



Flexible NetFlow Configuration Guide, Cisco IOS XE 17

First Published: 2013-02-24

Last Modified: 2013-02-24

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

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.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

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: [www.cisco.com go trademarks](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. (1721R)

© 2019 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1

Read Me First 1

CHAPTER 2

Flexible Netflow Overview 3

- Finding Feature Information 3
- Prerequisites for Flexible NetFlow 3
- Restrictions for Flexible Netflow 4
- Information About Flexible Netflow 5
 - Flexible NetFlow Overview 5
 - Typical Uses for NetFlow 5
 - Use of Flows in Original NetFlow and Flexible NetFlow 6
 - Original NetFlow and Benefits of Flexible NetFlow 6
 - Flexible NetFlow Components 7
 - Flow Records 8
 - Flow Monitors 8
 - Flow Exporters 10
 - Flow Samplers 11
 - Security Monitoring with Flexible NetFlow 11
 - Feature Comparison of Original NetFlow and Flexible NetFlow 12
 - Criteria for Identifying Traffic to Be Used in Analysis in Flexible NetFlow 13
 - Benefit of Emulating Original NetFlow with Flexible NetFlow 14
 - Flexible NetFlow Predefined Records 14
 - Benefits of Flexible NetFlow Predefined Records 14
 - NetFlow Original and NetFlow IPv4 Original Input Predefined Records 15
 - NetFlow IPv4 Original Output Predefined Record 16
 - NetFlow IPv6 Original Input Predefined Record 17
 - NetFlow IPv6 Original Output Predefined Record 18

| | |
|---|----|
| Autonomous System Predefined Record | 19 |
| Autonomous System ToS Predefined Record | 19 |
| BGP Next-Hop Predefined Record | 20 |
| BGP Next-Hop ToS Predefined Record | 21 |
| Destination Prefix Predefined Record | 22 |
| Destination Prefix ToS Predefined Record | 23 |
| Prefix Predefined Record | 24 |
| Prefix Port Predefined Record | 25 |
| Prefix ToS Predefined Record | 26 |
| Protocol Port Predefined Record | 27 |
| Protocol Port ToS Predefined Record | 28 |
| Source Prefix Predefined Record | 28 |
| Source Prefix ToS Predefined Record | 29 |
| How to Configure Flexible Netflow | 30 |
| Creating a Flow Record | 30 |
| Displaying the Current Status of a Flow Record | 33 |
| Verifying the Flow Record Configuration | 33 |
| Configuring a Flow Monitor for IPv4 or IPv6 Traffic Using the Predefined Record | 34 |
| Configuring a Flow Exporter for the Flow Monitor | 36 |
| Creating a Flow Monitor | 38 |
| Displaying the Current Status of a Flow Monitor | 40 |
| Displaying the Data in the Flow Monitor Cache | 41 |
| Verifying the Flow Monitor Configuration | 42 |
| Applying a Flow Monitor to an Interface | 43 |
| Verifying That Flexible NetFlow Is Enabled on an Interface | 44 |
| Configuration Examples for Flexible Netflow | 45 |
| Example: Configuring a Flexible NetFlow Predefined Record for IPv4 Traffic | 45 |
| Example: Configuring a Flexible NetFlow Predefined Record for IPv6 Traffic | 45 |
| Example: Configuring a Normal Flow Record Cache with a Limited Number of Flows | 46 |
| Example: Configuring a Customized Flow Record Cache for Monitoring IPv6 Traffic | 47 |
| Example: Configuring a Permanent Flow Record Cache with a Limited Number of Flows | 47 |
| Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic | 48 |
| Example: Configuring Flexible NetFlow Subinterface Support | 49 |
| Example: Configuring Flexible NetFlow Multiple Export Destinations | 50 |

| | | |
|------------------|---|-----------|
| | Additional References | 50 |
| | Feature Information for Flexible NetFlow | 51 |
| <hr/> | | |
| CHAPTER 3 | Flexible NetFlow—IPv4 Unicast Flows | 53 |
| | Finding Feature Information | 53 |
| | Information About Flexible NetFlow IPv4 Unicast Flows | 53 |
| | Flexible NetFlow—IPv4 Unicast Flows Overview | 53 |
| | How to Configure Flexible NetFlow IPv4 Unicast Flows | 53 |
| | Creating a Flow Record | 53 |
| | Configuring the Flow Exporter | 56 |
| | Creating a Flow Monitor | 59 |
| | Applying a Flow Monitor to an Interface | 60 |
| | Configuring and Enabling Flexible NetFlow with Data Export | 62 |
| | Configuration Examples for Flexible NetFlow IPv4 Unicast Flows | 64 |
| | Example: Configuring Multiple Export Destinations | 64 |
| | Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic | 65 |
| | Feature Information for Flexible NetFlow - IPv4 Unicast Flows | 66 |
| <hr/> | | |
| CHAPTER 4 | Flexible NetFlow—IPv6 Unicast Flows | 67 |
| | Finding Feature Information | 67 |
| | Information About Flexible NetFlow IPv6 Unicast Flows | 67 |
| | Flexible NetFlow IPv6 Unicast Flows Overview | 67 |
| | How to Configure Flexible NetFlow IPv6 Unicast Flows | 67 |
| | Creating a Flow Record | 67 |
| | Configuring the Flow Exporter | 70 |
| | Creating a Flow Monitor | 73 |
| | Applying a Flow Monitor to an Interface | 74 |
| | Configuring and Enabling Flexible NetFlow with Data Export | 76 |
| | Configuration Examples for Flexible NetFlow IPv6 Unicast Flows | 78 |
| | Example: Configuring Multiple Export Destinations | 78 |
| | Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic | 79 |
| | Feature Information for Flexible NetFlow - IPv6 Unicast Flows | 80 |
| <hr/> | | |
| CHAPTER 5 | Flexible NetFlow—MPLS Egress NetFlow | 81 |

| | |
|---|----|
| Finding Feature Information | 81 |
| Information About Flexible NetFlow MPLS Egress NetFlow | 81 |
| Flexible NetFlow MPLS Egress NetFlow | 81 |
| Limitations | 82 |
| How to Configure Flexible NetFlow MPLS Egress NetFlow | 83 |
| Configuring a Flow Exporter for the Flow Monitor | 83 |
| Creating a Flow Monitor | 85 |
| Applying a Flow Monitor to an Interface | 87 |
| Configuration Examples for Flexible NetFlow MPLS Egress NetFlow | 88 |
| Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic | 88 |
| Additional References | 89 |
| Feature Information for Flexible NetFlow - MPLS Egress NetFlow | 90 |

CHAPTER 6

| | |
|---|-----------|
| Flexible NetFlow v9 Export Format | 91 |
| Finding Feature Information | 91 |
| Prerequisites for Flexible NetFlow v9 Export Format | 91 |
| Information About Flexible NetFlow v9 Export Format | 91 |
| Flow Exporters | 91 |
| Benefits of Flexible NetFlow Flow Exporters | 92 |
| How to Configure Flexible NetFlow v9 Export Format | 92 |
| Configuring the Flow Exporter | 92 |
| Configuration Examples for Flexible NetFlow v9 Export Format | 95 |
| Example: Configuring NetFlow v9 Export Format | 95 |
| Additional Reference for Flexible NetFlow v9 Export Format | 95 |
| Feature Information for Flexible NetFlow - NetFlow v9 Export Format | 97 |

CHAPTER 7

| | |
|---|-----------|
| Flexible NetFlow Output Features on Data Export | 99 |
| Finding Feature Information | 99 |
| Prerequisites for Flexible NetFlow Output Features on Data Export | 99 |
| Information About Flexible NetFlow Output Features on Data Export | 100 |
| Flow Exporters | 100 |
| Benefits of Flexible NetFlow Flow Exporters | 100 |
| How to Configure Flexible NetFlow Output Features on Data Export | 101 |
| Restrictions | 101 |

| | |
|--|-----|
| Configuring the Flow Exporter | 101 |
| Displaying the Current Status of a Flow Exporter | 103 |
| Verifying the Flow Exporter Configuration | 104 |
| Configuring and Enabling Flexible NetFlow with Data Export | 105 |
| Configuration Examples for Flexible NetFlow Output Features on Data Export | 107 |
| Example: Configuring Sending Export Packets Using QoS | 107 |
| Additional References | 108 |
| Feature Information for Flexible NetFlow—Output Features on Data Export | 109 |

