuration Options

Exporter Configuration	Description
default	Sets a command to its default values.
description	Provides a description for the flow exporter.
destination	Export destination.
dscp	Optional DSCP value.
exit	Exits from the flow exporter configuration mode.
export-protocol	Export protocol version.
no	Negates the command or its default.
option	Selects option for exporting.
source	Originating interface for the net flow.

Exporter Configuration	Description
template	Flow exporter template configuration.
transport	Transport protocol.
ttl	Optional TTL or hop limit.

- Active timeout—The flow continues to have the packets for the past m seconds since the flow was created.
- Inactive timeout—The flow does not have any packets for the past n seconds.

Related Topics

[Creating a Flow Exporter, on page 31](#)

Export Formats

The switch supports only NetFlow Version 9 export formats. NetFlow Version 9 export format provides the following features and functionality:

- Variable field specification format
- Support for IPv4 destination address export
- More efficient network utilization



Note

For information about the Version 9 export format, see RFC 3954.

Monitors

A monitor references the flow record and flow exporter. You apply a monitor to an interface on the switch .

Note the following when applying a flow monitor to an interface:

- If you apply a flow monitor in the input direction:
 - Use the **match** keyword and use the input interface as a key field.
 - Use the **collect** keyword and use the output interface as a collect field. This field will be present in the exported records but with a value of 0.
- If you apply a flow monitor in the output direction:
 - Use the **match** keyword and use the output interface as a key field.
 - Use the **collect** keyword and use the input interface as a collect field. This field will be present in the exported records but with a value of 0.

Related Topics

[Creating a Flow Monitor, on page 34](#)

Samplers

If you are using sampled mode, you use the sampler to specify the rate at which packets are sampled.

Related Topics

[Creating a Sampler, on page 36](#)

Supported Flexible NetFlow Fields

The following tables provide a consolidated list of supported fields in Flexible NetFlow (FNF) for various traffic types and traffic direction.



Note If the packet has a VLAN field, then that length is not accounted for.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Key or Collect Fields							
Interface input	Yes	—	Yes	—	Yes	—	If you apply a flow monitor in the input direction: <ul style="list-style-type: none"> • Use the match keyword and use the input interface as a key field. • Use the collect keyword and use the output interface as a collect field. This field will be present in the exported records but with a value of 0.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Interface output	—	Yes	—	Yes	—	Yes	<p>If you apply a flow monitor in the output direction:</p> <ul style="list-style-type: none"> • Use the match keyword and use the output interface as a key field. • Use the collect keyword and use the input interface as a collect field. This field will be present in the exported records but with a value of 0.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Key Fields							
Flow direction	Yes	Yes	Yes	Yes	Yes	Yes	
Ethertype	Yes	Yes	—	—	—	—	
VLAN input	Yes	—	Yes	—	Yes	—	Supported only for a switch port.
VLAN output	—	Yes	—	Yes	—	Yes	Supported only for a switch port.
dot1q VLAN input	Yes	—	Yes	—	Yes	—	Supported only for a switch port.
dot1q VLAN output	—	Yes	—	Yes	—	Yes	Supported only for a switch port.
dot1q priority	Yes	Yes	Yes	Yes	Yes	Yes	Supported only for a switch port.

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
MAC source address input	Yes	Yes	Yes	Yes	Yes	Yes	
MAC source address output	—	—	—	—	—	—	
MAC destination address input	Yes	—	Yes	—	Yes	—	
MAC destination address output	—	Yes	—	Yes	—	Yes	
IPv4 version	—	—	Yes	Yes	Yes	Yes	
IPv4 TOS	—	—	Yes	Yes	Yes	Yes	
IPv4 protocol	—	—	Yes	Yes	Yes	Yes	Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used.
IPv4 TTL	—	—	Yes	Yes	Yes	Yes	
IPv4 source address	—	—	Yes	Yes	—	—	
IPv4 destination address	—	—	Yes	Yes	—	—	
ICMP IPv4 type	—	—	Yes	Yes	—	—	
ICMP IPv4 code	—	—	Yes	Yes	—	—	