CHAPTER 8**Flexible NetFlow NetFlow V5 Export Protocol 111**

| | |
|--|-----|
| Finding Feature Information | 111 |
| Restrictions for Flexible NetFlow NetFlow V5 Export Protocol | 111 |
| Information about Flexible NetFlow NetFlow V5 Export Protocol | 112 |
| Flexible NetFlow V5 Export Protocol Overview | 112 |
| How to Configure Flexible NetFlow NetFlow V5 Export Protocol | 112 |
| Configuring the Flow Exporter | 112 |
| Configuration Examples for Flexible NetFlow NetFlow V5 Export Protocol | 114 |
| Example: Configuring Version 5 Export | 114 |
| Additional References | 115 |
| Feature Information for Flexible NetFlow NetFlow V5 Export Protocol | 116 |

CHAPTER 9**Using Flexible NetFlow Flow Sampling 117**

| | |
|--|-----|
| Finding Feature Information | 117 |
| Prerequisites for Using Flexible NetFlow Flow Sampling | 117 |
| Restrictions for Using Flexible NetFlow Flow Sampling | 118 |
| Information About Flexible NetFlow Flow Sampling | 118 |
| Flow Samplers | 118 |
| How to Configure Flexible NetFlow Flow Sampling | 118 |
| Configuring a Flow Monitor | 118 |
| 119 | |
| Displaying the Status and Statistics of the Flow Sampler Configuration | 121 |
| Configuration Examples for Flexible NetFlow Flow Sampling | 122 |
| Example: Configuring and Enabling a Random Sampler for IPv4 Traffic | 122 |
| Example: Adding a Sampler to a Flow Monitor When a Flow Monitor Is Already Enabled | 123 |

| | |
|--|-----|
| Example: Removing a Sampler from a Flow Monitor | 123 |
| Additional References | 124 |
| Feature Information for Flexible NetFlow Flow Sampling | 124 |

| | | |
|-------------------|--|------------|
| CHAPTER 10 | Flexible NetFlow - Layer 2 Fields | 127 |
| | Finding Feature Information | 127 |
| | Information About Flexible NetFlow Layer 2 Fields | 127 |
| | Flexible NetFlow - Layer 2 Fields Overview | 127 |
| | How to Configure Flexible NetFlow Layer 2 Fields | 128 |
| | Creating a Flow Record | 128 |
| | Creating a Flow Monitor | 130 |
| | Applying a Flow Monitor to an Interface | 132 |
| | Configuration Examples for Flexible NetFlow Layer 2 Fields | 133 |
| | Example: Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics | 133 |
| | Additional References | 134 |
| | Feature Information for Flexible NetFlow - Layer 2 Fields | 135 |

| | | |
|-------------------|---|------------|
| CHAPTER 11 | Flexible Netflow - Ingress VRF Support | 137 |
| | Finding Feature Information | 137 |
| | Information About Flexible NetFlow Ingress VRF Support | 137 |
| | Flexible NetFlow—Ingress VRF Support Overview | 137 |
| | How to Configure Flexible NetFlow Ingress VRF Support | 138 |
| | Creating a Flow Record | 138 |
| | Creating a Flow Monitor | 140 |
| | Applying a Flow Monitor to an Interface | 142 |
| | Configuration Examples for Flexible NetFlow Ingress VRF Support | 143 |
| | Example: Configuring Flexible NetFlow for Ingress VRF Support | 143 |
| | Additional References | 144 |
| | Feature Information for Flexible NetFlow—Ingress VRF Support | 145 |

| | | |
|-------------------|---|------------|
| CHAPTER 12 | Flexible NetFlow NBAR Application Recognition Overview | 147 |
| | Finding Feature Information | 147 |
| | Information About Flexible NetFlow NBAR Application Recognition | 147 |
| | Flexible NetFlow NBAR Application Recognition Overview | 147 |

| | |
|---|-----|
| How to Configure Flexible NetFlow NBAR Application Recognition | 148 |
| Creating a Flow Record | 148 |
| Creating a Flow Monitor | 151 |
| Applying a Flow Monitor to an Interface | 153 |
| Configuration Examples for Flexible NetFlow NBAR Application Recognition | 154 |
| Example: Configuring Flexible NetFlow for Network-Based Application Recognition | 154 |
| Additional References | 154 |
| Feature Information for Flexible NetFlow NBAR Application Recognition | 155 |

CHAPTER 13**Support for ISSU and SSO 157**

| | |
|---|-----|
| Finding Feature Information | 157 |
| Prerequisites for Flexible Netflow High Availability | 157 |
| Information About Flexible Netflow High Availability | 158 |
| ISSU | 158 |
| SSO | 158 |
| How to Configure Flexible Netflow High Availability | 158 |
| How to Verify Flexible Netflow High Availability | 158 |
| Configuration Examples for Flexible Netflow High Availability | 159 |
| Example: Displaying Detailed Status for the Sampler Broker | 160 |
| Example: Displaying a Status Summary for the Flow Record Broker | 160 |
| Example: Verifying Whether SSO is Configured | 160 |
| Example: Displaying which SSO Protocols and Applications are Registered | 161 |
| Additional References | 162 |
| Feature Information for Flexible Netflow High Availability Features | 164 |
| Glossary | 164 |

CHAPTER 14**Flexible NetFlow IPFIX Export Format 165**

| | |
|---|-----|
| Finding Feature Information | 165 |
| Information About Flexible NetFlow IPFIX Export Format | 165 |
| Flexible NetFlow IPFIX Export Format Overview | 165 |
| How to Configure Flexible NetFlow IPFIX Export Format | 166 |
| Configuring the Flow Exporter | 166 |
| Configuration Examples for Flexible NetFlow IPFIX Export Format | 168 |
| Example: Configuring Flexible NetFlow IPFIX Export Format | 168 |

Feature Information for Flexible NetFlow: IPFIX Export Format 169

CHAPTER 15**Flexible Netflow Export to an IPv6 Address 171**

Finding Feature Information 171

Information About Flexible Netflow Export to an IPv6 Address 171

Flexible Netflow Export to an IPv6 Address Overview 171

How to Configure Flexible Netflow Export to an IPv6 Address 171

Configuring the Flow Exporter 171

Configuration Examples for Flexible Netflow Export to an IPv6 Address 174

Example: Configuring Multiple Export Destinations 174

Additional References 176

Feature Information for Flexible NetFlow Export to an IPv6 Address 177

CHAPTER 16**Flexible Netflow—Egress VRF Support 179**

Finding Feature Information 179

Information About Flexible Netflow Egress VRF Support 179

Flexible Netflow—Egress VRF Support Overview 179

How to Configure Flexible Netflow Egress VRF Support 180

Creating a Flow Record 180

Creating a Customized Flow Monitor 182

Applying a Flow Monitor to an Interface 184

Configuration Examples for Flexible Netflow Egress VRF Support 186

Example Configuring Flexible NetFlow for Egress VRF Support 186

Additional References 186

Feature Information for Flexible NetFlow—Egress VRF Support 187

CHAPTER 17**Flexible NetFlow - MPLS Support 189**

Finding Feature Information 189

Information About Flexible NetFlow MPLS Support 189

Flexible NetFlow—MPLS Support Overview 189

How to Configure Flexible NetFlow MPLS Support 190

Configuring a Flow Exporter for the Flow Monitor 190

Creating a Flow Monitor 192

Applying a Flow Monitor to an Interface 194

| | |
|--|-----|
| Configuration Examples for Flexible NetFlow MPLS Support | 195 |
| Example: Configuring Flexible NetFlow for MPLS Support | 195 |
| Additional References | 196 |
| Feature Information for Flexible NetFlow: MPLS Support | 197 |

CHAPTER 18**Flexible NetFlow—Prevent Export Storms 199**

| | |
|---|-----|
| Finding Feature Information | 199 |
| Information About Flexible NetFlow—Prevent Export Storms | 199 |
| Flexible NetFlow—Prevent Export Storms Overview | 199 |
| How to Configure Flexible NetFlow—Prevent Export Storms | 200 |
| Configuring Flexible NetFlow—Prevent Export Storms | 200 |
| Configuration Examples for Flexible NetFlow—Prevent Export Storms | 201 |
| Example: Flexible NetFlow—Prevent Export Storms Configuration | 201 |
| Additional References for Flexible NetFlow—Prevent Export Storms | 202 |
| Feature Information for Flexible NetFlow—Prevent Export Storms | 202 |



CHAPTER 1

Read Me First

Important Information about Cisco IOS XE 16

Effective Cisco IOS XE Release 3.7.0E for Catalyst Switching and Cisco IOS XE Release 3.17S (for Access and Edge Routing) the two releases evolve (merge) into a single version of converged release—the Cisco IOS XE 16—providing one release covering the extensive range of access and edge products in the Switching and Routing portfolio.

Feature Information

Use [Cisco Feature Navigator](#) to find information about feature support, platform support, and Cisco software image support. An account on Cisco.com is not required.

Related References

- [Cisco IOS Command References, All Releases](#)

Obtaining Documentation and Submitting a Service Request

- To receive timely, relevant information from Cisco, sign up at [Cisco Profile Manager](#).
- To get the business impact you're looking for with the technologies that matter, visit [Cisco Services](#).
- To submit a service request, visit [Cisco Support](#).
- To discover and browse secure, validated enterprise-class apps, products, solutions and services, visit [Cisco Marketplace](#).
- To obtain general networking, training, and certification titles, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, access [Cisco Warranty Finder](#).



CHAPTER 2

Flexible Netflow Overview

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through the router. 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.

- [Finding Feature Information, on page 3](#)
- [Prerequisites for Flexible NetFlow, on page 3](#)
- [Restrictions for Flexible Netflow, on page 4](#)
- [Information About Flexible Netflow , on page 5](#)
- [How to Configure Flexible Netflow , on page 30](#)
- [Configuration Examples for Flexible Netflow , on page 45](#)
- [Additional References, on page 50](#)
- [Feature Information for Flexible NetFlow, on page 51](#)

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.

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

Prerequisites for Flexible NetFlow

- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands:
 - **match flow**
 - **match interface**
 - **match {ipv4 | ipv6}**
 - **match routing**

- **match transport**
- You are familiar with the Flexible NetFlow nonkey fields as they are defined in the following commands:
 - **collect counter**
 - **collect flow**
 - **collect interface**
 - **collect {ipv4 | ipv6}**
 - **collect routing**
 - **collect timestamp sys-uptime**
 - **collect transport**
- The networking device must be running a Cisco release that supports Flexible NetFlow.

IPv4 Traffic

- The networking device must be configured for IPv4 routing.
- One of the following must be enabled on your device 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 device and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding IPv6 or distributed Cisco Express Forwarding.

Restrictions for Flexible Netflow

- Flexible NetFlow is not supported on Switch Virtual Interface (SVI).
- Flexible Netflow has a significant impact on Embedded Services Processor (ESP) resources on the ASR 1000 Series Router. Depending on the cache record size and number, Flexible Netflow caches can consume a large amount of ESP DRAM.
- It is recommended that the total dataplane memory consumed by Flexible Netflow or Original Netflow is limited to a maximum of 25% of the amount of data plane DRAM for an ESP/FP.
- Predefined records specifying mask and prefix are not supported on Cisco IOS Release 12.2(50)SY.
- Flexible Netflow export will not work over an IPSEC VPN tunnel if the source of the netflow data is the same router where the VPN tunnel is terminated unless you configure the output-features command under the flow exporter. This command was added in IOS version 12.4(20)T with the fix for CSCsk25481

Information About Flexible Netflow

Flexible NetFlow Overview

Flexible NetFlow facilitates the creation of more complex configurations for traffic analysis and data export through the use of reusable configuration components.

Typical Uses for NetFlow

NetFlow is typically used for several key customer applications, including the following:

- **Network monitoring.** NetFlow data enables extensive near-real-time network monitoring capabilities. Flow-based analysis techniques are used by network operators to visualize traffic patterns associated with individual routers and switches and network-wide traffic patterns (providing aggregate traffic or application-based views) to provide proactive problem detection, efficient troubleshooting, and rapid problem resolution.
- **Application monitoring and profiling.** NetFlow data enables network managers to gain a detailed time-based view of application usage over the network. This information is used to plan, understand new services, and allocate network and application resources (for example, web server sizing and VoIP deployment) to meet customer demands responsively.
- **User monitoring and profiling.** NetFlow data enables network engineers to gain detailed understanding of customer and user use of network and application resources. This information may then be used to efficiently plan and allocate access, backbone, and application resources and to detect and resolve potential security and policy violations.
- **Network planning.** NetFlow can be used to capture data over a long period of time, affording the opportunity to track and anticipate network growth and plan upgrades to increase the number of routing devices, ports, and higher-bandwidth interfaces. NetFlow services data optimizes network planning for peering, backbone upgrades, and routing policy. NetFlow helps to minimize the total cost of network operations while maximizing network performance, capacity, and reliability. NetFlow detects unwanted WAN traffic, validates bandwidth and quality of service (QoS), and allows the analysis of new network applications. NetFlow will give you valuable information to reduce the cost of operating your network.
- **Security analysis.** NetFlow identifies and classifies distributed denial of service (DDoS) attacks, viruses, and worms in real time. Changes in network behavior indicate anomalies that are clearly demonstrated in Flexible NetFlow data. The data is also a valuable forensic tool to understand and replay the history of security incidents.
- **Billing and accounting.** NetFlow data provides fine-grained metering (for instance, flow data includes details such as IP addresses, packet and byte counts, time stamps, type of service (ToS), and application ports) for highly flexible and detailed resource utilization accounting. Service providers may use the information for billing based on time of day, bandwidth usage, application usage, quality of service, and so on. Enterprise customers may use the information for departmental charge back or cost allocation for resource utilization.
- **NetFlow data warehousing and data mining.** NetFlow data (or derived information) can be warehoused for later retrieval and analysis in support of proactive marketing and customer service programs (for example, discovering which applications and services are being used by internal and external users and targeting them for improved service, advertising, and so on). In addition, Flexible NetFlow data gives

market researchers access to the "who," "what," "where," and "how long" information relevant to enterprises and service providers.

Use of Flows in Original NetFlow and Flexible NetFlow

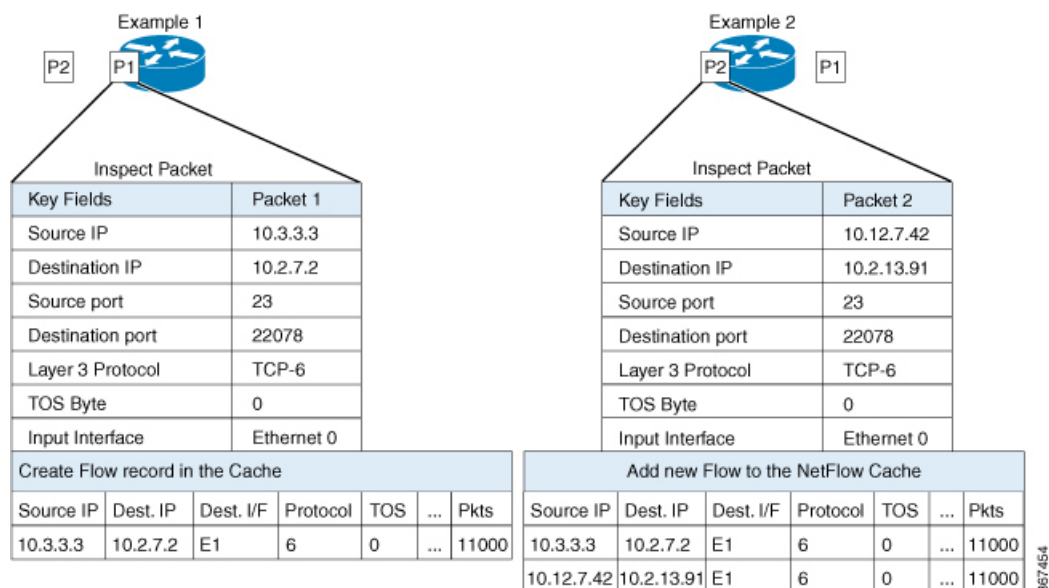
Original NetFlow and Flexible NetFlow both use the concept of flows. A *flow* is defined as a stream of packets between a given source and a given destination.

Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. When the value of the data in the key field of a datagram is unique with respect to the flows that already exist, a new flow is created.

Original NetFlow and Flexible NetFlow both use nonkey fields as the criteria for identifying fields from which data is captured from the flows. The flows are populated with data that is captured from the values in the nonkey fields.