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
IGMP type	—	—	Yes	Yes	—	—	

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Key Fields continued							
IPv6 version	—	—	Yes	Yes	Yes	Yes	Same as IP version.
IPv6 protocol	—	—	Yes	Yes	Yes	Yes	Same as IP protocol. Must use if any of src/dest port, ICMP code/type, IGMP type or TCP flags are used.
IPv6 source address	—	—	—	—	Yes	Yes	
IPv6 destination address	—	—	—	—	Yes	Yes	
IPv6 traffic-class	—	—	Yes	Yes	Yes	Yes	Same as IP TOS.
IPv6 hop-limit	—	—	Yes	Yes	Yes	Yes	Same as IP TTL.
ICMP IPv6 type	—	—	—	—	Yes	Yes	
ICMP IPv6 code	—	—	—	—	Yes	Yes	
source-port	—	—	Yes	Yes	Yes	Yes	
dest-port	—	—	Yes	Yes	Yes	Yes	

Field	Layer 2 In	Layer 2 Out	IPv4 In	IP v4 Out	IPv6 In	IPv6 Out	Notes
Collect Fields							
Bytes long	Yes	Yes	Yes	Yes	Yes	Yes	Packet size = (Ethernet frame size including FCS - 18 bytes) Recommendat Avoid this field and use Bytes layer2 long.
Packets long	Yes	Yes	Yes	Yes	Yes	Yes	
Timestamp absolute first	Yes	Yes	Yes	Yes	Yes	Yes	
Timestamp absolute last	Yes	Yes	Yes	Yes	Yes	Yes	
TCP flags	Yes	Yes	Yes	Yes	Yes	Yes	Collects all flags.
Bytes layer2 long	Yes	Yes	Yes	Yes	Yes	Yes	

Default Settings

The following table lists the Flexible NetFlow default settings for the switch.

Table 7: Default Flexible NetFlow Settings

Setting	Default
Flow active timeout	1800 seconds
Flow timeout inactive	15 seconds

How to Configure Flexible NetFlow

To configure Flexible NetFlow, follow these general steps:

- 1 Create a flow record by specifying keys and non-key fields to the flow.
- 2 Create an optional flow exporter by specifying the protocol and transport destination port, destination, and other parameters.
- 3 Create a flow monitor based on the flow record and flow exporter.
- 4 Create an optional sampler.
- 5 Apply the flow monitor to a Layer 2 port, Layer 3 port, or VLAN.
- 6 If applicable to your configuration, configure a WLAN to apply a flow monitor to.

Creating a Flow Record

You can create a flow record and add keys to match on and fields to collect in the flow.

SUMMARY STEPS

1. **configure terminal**
2. **flow record** *name*
3. **description** *string*
4. **match** *type*
5. **collect** *type*
6. **end**
7. **show flow record** [*name record-name*]
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	flow record <i>name</i> Example: Switch(config)# flow record test Switch(config-flow-record)#	Creates a flow record and enters flow record configuration mode.