The figure below is an example of the process for inspecting packets and creating flow records in the cache. In this example, two unique flows are created in the cache because different values are in the source and destination IP address key fields.

Figure 1: Packet Inspection



Original NetFlow and Benefits of Flexible NetFlow

Flexible NetFlow allows the flow to be user defined. The benefits of Flexible NetFlow include:

- High-capacity flow recognition, including scalability and aggregation of flow information.
- Enhanced flow infrastructure for security monitoring and DDoS detection and identification.
- New information from packets to adapt flow information to a particular service or operation in the network. The flow information available will be customizable by Flexible NetFlow users.

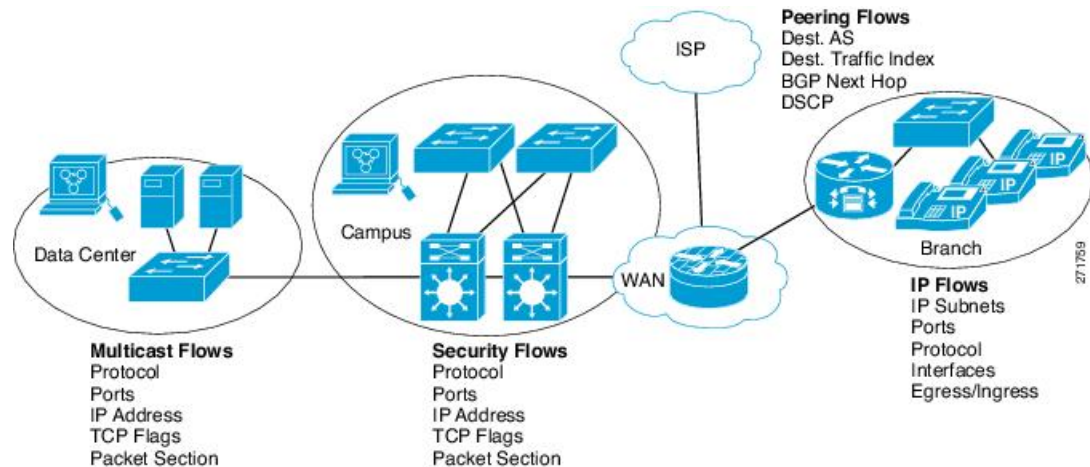
- Extensive use of Cisco's flexible and extensible NetFlow Version 9.
- A comprehensive IP accounting feature that can be used to replace many accounting features, such as IP accounting, Border Gateway Protocol (BGP) Policy Accounting, and persistent caches.

Flexible NetFlow allows you to understand network behavior with more efficiency, with specific flow information tailored for various services used in the network. The following are some example applications for a Flexible NetFlow feature:

- Flexible NetFlow enhances Cisco NetFlow as a security monitoring tool. For instance, new flow keys can be defined for packet length or MAC address, allowing users to search for a specific type of attack in the network.
- Flexible NetFlow allows you to quickly identify how much application traffic is being sent between hosts by specifically tracking TCP or UDP applications by the class of service (CoS) in the packets.
- The accounting of traffic entering a Multiprotocol Label Switching (MPLS) or IP core network and its destination for each next hop per class of service. This capability allows the building of an edge-to-edge traffic matrix.

The figure below is an example of how Flexible NetFlow might be deployed in a network.

Figure 2: Typical Deployment for Flexible NetFlow



Flexible NetFlow Components

Flexible NetFlow consists of components that can be used together in several variations to perform traffic analysis and data export. The user-defined flow records and the component structure of Flexible NetFlow facilitates the creation of various configurations for traffic analysis and data export on a networking device with a minimum number of configuration commands. Each flow monitor can have a unique combination of flow record, flow exporter, and cache type. If you change a parameter such as the destination IP address for a flow exporter, it is automatically changed for all the flow monitors that use the flow exporter. The same flow monitor can be used in conjunction with different flow samplers to sample the same type of network traffic at different rates on different interfaces. The following sections provide more information on Flexible NetFlow components:

Flow Records

In Flexible NetFlow a combination of key and non-key fields is called a *flow 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.

To use Flexible NetFlow to its fullest potential, you need to create your own customized records, as described in the following section(s):

NetFlow Predefined Records

Flexible NetFlow includes several predefined records that you can use to start monitoring traffic in your network. The predefined records are available to help you quickly deploy Flexible NetFlow and are easier to use than user-defined flow records. You can choose from a list of already defined records that may meet the needs for network monitoring. As Flexible NetFlow evolves, popular user-defined flow records will be made available as predefined records to make them easier to implement.

The predefined records ensure backward compatibility with your existing NetFlow collector configurations for the data that is exported. Each of the predefined records has a unique combination of key and nonkey fields that offer you the built-in ability to monitor various types of traffic in your network without customizing Flexible NetFlow on your router.

Two of the predefined records (NetFlow original and NetFlow IPv4/IPv6 original output), which are functionally equivalent, emulate original (ingress) NetFlow and the Egress NetFlow Accounting feature in original NetFlow, respectively. Some of the other Flexible NetFlow predefined records are based on the aggregation cache schemes available in original NetFlow. The Flexible NetFlow predefined records that are based on the aggregation cache schemes available in original NetFlow do not perform aggregation. Instead each flow is tracked separately by the predefined records.

User-Defined Records

Flexible NetFlow enables you to define your own records for a Flexible NetFlow flow monitor cache by specifying the key and nonkey fields to customize the data collection to your specific requirements. When you define your own records for a Flexible NetFlow flow monitor cache, they are referred to as *user-defined records*. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow. Flexible NetFlow enables you to capture counter values such as the number of bytes and packets in a flow as nonkey fields.

Flexible NetFlow adds a new Version 9 export format field type for the header and packet section types. Flexible NetFlow will communicate to the NetFlow collector the configured section sizes in the corresponding Version 9 export template fields. The payload sections will have a corresponding length field that can be used to collect the actual size of the collected section.

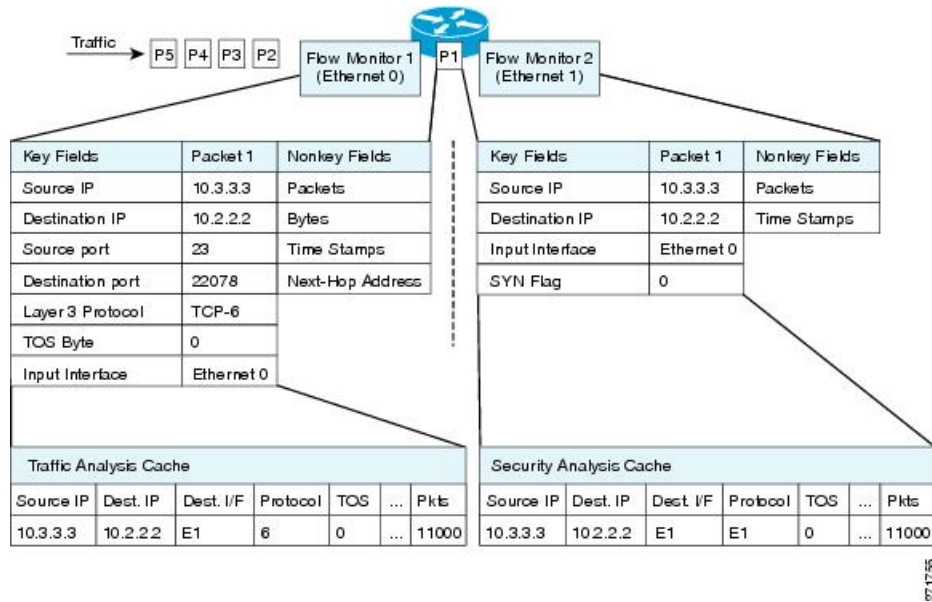
Flow Monitors

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring.

Flow data is collected from the network traffic and added to the flow monitor cache during the monitoring process based on the key and nonkey fields in the flow record.

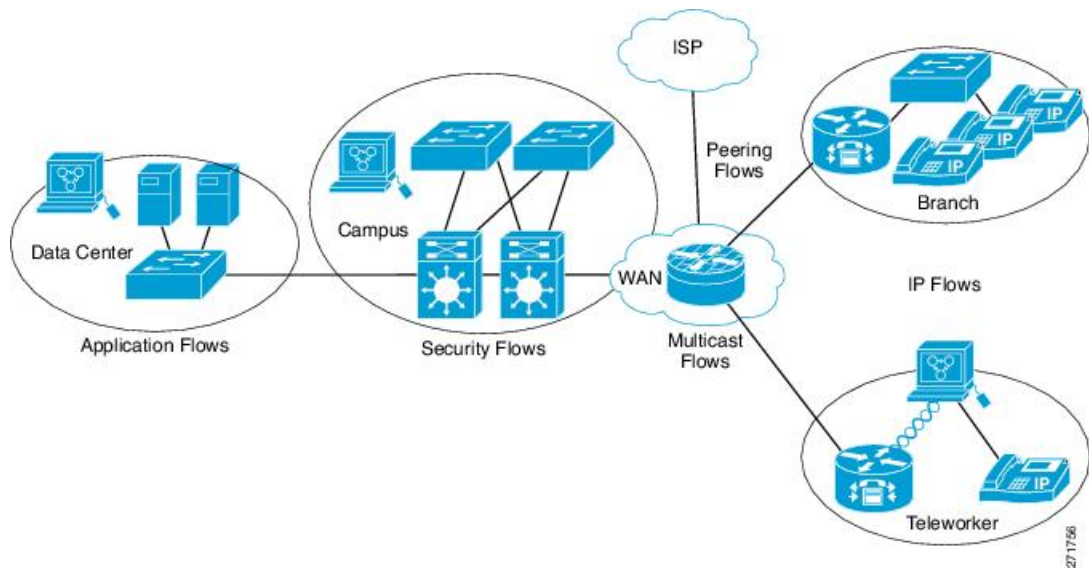
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

Figure 3: Example of Using Two Flow Monitors to Analyze the Same Traffic



The figure below shows a more complex example of how you can apply different types of flow monitors with custom records.

Figure 4: Complex Example of Using Multiple Types of Flow Monitors with Custom Records



Normal

The default cache type is “normal”. In this mode, the entries in the cache are aged out according to the timeout active and timeout inactive settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured.

Flow Exporters

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running NetFlow collector, for analysis and storage. Flow exporters are created as separate entities in the configuration. Flow exporters are assigned to flow monitors to provide data export capability for the flow monitors. You can create several flow exporters and assign them to one or more flow monitors to provide several export destinations. You can create one flow exporter and apply it to several flow monitors.

NetFlow Data Export Format Version 9

The basic output of NetFlow is a flow record. Several different formats for flow records have evolved as NetFlow has matured. The most recent evolution of the NetFlow export format is known as Version 9. The distinguishing feature of the NetFlow Version 9 export format is that it is template-based. Templates provide an extensible design to the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Using templates provides several key benefits:

- Third-party business partners who produce applications that provide collector or display services for NetFlow do not have to recompile their applications each time a new NetFlow feature is added. Instead, they should be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow quickly without breaking current implementations.
- NetFlow is “future-proofed” against new or developing protocols because the Version 9 format can be adapted to provide support for them.

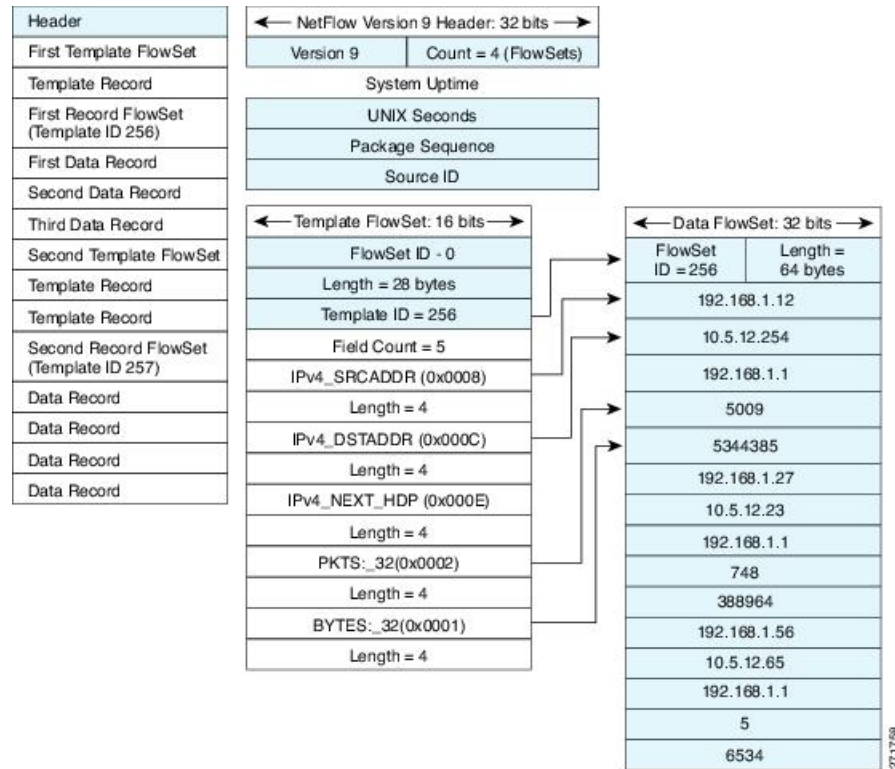
The Version 9 export format consists of a packet header followed by one or more template flow or data flow sets. A template flow set provides a description of the fields that will be present in future data flow sets. These data flow sets may occur later within the same export packet or in subsequent export packets. Template flow and data flow sets can be intermingled within a single export packet, as illustrated in the figure below.

Figure 5: Version 9 Export Packet



NetFlow Version 9 will periodically export the template data so the NetFlow collector will understand what data is to be sent and also export the data flow set for the template. The key advantage to Flexible NetFlow is that the user configures a flow record, which is effectively converted to a Version 9 template and then forwarded to the collector. The figure below is a detailed example of the NetFlow Version 9 export format, including the header, template flow, and data flow sets.

Figure 6: Detailed Example of the NetFlow Version 9 Export Format



For more information on the Version 9 export format, refer to the white paper titled [Cisco IOS NetFlow Version 9 Flow-Record Format](http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml), available at this URL:
http://www.cisco.com/en/US/tech/tk648/tk362/technologies_white_paper09186a00800a3db9.shtml.

Flow Samplers

Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running by limiting the number of packets that are selected for analysis.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the router of running the flow monitor is reduced because the number of packets that the flow monitor must analyze is reduced. The reduction in the number of packets that are analyzed by the flow monitor causes a corresponding reduction in the accuracy of the information stored in the flow monitor's cache.

Samplers are combined with flow monitors when they are applied to an interface with the **ip flow monitor** command.

Security Monitoring with Flexible NetFlow

Flexible NetFlow can be used as a network attack detection tool with capabilities to track all parts of the IP header and even packet sections and characterize this information into flows. Security monitoring systems can analyze Flexible NetFlow data, and upon finding an issue in the network, create a virtual bucket or virtual cache that will be configured to track specific information and identify details about the attack pattern or worm

propagation. The capability to create caches dynamically with specific information combined with input filtering (for example, filtering all flows to a specific destination) makes Flexible NetFlow a powerful security monitoring tool.

One common type of attack occurs when TCP flags are used to flood open TCP requests to a destination server (for example, a SYN flood attack). The attacking device sends a stream of TCP SYNs to a given destination address but never sends the ACK in response to the servers SYN-ACK as part of the TCP three-way handshake. The flow information needed for a security detection server requires the tracking of three key fields: destination address or subnet, TCP flags, and packet count. The security detection server may be monitoring general Flexible NetFlow information, and this data may trigger a detailed view of this particular attack by the Flexible NetFlow dynamically creating a new flow monitor in the router's configuration. The new flow monitor might include input filtering to limit what traffic is visible in the Flexible NetFlow cache along with the tracking of the specific information to diagnose the TCP-based attack. In this case the user may want to filter all flow information to the server destination address or subnet to limit the amount of information the security detection server needs to evaluate. If the security detection server decided it understood this attack, it might then program another flow monitor to collect and export payload information or sections of packets to take a deeper look at a signature within the packet. This example is just one of many possible ways that Flexible NetFlow can be used to detect security incidents.

Feature Comparison of Original NetFlow and Flexible NetFlow

The table below provides a feature-by-feature comparison of original NetFlow and Flexible NetFlow.