	Command or Action	Purpose
Step 3	<p><code>description <i>string</i></code></p> <p>Example:</p> <pre>Switch(config-flow-record) # description Ipv4Flow</pre>	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	<p><code>match <i>type</i></code></p> <p>Example:</p> <pre>Switch(config-flow-record) # match ipv4 source address Switch(config-flow-record) # match ipv4 destination address Switch(config-flow-record) # match flow direction Switch(config-flow-record) # match datalink mac output Switch(config-flow-record) # match ip destination address Switch(config-flow-record) # match ipv6 destination address</pre>	Specifies a match key. For information about possible match key values, see Flexible NetFlow Match Parameters , on page 20.
Step 5	<p><code>collect <i>type</i></code></p> <p>Example:</p> <pre>Switch(config-flow-record) # collect counter bytes layer2 long Switch(config-flow-record) # collect counter bytes long Switch(config-flow-record) # collect timestamp absolute first Switch(config-flow-record) # collect transport tcp flags Switch(config-flow-record) # collect interface output</pre>	<p>Specifies the collection field. For information about possible collection field values, see Flexible NetFlow Collect Parameters, on page 21.</p> <p>Note For collect interface output, mandatory match fields have to be configured in the flow record as shown below.</p> <ul style="list-style-type: none"> • To attach datalink monitor, configure match datalink mac output in corresponding record. • To attach ip monitor, configure match ip destination address in corresponding record. • To attach ipv6 monitor, configure match ipv6 destination address in corresponding record <p>Note The collect interface output command will return a value of NULL for L3 broadcast, L2 broadcast, L3 Multicast, L2 Multicast, and L2 unknown destination.</p>
Step 6	<p><code>end</code></p> <p>Example:</p> <pre>Switch(config-flow-record) # end</pre>	Returns to privileged EXEC mode.
Step 7	<code>show flow record [name <i>record-name</i>]</code>	(Optional) Displays information about NetFlow flow records.

	Command or Action	Purpose
	Example: Switch <code>show flow record test</code>	
Step 8	copy running-config startup-config Example: Switch# <code>copy running-config startup-config</code>	(Optional) Saves your entries in the configuration file.

What to Do Next

Define an optional flow exporter by specifying the export format, protocol, destination, and other parameters.

Related Topics

[Flow Records, on page 19](#)

Creating a Flow Exporter

You can create a flow export to define the export parameters for a flow.



Note

Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor.

You can export to a destination using IPv4 or IPv6 address.

SUMMARY STEPS

1. **configure terminal**
2. **flow exporter** *name*
3. **description** *string*
4. **destination** {*ipv4-address|ipv6-address*}
5. **dscp** *value*
6. **source** { *source type* }
7. **transport udp** *number*
8. **ttl** *seconds*
9. **export-protocol** {*netflow-v9 | ipfix*}
10. **end**
11. **show flow exporter** [*name record-name*]
12. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	flow exporter <i>name</i> Example: Switch(config)# flow exporter ExportTest	Creates a flow exporter and enters flow exporter configuration mode.
Step 3	description <i>string</i> Example: Switch(config-flow-exporter)# description ExportV9	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	destination { <i>ipv4-address ipv6-address</i> } Example: Switch(config-flow-exporter)# destination 192.0.2.1 (IPv4 destination) Switch(config-flow-exporter)# destination 2001:0:0:24::10 (IPv6 destination)	Sets the IPv4/IPv6 destination address or hostname for this exporter.

	Command or Action	Purpose
Step 5	<p>dscp <i>value</i></p> <p>Example:</p> <pre>Switch(config-flow-exporter)# dscp 0</pre>	(Optional) Specifies the differentiated services codepoint value. The range is from 0 to 63. The default is 0.
Step 6	<p>source { <i>source type</i> }</p> <p>Example:</p> <pre>Switch(config-flow-exporter)# source gigabitEthernet1/0/1</pre>	<p>(Optional) Specifies the interface to use to reach the NetFlow collector at the configured destination. The following interfaces can be configured as source:</p> <ul style="list-style-type: none"> • Auto Template—Auto-Template interface • Capwap—CAPWAP tunnel interface • GigabitEthernet—Gigabit Ethernet IEEE 802 • GroupVI—Group virtual interface • Internal Interface—Internal interface • Loopback—Loopback interface • Null—Null interface • Port-channel—Ethernet Channel of interface • TenGigabitEthernet—10-Gigabit Ethernet • Tunnel—Tunnel interface • Vlan—Catalyst VLANs
Step 7	<p>transport udp <i>number</i></p> <p>Example:</p> <pre>Switch(config-flow-exporter)# transport udp 200</pre>	(Optional) Specifies the UDP port to use to reach the NetFlow collector. The range is from 0 to 65535. For IPFIX exporting protocol, the default destination port is 4739.
Step 8	<p>ttl <i>seconds</i></p> <p>Example:</p> <pre>Switch(config-flow-exporter)# ttl 210</pre>	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. The range is from 1 to 255 seconds. The default is 255.
Step 9	<p>export-protocol { <i>netflow-v9</i> <i>ipfix</i> }</p> <p>Example:</p> <pre>Device(config-flow-exporter)# export-protocol netflow-v9</pre>	<p>Specifies the version of the NetFlow export protocol used by the exporter.</p> <ul style="list-style-type: none"> • Default: netflow-v9.