Table 1: Feature-by-Feature Comparison of Original NetFlow and Flexible NetFlow

| Feature | Original NetFlow | Flexible NetFlow | Comments |
|-------------------------------|------------------|------------------|---|
| NetFlow Data Capture | Supported | Supported | Data capture is available with the predefined and user-defined records in Flexible NetFlow. Flexible NetFlow has several predefined keys that emulate the traffic analysis capabilities of original NetFlow. |
| NetFlow Data Export | Supported | Supported | Flow exporters export data from the Flexible NetFlow flow monitor caches to remote systems. |
| NetFlow for IPv6 | Supported | Supported | IPv6 support was removed from original NetFlow in Cisco IOS Release 12.4(20)T. The Flexible NetFlow--IPv6 Unicast Flows feature implemented IPv6 support for Flexible NetFlow in Cisco IOS Release 12.4(20)T. |
| NetFlow BGP Next Hop Support | Supported | Supported | Available in the predefined and user-defined keys in Flexible NetFlow records. |
| Random Packet Sampled NetFlow | Supported | Supported | Available with Flexible NetFlow sampling. |

| Feature | Original NetFlow | Flexible NetFlow | Comments |
|--|------------------|------------------|--|
| NetFlow v9 Export Format | Supported | Supported | Available with Flexible NetFlow exporters. |
| NetFlow Subinterface Support | Supported | Supported | Flexible NetFlow monitors can be assigned to subinterfaces. |
| NetFlow Multiple Export Destinations | Supported | Supported | Available with Flexible NetFlow exporters. |
| NetFlow ToS-Based Router Aggregation | Supported | Supported | Available in the predefined and user-defined records in Flexible NetFlow records. |
| NetFlow Minimum Prefix Mask for Router-Based Aggregation | Supported | Supported | Available in the predefined and user-defined records. |
| NetFlow Input Filters | Supported | Not supported | -- |
| NetFlow MIB | Supported | Not supported | -- |
| Egress NetFlow Accounting | Supported | Supported | Flexible NetFlow monitors can be used to monitor egress traffic on interfaces and subinterfaces. |

Criteria for Identifying Traffic to Be Used in Analysis in Flexible NetFlow

If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a user-defined (custom) record using the Flexible NetFlow **collect** and **match** commands. Before you can create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields.

If you want to create a customized record for detecting network attacks, you must include the appropriate key and nonkey fields in the record to ensure that the router creates the flows and captures the data that you need to analyze the attack and respond to it. For example, SYN flood attacks are a common denial of service (DoS) attack in which TCP flags are used to flood open TCP requests to a destination host. When a normal TCP connection starts, a destination host receives a SYN (synchronize/start) packet from a source host and sends back a SYN ACK (synchronize acknowledge). The destination host must then hear an ACK (acknowledge) of the SYN ACK before the connection is established. This is referred to as the "TCP three-way handshake. While the destination host waits for the ACK to the SYN ACK, a connection queue of finite size on the destination host keeps track of connections waiting to be completed. This queue typically empties quickly because the ACK is expected to arrive a few milliseconds after the SYN ACK. The TCP SYN attack exploits this design by having an attacking source host generate TCP SYN packets with random source addresses toward a victim host. The victim destination host sends a SYN ACK back to the random source address and adds an entry to the connection queue. Because the SYN ACK is destined for an incorrect or nonexistent host, the last part of the TCP three-way handshake is never completed and the entry remains in the connection queue until a timer expires, typically for about one minute. When the source host rapidly generates TCP SYN packets from random IP addresses, the connection queue can be filled and TCP services (such as e-mail, file transfer, or WWW) can be denied to legitimate users.

The information needed for a security monitoring record for this type of DoS attack might include the following key and nonkey fields:

- Key fields:
 - Destination IP address or destination IP subnet
 - TCP flags
 - Packet count
- Nonkey fields
 - Destination IP address
 - Source IP address
 - Interface input and output



Tip Many users configure a general Flexible NetFlow monitor that triggers a more detailed Flexible NetFlow view of a DoS attack using these key and nonkey fields.

Benefit of Emulating Original NetFlow with Flexible NetFlow

Emulating original NetFlow with Flexible NetFlow enables you to deploy Flexible NetFlow quickly because you can use a predefined record instead of designing and configuring a custom user-defined record. You need only configure a flow monitor and apply it to an interface for Flexible NetFlow to start working like original NetFlow. You can add an optional exporter if you want to analyze the data that you collect with an application such as NetFlow collector.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.

Flow exporters are used to send the data that you collect with Flexible NetFlow to a remote system such as a NetFlow Collection Engine. Exporters use UDP as the transport protocol and use the Version 9 export format.

If you are familiar with original NetFlow, you already understand the format and content of the data that you collect and export with Flexible NetFlow when you emulate original NetFlow. You will be able to use the same techniques for analyzing the data.

Flexible NetFlow Predefined Records

Flexible NetFlow predefined records are based on the original NetFlow ingress and egress caches and the aggregation caches. The difference between the original NetFlow aggregation caches and the corresponding predefined Flexible NetFlow records is that the predefined records do not perform aggregation. Flexible NetFlow predefined records are associated with a Flexible NetFlow flow monitor the same way that you associate a user-defined (custom) record.

Benefits of Flexible NetFlow Predefined Records

If you have been using original NetFlow or original NetFlow with aggregation caches you can continue to capture the same traffic data for analysis when you migrate to Flexible NetFlow by using the predefined records available with Flexible NetFlow. Many users will find that the preexisting Flexible NetFlow records are suitable for the majority of their traffic analysis requirements.

NetFlow Original and NetFlow IPv4 Original Input Predefined Records

The Flexible NetFlow "NetFlow original" and "NetFlow IPv4 original input" predefined records can be used interchangeably because they have the same key and nonkey fields. The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow original" and "NetFlow IPv4 original input" predefined records are shown in the table below.

Table 2: Key and Nonkey Fields Used by the Flexible NetFlow NetFlow Original and NetFlow IPv4 Original Input Predefined Records

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| IP ToS | Key | Value in the type of service (ToS) field. |
| IP Protocol | Key | Value in the IP protocol field. |
| IP Source Address | Key | IP source address. |
| IP Destination Address | Key | IP destination address. |
| Transport Source Port | Key | Value of the transport layer source port field. |
| Transport Destination Port | Key | Value of the transport layer destination port field. |
| Interface Input | Key | Interface on which the traffic is received. |
| Flow Sampler ID | Key | ID number of the flow sampler (if flow sampling is enabled). |
| IP Source AS | Nonkey | Source autonomous system number. |
| IP Destination AS | Nonkey | Destination autonomous system number. |
| IP Next Hop Address | Nonkey | IP address of the next hop. |
| IP Source Mask | Nonkey | Mask for the IP source address. |
| IP Destination Mask | Nonkey | Mask for the IP destination address. |
| TCP Flags | Nonkey | Value in the TCP flag field. |
| Interface Output | Nonkey | Interface on which the traffic is transmitted. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

NetFlow IPv4 Original Output Predefined Record

The Flexible NetFlow "NetFlow IPv4 original output" predefined record is used to emulate the original NetFlow Egress NetFlow Accounting feature that was released in Cisco IOS Release 12.3(11)T. The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow IPv4 original output" predefined record are shown in the table below.

Table 3: Key and Nonkey Fields Used by the Flexible NetFlow NetFlow IPv4 Original Output Predefined Record

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| IP ToS | Key | Value in the ToS field. |
| IP Protocol | Key | Value in the IP protocol field. |
| IP Source Address | Key | IP source address. |
| IP Destination Address | Key | IP destination address. |
| Transport Source Port | Key | Value of the transport layer source port field. |
| Transport Destination Port | Key | Value of the transport layer destination port field. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Sampler ID | Key | ID number of the flow sampler (if flow sampling is enabled). |
| IP Source AS | Nonkey | Source autonomous system number. |
| IP Destination AS | Nonkey | Destination autonomous system number. |
| IP Next Hop Address | Nonkey | IP address of the next hop. |
| IP Source Mask | Nonkey | Mask for the IP source address. |
| IP Destination Mask | Nonkey | Mask for the IP destination address. |
| TCP Flags | Nonkey | Value in the TCP flag field. |
| Interface Input | Nonkey | Interface on which the traffic is received. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

The configuration in the [Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic, on page 48](#) uses the predefined Flexible NetFlow "NetFlow original output" record.