	Command or Action	Purpose
Step 10	end Example: <pre>Switch(config-flow-record)# end</pre>	Returns to privileged EXEC mode.
Step 11	show flow exporter [<i>name record-name</i>] Example: <pre>Switch show flow exporter ExportTest</pre>	(Optional) Displays information about NetFlow flow exporters.
Step 12	copy running-config startup-config Example: <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

What to Do Next

Define a flow monitor based on the flow record and flow exporter.

Related Topics

[Exporters, on page 22](#)

Creating a Flow Monitor

You can create a flow monitor and associate it with a flow record and a flow exporter.

SUMMARY STEPS

1. **configure terminal**
2. **flow monitor** *name*
3. **description** *string*
4. **exporter** *name*
5. **record** *name*
6. **cache** { **timeout** { **active** | **inactive** } *seconds* | **type normal** }
7. **end**
8. **show flow monitor** [*name record-name*]
9. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	flow monitor name Example: Switch(config)# flow monitor MonitorTest Switch (config-flow-monitor)#	Creates a flow monitor and enters flow monitor configuration mode.
Step 3	description string Example: Switch(config-flow-monitor)# description Ipv4Monitor	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	exporter name Example: Switch(config-flow-monitor)# exporter ExportTest	Associates a flow exporter with this flow monitor.
Step 5	record name Example: Switch(config-flow-monitor)# record test	Associates a flow record with the specified flow monitor.
Step 6	cache { timeout {active inactive} seconds type normal } Example: Switch(config-flow-monitor)# cache timeout active 15000	Associates a flow cache with the specified flow monitor.
Step 7	end Example: Switch(config-flow-monitor)# end	Returns to privileged EXEC mode.

	Command or Action	Purpose
Step 8	show flow monitor [<i>name record-name</i>] Example: Switch show flow monitor name MonitorTest	(Optional) Displays information about NetFlow flow monitors.
Step 9	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

Apply the flow monitor to a Layer 2 interface, Layer 3 interface, or VLAN.

Related Topics

[Monitors, on page 23](#)

Creating a Sampler

You can create a sampler to define the NetFlow sampling rate for a flow.

SUMMARY STEPS

1. **configure terminal**
2. **sampler** *name*
3. **description** *string*
4. **mode** {random}
5. **end**
6. **show sampler** [*name*]
7. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	sampler <i>name</i> Example: Switch(config)# sampler SampleTest Switch(config-flow-sampler)#	Creates a sampler and enters flow sampler configuration mode.
Step 3	description <i>string</i> Example: Switch(config-flow-sampler)# description samples	(Optional) Describes this flow record as a maximum 63-character string.
Step 4	mode {random} Example: Switch(config-flow-sampler)# mode random 1 out-of 1024	Defines the random sample mode.
Step 5	end Example: Switch(config-flow-sampler)# end	Returns to privileged EXEC mode.
Step 6	show sampler [<i>name</i>] Example: Switch show sample SampleTest	(Optional) Displays information about NetFlow samplers.
Step 7	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

What to Do Next

Apply the flow monitor to a source interface, subinterface, VLAN interface, or a VLAN.

Related Topics[Samplers, on page 24](#)

Applying a Flow to an Interface

You can apply a flow monitor and an optional sampler to an interface.

SUMMARY STEPS

1. **configure terminal**
2. **interface *type***
3. **{ip flow monitor | ipv6 flow monitor} *name* [[*sampler name*] { **input**}**
4. **end**
5. **show flow interface [*interface-type number*]**
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	interface <i>type</i> Example: Switch(config)# interface GigabitEthernet1/0/1	Enters interface configuration mode and configures an interface. Command parameters for the interface configuration include: <ul style="list-style-type: none"> • GigabitEthernet—GigabitEthernet IEEE 802 • Loopback—Loopback interface • TenGigabitEthernet—10- Gigabit Ethernet • Vlan—Catalyst VLANs • Range—Interface range • WLAN—WLAN interface
Step 3	{ip flow monitor ipv6 flow monitor} <i>name</i> [[<i>sampler name</i>] { input} Example: Switch(config-if)# ip flow monitor MonitorTest input	Associate an IPv4 or an IPv6 flow monitor, and an optional sampler to the interface for input or output packets.

	Command or Action	Purpose
Step 4	end Example: Switch(config-flow-monitor)# end	Returns to privileged EXEC mode.
Step 5	show flow interface [<i>interface-type number</i>] Example: Switch# show flow interface	(Optional) Displays information about NetFlow on an interface.
Step 6	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring a Bridged NetFlow on a VLAN

You can apply a flow monitor and an optional sampler to a VLAN.

SUMMARY STEPS

1. **configure terminal**
2. **vlan** [*configuration*] *vlan-id*
3. **ip flow monitor** *monitor name* [**sampler** *sampler name*] {**input** |**output**}
4. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# configure terminal	Enters the global configuration mode.
Step 2	vlan [<i>configuration</i>] <i>vlan-id</i>	Enters VLAN or VLAN configuration mode.

	Command or Action	Purpose
	<p>Example:</p> <pre>Switch(config)# vlan configuration 30 Switch(config-vlan-config)#</pre>	
Step 3	<p>ip flow monitor <i>monitor name</i> [sampler <i>sampler name</i>] {input output}</p> <p>Example:</p> <pre>Switch(config-vlan-config)# ip flow monitor MonitorTest input</pre>	Associates a flow monitor and an optional sampler to the VLAN for input or output packets.
Step 4	<p>copy running-config startup-config</p> <p>Example:</p> <pre>Switch# copy running-config startup-config</pre>	(Optional) Saves your entries in the configuration file.

Configuring Layer 2 NetFlow

You can define Layer 2 keys in Flexible NetFlow records that you can use to capture flows in Layer 2 interfaces.

SUMMARY STEPS

1. **configure terminal**
2. **flow record** *name*
3. **match datalink** {**dot1q** | **ethertype** | **mac** | **vlan**}
4. **end**
5. **show flow record** [*name*]
6. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters the global configuration mode.

	Command or Action	Purpose
Step 2	flow record <i>name</i> Example: Switch(config)# flow record L2_record Switch(config-flow-record)#	Enters flow record configuration mode.
Step 3	match datalink {dot1q ethertype mac vlan} Example: Switch(config-flow-record)# match datalink ethertype	Specifies the Layer 2 attribute as a key.
Step 4	end Example: Switch(config-flow-record)# end	Returns to privileged EXEC mode.
Step 5	show flow record [<i>name</i>] Example: Switch# show flow record	(Optional) Displays information about NetFlow on an interface.
Step 6	copy running-config startup-config Example: Switch# copy running-config startup-config	(Optional) Saves your entries in the configuration file.