NetFlow IPv6 Original Input Predefined Record

The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow IPv6 original input" predefined record are shown in the table below.

Table 4: Key and Nonkey Fields Used by the Flexible NetFlow NetFlow IPv6 Original Input Predefined Record

| Field | Key or NonKey Field | Definition |
|--------------------------------|---------------------|---|
| Traffic Class | Key | Value in the traffic class field. |
| Flow Label | Key | Flow label. |
| Protocol | Key | Value in the protocol field. |
| Extension Map | Key | Value in the extension map bitmap. |
| IP Source Address | Key | IP source address. |
| IP Destination Address | Key | IP destination address. |
| Transport Source Port | Key | Value of the transport layer source port field. |
| Transport Destination Port | Key | Value of the transport layer destination port field. |
| Interface Input | Key | Interface on which the traffic is received. |
| Flow Direction | Key | The direction of the flow. |
| Flow Sampler | Key | ID number of the flow sampler (if flow sampling is enabled). |
| Routing Source AS | Nonkey | Source autonomous system number. |
| Routing Destination AS | Nonkey | Destination autonomous system number. |
| Routing Next-hop Address | Nonkey | IP address of the next hop. |
| IP Source Mask | Nonkey | Mask for the IP source address. |
| IP Destination Mask | Nonkey | Mask for the IP destination address. |
| Transport TCP Flags | Nonkey | Value in the TCP flag field. |
| Interface Output | Nonkey | Interface over which the traffic is transmitted. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |

| Field | Key or NonKey Field | Definition |
|-------------------------------|---------------------|--|
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

NetFlow IPv6 Original Output Predefined Record

The key and nonkey fields and the counters for the Flexible NetFlow "NetFlow IPv6 original output" predefined record are shown in the table below.

Table 5: Key and Nonkey Fields Used by the Flexible NetFlow NetFlow IPv6 Original Output Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------|---------------------|--|
| Traffic Class | Key | Value in the traffic class field. |
| Flow Label | Key | The flow label. |
| Protocol | Key | Value in the protocol field. |
| Extension Map | Key | Value in the extension map bitmap. |
| IP Source Address | Key | IP source address. |
| IP Destination Address | Key | IP destination address. |
| Transport Source Port | Key | Value of the transport layer source port field. |
| Transport Destination Port | Key | Value of the transport layer destination port field. |
| Interface Output | Key | Interface over which the traffic is transmitted. |
| Flow Direction | Key | The direction of the flow. |
| Flow Sampler | Key | ID number of the flow sampler (if flow sampling is enabled). |
| Routing Source AS | Nonkey | Source autonomous system number. |
| Routing Destination AS | Nonkey | Destination autonomous system number. |
| Routing Next-hop Address | Nonkey | IP address of the next hop. |
| IP Source Mask | Nonkey | Mask for the IP source address. |
| IP Destination Mask | Nonkey | Mask for the IP destination address. |
| Transport TCP Flags | Nonkey | Value in the TCP flag field. |
| Interface Input | Nonkey | Interface on which the traffic is received. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Autonomous System Predefined Record

The Flexible NetFlow "autonomous system" predefined record creates flows based on autonomous system-to-autonomous system traffic flow data. The Flexible NetFlow "autonomous system" predefined record uses the same key and nonkey fields as the original NetFlow "autonomous system" aggregation cache.



Note This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "autonomous system" predefined record.

Table 6: Key and Nonkey Fields Used by the Flexible NetFlow Autonomous System Predefined Record

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|--|
| IP Source AS | Key | Autonomous system of the source IP address (peer or origin). |
| IP Destination AS | Key | Autonomous system of the destination IP address (peer or origin). |
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds since this device was first booted) when the last packet was switched. |

Autonomous System ToS Predefined Record

The Flexible NetFlow "autonomous system ToS" predefined record creates flows based on autonomous system-to-autonomous system and type of service (ToS) traffic flow data. The Flexible NetFlow "autonomous

system ToS" predefined record uses the same key and nonkey fields as the original NetFlow "autonomous system ToS" aggregation cache.



Note This predefined record can be used to analyze only IPv4 traffic.



Tip This predefined record is particularly useful for generating autonomous system-to-autonomous system traffic flow data.

The table below lists the key and nonkey fields used in the Flexible NetFlow "autonomous system ToS" predefined record.

Table 7: Key and Nonkey Fields Used by the Flexible NetFlow Autonomous System ToS Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------------|---------------------|---|
| IP ToS | Key | Value in the ToS field. |
| IP Source autonomous system | Key | Autonomous system of the source IP address (peer or origin). |
| IP Destination autonomous system | Key | Autonomous system of the destination IP address (peer or origin). |
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

BGP Next-Hop Predefined Record

The Flexible NetFlow "BGP next-hop" predefined record creates flows based on Border Gateway Protocol (BGP) traffic flow data.



Note This predefined record can be used to analyze only IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "BGP next-hop" predefined record.

Table 8: Key and Nonkey Fields Used by the Flexible NetFlow BGP Next-Hop Predefined Record

| Field | Key or Nonkey Field | Definition |
|-----------------------------------|---------------------|---|
| Routing Source AS | Key | Autonomous system of the source IP address. |
| Routing Destination AS | Key | Autonomous system of the destination IP address. |
| Routing Next-hop Address IPv6 BGP | Key | IPv6 address of the BGP next hop. |
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Timestamp Sys-uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Timestamp Sys-uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

BGP Next-Hop ToS Predefined Record

The Flexible NetFlow "BGP next-hop ToS" predefined record creates flows based on BGP and ToS traffic flow data. The Flexible NetFlow "BGP next-hop ToS" predefined record uses the same key and nonkey fields as the original NetFlow "BGP next-hop ToS" aggregation cache.



Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the "BGP next-hop ToS" predefined record.

Table 9: Key and Nonkey Fields Used by the Flexible NetFlow BGP Next-Hop ToS Predefined Record

| Field | Key or Nonkey Field | Definition |
|-----------------------------|---------------------|--|
| IP ToS | Key | Value in the ToS field. |
| IP Source autonomous system | Key | Autonomous system of the source IP address (peer or origin). |

| Field | Key or Nonkey Field | Definition |
|----------------------------------|---------------------|---|
| IP Destination autonomous system | Key | Autonomous system of the destination IP address (peer or origin). |
| IPv4 Next Hop Address BGP | Key | IPv4 address of the BGP next hop. |
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Destination Prefix Predefined Record

The Flexible NetFlow "destination prefix" predefined record creates flows based on destination prefix traffic flow data. The Flexible NetFlow "destination prefix" predefined record uses the same key and nonkey fields as the original NetFlow "destination prefix" aggregation cache.



Note This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "destination prefix" predefined record.

Table 10: Key and Nonkey Fields Used by the Flexible NetFlow Destination Prefix Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------------|---------------------|---|
| IP Destination autonomous system | Key | Autonomous system of the destination IP address (peer or origin). |
| IPv4 or IPv6 Destination Prefix | Key | Destination IP address ANDed with the destination prefix mask. |
| IPv4 or IPv6 Destination Mask | Key | Number of bits in the destination prefix. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Destination Prefix ToS Predefined Record

The Flexible NetFlow "destination prefix ToS" predefined record creates flows based on destination prefix and ToS traffic flow data. The Flexible NetFlow "destination prefix ToS" predefined record uses the same key and nonkey fields as the original NetFlow "destination prefix ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the destinations of network traffic passing through a NetFlow-enabled device.



Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "destination prefix ToS" predefined record.

Table 11: Key and Nonkey Fields Used by the Flexible NetFlow Destination Prefix ToS Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------------|---------------------|---|
| IP ToS | Key | Value in the ToS field. |
| IP Destination autonomous system | Key | Autonomous system of the destination IP address (peer or origin). |
| IPv4 Destination Prefix | Key | Destination IP address ANDed with the destination prefix mask. |
| IPv4 Destination Mask | Key | Number of bits in the destination prefix. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Prefix Predefined Record

The Flexible NetFlow "prefix" predefined record creates flows based on the source and destination prefixes in the traffic flow data. The Flexible NetFlow "prefix" predefined record uses the same key and nonkey fields as the original NetFlow "prefix" aggregation cache.



Note This predefined record can be used to analyze IPv4 and IPv6 traffic. For IPv6 traffic, a minimum prefix mask length of 0 bits is assumed.