Configuring WLAN to Apply Flow Monitor in Data Link Input/Output Direction

SUMMARY STEPS

1. **configure terminal**
2. **wlan** [wlan-name { wlan-id SSID_NetworkName | wlan_id } | wlan-name | shutdown]
3. **datalink flow monitor monitor-name** {input | output}
4. **end**
5. **show run wlan** *wlan-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Switch# <code>configure terminal</code>	Enters global configuration mode.
Step 2	wlan [wlan-name { wlan-id SSID_NetworkName wlan_id } wlan-name shutdown] Example: Switch (config) # <code>wlan wlan1</code>	Enters WLAN configuration submode. <i>wlan-id</i> is the wireless LAN identifier. The range is 1 to 64. <i>SSID_NetworkName</i> is the SSID which can contain 32 alphanumeric characters. Note If you have already configured this command, enter the <code>wlan wlan-name</code> command.
Step 3	datalink flow monitor monitor-name {input output} Example: Switch (config-wlan) # <code>datalink flow monitor flow-monitor-1 {input output}</code>	Applies flow monitor to Layer 2 traffic in the direction of interest.
Step 4	end Example: Switch (config) # <code>end</code>	Returns to privileged EXEC mode.
Step 5	show run wlan wlan-name Example: Switch # <code>show wlan mywlan</code>	(Optional) Verifies your configuration.

Configuring WLAN to Apply Flow Monitor in IPV4 and IPv6 Input/Output Direction

SUMMARY STEPS

1. `configure terminal`
2. `wlan {wlan-name { wlan-id SSID_NetworkName | wlan_id } | wlan-name | shutdown}`
3. `{ip | ipv6} flow monitor monitor-name {input | output}`
4. `end`
5. `show run wlan wlan-name`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example:</p> <pre>Switch# configure terminal</pre>	Enters global configuration mode.
Step 2	<p>wlan {wlan-name { wlan-id SSID_NetworkName wlan_id} wlan-name shutdown}</p> <p>Example:</p> <pre>Switch (config) # wlan wlan1</pre>	<p>Enters WLAN configuration submode.</p> <p><i>wlan-id</i> is the wireless LAN identifier. The range is 1 to 64.</p> <p>SSID_NetworkName is the SSID which can contain 32 alphanumeric characters.</p> <p>Note If you have already configured this command, enter the wlan wlan-name command.</p>
Step 3	<p>{ip ipv6} flow monitor monitor-name {input output}</p> <p>Example:</p> <pre>Switch (config-wlan) # ip flow monitor flow-monitor-1 input</pre>	Associates a flow monitor to the WLAN for input or output packets.
Step 4	<p>end</p> <p>Example:</p> <pre>Switch (config) # end</pre>	Returns to privileged EXEC mode.
Step 5	<p>show run wlan wlan-name</p> <p>Example:</p> <pre>Switch # show wlan mywlan</pre>	(Optional) Verifies your configuration.

Related Topics

[Wireless Flexible NetFlow Overview, on page 18](#)

[Example: Configuring IPv4 Flexible NetFlow in WLAN \(Ingress Direction\), on page 45](#)

[Example: Configuring IPv6 and Transport Flag Flexible NetFlow in WLAN \(Egress Direction\), on page 45](#)

[Example: Configuring IPv6 Flexible NetFlow in WLAN \(Both Ingress and Egress Directions\), on page 46](#)

Monitoring Flexible NetFlow

The commands in the following table can be used to monitor Flexible NetFlow.

Table 8: Flexible NetFlow Monitoring Commands

Command	Purpose
show flow exporter [broker export-ids name <i>name</i> statistics templates]	Displays information about NetFlow flow exporters and statistics.
show flow exporter [name <i>exporter-name</i>]	Displays information about NetFlow flow exporters and statistics.
show flow interface	Displays information about NetFlow interfaces.
show flow monitor [name <i>exporter-name</i>]	Displays information about NetFlow flow monitors and statistics.
show flow monitor statistics	Displays the statistics for the flow monitor
show flow monitor cache format { table record csv }	Displays the contents of the cache for the flow monitor, in the format specified.
show flow record [name <i>record-name</i>]	Displays information about NetFlow flow records.
show flow ssid	Displays NetFlow monitor installation status for a WLAN.
show sampler [broker name <i>name</i>]	Displays information about NetFlow samplers.
show wlan <i>wlan-name</i>	Displays the WLAN configured on the device.

Configuration Examples for Flexible NetFlow

Example: Configuring a Flow

This example shows how to create a flow and apply it to an interface:

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.

Switch(config)# flow export export1
Switch(config-flow-exporter)# destination 10.0.101.254
Switch(config-flow-exporter)# transport udp 2055
Switch(config-flow-exporter)# exit
Switch(config)# flow record record1
Switch(config-flow-record)# match ipv4 source address
Switch(config-flow-record)# match ipv4 destination address
Switch(config-flow-record)# match ipv4 protocol
Switch(config-flow-record)# match transport source-port
Switch(config-flow-record)# match transport destination-port
Switch(config-flow-record)# collect counter byte long
Switch(config-flow-record)# collect counter packet long
```

```
Switch(config-flow-record) # collect timestamp absolute first
Switch(config-flow-record) # collect timestamp absolute last
Switch(config-flow-record) # exit
Switch(config) # flow monitor monitor1
Switch(config-flow-monitor) # record record1
Switch(config-flow-monitor) # exporter export1
Switch(config-flow-monitor) # exit
Switch(config) # interface tenGigabitEthernet 1/0/1
Switch(config-if) # ip flow monitor monitor1 input
Switch(config-if) # end
```

Example: Configuring IPv4 Flexible NetFlow in WLAN (Ingress Direction)

The following example shows how to configure IPv4 Flexible NetFlow on WLAN ingress direction:

```
Switch# configure terminal
Switch(config) # flow record fr_v4
Switch(config-flow-record) # match ipv4 destination address
Switch(config-flow-record) # match ipv4 source address
Switch(config-flow-record) # match ipv4 protocol
Switch(config-flow-record) # match ipv4 tos
Switch(config-flow-record) # match ipv4 ttl
Switch(config-flow-record) # match ipv4 version
Switch(config-flow-record) # match wireless ssid
Switch(config-flow-record) # collect wireless ap mac address
Switch(config-flow-record) # collect counter packets long
Switch(config-flow-record) # collect counter bytes long
Switch(config-flow-record) # collect timestamp absolute first
Switch(config-flow-record) # collect timestamp absolute last
Switch(config-flow-record) # exit

Switch(config) # flow monitor fm_v4
Switch(config-flow-monitor) # record fr_v4
Switch(config-flow-monitor) # exit

Switch(config) # wlan wlan_1
Switch(config-wlan) # ip flow monitor fm_v4 in
Switch(config-wlan) # end

Switch# show flow monitor fm_v4 cache
```

Related Topics

[Configuring WLAN to Apply Flow Monitor in IPV4 and IPV6 Input/Output Direction](#), on page 42
[Wireless Flexible NetFlow Overview](#), on page 18

Example: Configuring IPv6 and Transport Flag Flexible NetFlow in WLAN (Egress Direction)

The following example shows how to configure IPv6 and transport flag Flexible NetFlow on WLAN egress direction:

```
Switch# configure terminal
Switch(config) # flow record fr_v6
Switch(config-flow-record) # match ipv6 destination address
Switch(config-flow-record) # match ipv6 source address
Switch(config-flow-record) # match ipv6 hop-limit
```

```

Switch(config-flow-record)# match ipv6 protocol
Switch(config-flow-record)# match ipv6 traffic
Switch(config-flow-record)# match ipv6 version
Switch(config-flow-record)# match wireless ssid
Switch(config-flow-record)# collect wireless ap mac address
Switch(config-flow-record)# collect counter bytes long
Switch(config-flow-record)# collect transport tcp flags
Switch(config-flow-record)# exit

Switch(config)# flow monitor fm_v6
Switch(config-flow-monitor)# record fr_v6
Switch(config-flow-monitor)# exit

Switch(config)# wlan wlan_1
Switch(config-wlan)# ipv6 flow monitor fm_v6 out
Switch(config-wlan)# end

Switch# show flow monitor fm_v6 cache

```

**Note**

On the switch, you cannot specify which TCP flag to collect. You can only specify to collect transport TCP flags.

Related Topics

[Configuring WLAN to Apply Flow Monitor in IPV4 and IPv6 Input/Output Direction](#), on page 42
[Wireless Flexible NetFlow Overview](#), on page 18

Example: Configuring IPv6 Flexible NetFlow in WLAN (Both Ingress and Egress Directions)

The following example shows how to configure IPv6 Flexible NetFlow on WLAN in both directions:

```

Switch# configure terminal
Switch (config)# flow record fr_v6
Switch (config-flow-record)# match ipv6 destination address
Switch (config-flow-record)# match ipv6 source address
Switch (config-flow-record)# match ipv6 hop-limit
Switch (config-flow-record)# match ipv6 protocol
Switch (config-flow-record)# match ipv6 traffic
Switch (config-flow-record)# match ipv6 version
Switch (config-flow-record)# match wireless ssid
Switch (config-flow-record)# collect wireless ap mac address
Switch (config-flow-record)# collect counter packets long
Switch (config-flow-record)# exit

Switch (config)# flow monitor fm_v6
Switch (config-flow-monitor)# record fr_v6
Switch (config-flow-monitor)# exit

Switch (config)# wlan wlan_1
Switch (config-wlan)# ipv6 flow monitor fm_v6 in
Switch (config-wlan)# ipv6 flow monitor fm_v6 out
Switch (config-wlan)# end

Switch# show flow monitor fm_v6 cache

```


Related Topics

[Configuring WLAN to Apply Flow Monitor in IPV4 and IPV6 Input/Output Direction](#), on page 42
[Wireless Flexible NetFlow Overview](#), on page 18

Additional References

Related Documents

Related Topic	Document Title
Platform-independent command references	<i>Configuration Fundamentals Command Reference, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Platform-independent configuration information	<i>Configuration Fundamentals Configuration Guide, Cisco IOS XE Release 3S (Catalyst 3650 Switches)</i>
Flexible NetFlow CLI Commands	<i>Cisco Flexible NetFlow Command Reference (Catalyst 3650 Switches)</i> <i>Flexible NetFlow Command Reference, Cisco IOS XE Release 3SE (Cisco WLC 5700 Series)</i>

Error Message Decoder

Description	Link
To help you research and resolve system error messages in this release, use the Error Message Decoder tool.	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

Standards and RFCs

Standard/RFC	Title
RFC 3954	Cisco Systems NetFlow Services Export Version 9

MIBs

MIB	MIBs Link
All supported MIBs for this release.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

Technical Assistance

Description	Link
<p>The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies.</p> <p>To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds.</p> <p>Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.</p>	http://www.cisco.com/support

Feature Information for Flexible NetFlow

Release	Modification
Cisco IOS XE 3.3SE	This feature was introduced.



INDEX

B

bridged NetFlow [39](#)

C

collect parameters [21](#)

D

default settings [28](#)

E

export formats [23](#)

exporters [22](#)

F

flow exporter [31](#)

flow monitor [34](#)

flow record [19, 29](#)

I

interface configuration [38](#)

L

Layer 2 NetFlow [40](#)

M

match [19](#)

 datalink [19](#)

 flow [19](#)

 interface [19](#)

 ipv4 [19](#)

 ipv6 [19](#)

 transport [19](#)

match parameters [20](#)

monitoring [43](#)

monitors [23](#)

S

sampler [24, 36](#)