The table below lists the key and nonkey fields used in the Flexible NetFlow "prefix" predefined record.

Table 12: Key and Nonkey Fields Used by the Flexible NetFlow Prefix Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------------|---------------------|--|
| IP Source autonomous system | Key | Autonomous system of the source IP address (peer or origin). |
| IP Destination autonomous system | Key | Autonomous system of the destination IP address (peer or origin). |
| IPv4 or IPv6 Source Prefix | Key | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs. |
| IPv4 or IPv6 Source Mask | Key | Number of bits in the source prefix. |
| IPv4 or IPv6 Destination Prefix | Key | Destination IP address ANDed with the destination prefix mask. |
| IPv4 or IPv6 Destination Mask | Key | Number of bits in the destination prefix. |
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Prefix Port Predefined Record

The Flexible NetFlow "prefix port" predefined record creates flows based on source and destination prefixes and ports in the traffic flow data. The Flexible NetFlow "prefix port" predefined record uses the same key and nonkey fields as the original NetFlow "prefix port" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device.



Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the destination Flexible NetFlow "prefix port" predefined record.

Table 13: Key and Nonkey Fields Used by the Flexible NetFlow Prefix Port Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------|---------------------|--|
| IP ToS | Key | Value in the ToS field. |
| IP Protocol | Key | Value in the IP protocol field. |
| IPv4 Source Prefix | Key | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs. |
| IPv4 Source Mask | Key | Number of bits in the source prefix. |
| IPv4 Destination Prefix | Key | Destination IP address ANDed with the destination prefix mask. |
| IPv4 Destination Mask | Key | Number of bits in the destination prefix. |
| Transport Source Port | Key | Value in the transport layer source port field. |
| Transport Destination Port | Key | Value in the transport layer destination port field. |
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Prefix ToS Predefined Record

The Flexible NetFlow "prefix ToS" predefined record creates flows based on source and destination prefixes and ToS traffic flow data. The Flexible NetFlow "prefix ToS" predefined record uses the same key and nonkey fields as the original NetFlow "destination prefix ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device.



Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "prefix ToS" predefined record.

Table 14: Key and Nonkey Fields Used by the Flexible NetFlow Prefix ToS Predefined Record

| Field | Key or Nonkey Field | Definition |
|----------------------------------|---------------------|--|
| IP ToS | Key | Value in the ToS field. |
| IP Source autonomous system | Key | Autonomous system of the source IP address (peer or origin). |
| IP Destination autonomous system | Key | Autonomous system of the destination IP address (peer or origin). |
| IPv4 Source Prefix | Key | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs. |
| IPv4 Source Mask | Key | Number of bits in the source prefix. |
| IPv4 Destination Prefix | Key | Destination IP address ANDed with the destination prefix mask. |
| IPv4 Destination Mask | Key | Number of bits in the destination prefix. |

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| Interface Input | Key | Interface on which the traffic is received. |
| Interface Output | Key | Interface on which the traffic is transmitted. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Protocol Port Predefined Record

The Flexible NetFlow "protocol port" predefined record creates flows based on protocols and ports in the traffic flow data. The Flexible NetFlow "protocol port" predefined record uses the same key and nonkey fields as the original NetFlow "protocol port" aggregation cache.



Note This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "protocol port" predefined record.

Table 15: Key and Nonkey Fields Used by the Flexible NetFlow Protocol Port Predefined Record

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| IP Protocol | Key | Value in the IP protocol field. |
| Transport Source Port | Key | Value in the transport layer source port field. |
| Transport Destination Port | Key | Value in the transport layer destination port field. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |

| Field | Key or Nonkey Field | Definition |
|-------------------------------|---------------------|--|
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Protocol Port ToS Predefined Record

The Flexible NetFlow "protocol port ToS" predefined record creates flows based on the protocol, port, and ToS value in the traffic data. The Flexible NetFlow "protocol port ToS" predefined record uses the same key and nonkey fields as the original NetFlow "protocol port ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine network usage by type of traffic.



Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "protocol port ToS" predefined record.

Table 16: Key and Nonkey Fields Used by the Flexible NetFlow Protocol Port ToS Predefined Record

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|---|
| IP ToS | Key | Value in the ToS field. |
| IP Protocol | Key | Value in the IP protocol field. |
| Transport Source Port | Key | Value in the transport layer source port field. |
| Transport Destination Port | Key | Value in the transport layer destination port field. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Source Prefix Predefined Record

The Flexible NetFlow "source prefix" predefined record creates flows based on source prefixes in the network traffic. The Flexible NetFlow "source prefix" predefined record uses the same key and nonkey fields as the original NetFlow "source prefix" aggregation cache.



Note This predefined record can be used to analyze IPv4 and IPv6 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "source prefix" predefined record.

Table 17: Key and Nonkey Fields Used by the Flexible NetFlow Source Prefix Predefined Record

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|--|
| IP Source autonomous system | Key | Autonomous system of the source IP address (peer or origin). |
| IPv4 or IPv6 Source Prefix | Key | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs. |
| IPv4 or IPv6 Source Mask | Key | Number of bits in the source prefix. |
| Interface Input | Key | Interface on which the traffic is received. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

Source Prefix ToS Predefined Record

The Flexible NetFlow "source prefix ToS" predefined record creates flows based on source prefixes and ToS values in the network traffic. The Flexible NetFlow "source prefix ToS" predefined record uses the same key and nonkey fields as the original NetFlow "source prefix ToS" aggregation cache.

This predefined record is particularly useful for capturing data with which you can examine the sources of network traffic passing through a NetFlow-enabled device.



Note This predefined record can be used to analyze only IPv4 traffic.

The table below lists the key and nonkey fields used in the Flexible NetFlow "source prefix ToS" predefined record.

Table 18: Key and Nonkey Fields Used by the Flexible NetFlow Source Prefix ToS Predefined Record

| Field | Key or Nonkey Field | Definition |
|--------------------------------|---------------------|--|
| IP ToS | Key | Value in the ToS field. |
| IP Source autonomous system | Key | Autonomous system of the source IP address (peer or origin). |
| IPv4 Source Prefix | Key | Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs. |
| IPv4 Source Mask | Key | Number of bits in the source prefix. |
| Interface Input | Key | Interface on which the traffic is received. |
| Flow Direction | Key | Direction in which the flow is being monitored. |
| Counter Bytes | Nonkey | Number of bytes seen in the flow. |
| Counter Packets | Nonkey | Number of packets seen in the flow. |
| Time Stamp System Uptime First | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the first packet was switched. |
| Time Stamp System Uptime Last | Nonkey | System uptime (time, in milliseconds, since this device was first booted) when the last packet was switched. |

How to Configure Flexible Netflow

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} address
6. Repeat Step 5 as required to configure additional key fields for the record.

7. **match flow cts** {source | destination} group-tag
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** record-name
12. **show running-config flow record** record-name

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow record record-name Example: Device(config)# flow record FLOW-RECORD-1 | Creates a flow record and enters Flexible NetFlow flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record. |
| Step 4 | description description Example: Device(config-flow-record)# description Used for basic traffic analysis | (Optional) Creates a description for the flow record. |
| Step 5 | match {ip ipv6} {destination source} address Example: Device(config-flow-record)# match ipv4 destination address | Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields. |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | match flow cts {source destination} group-tag Example: Device(config-flow-record)# match flow cts source group-tag Device(config-flow-record)# match flow cts destination group-tag | Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields. |

| | Command or Action | Purpose |
|----------------|--|--|
| | | <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |
| Step 8 | <p>collect interface {input output}</p> <p>Example:</p> <pre>Device(config-flow-record)# collect interface input</pre> | <p>Configures the input interface as a nonkey field for the record.</p> <p>Note This example configures the input interface as a nonkey field for the record.</p> |
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | <p>end</p> <p>Example:</p> <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | <p>show flow record <i>record-name</i></p> <p>Example:</p> <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | <p>show running-config flow record <i>record-name</i></p> <p>Example:</p> | (Optional) Displays the configuration of the specified flow record. |

| | Command or Action | Purpose |
|--|--|---------|
| | Device# show running-config flow record FLOW_RECORD-1 | |

Displaying the Current Status of a Flow Record

Perform this optional task to display the current status of a flow record.

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 show flow record

The **show flow record** command shows the current status of the flow monitor that you specify.

Example:

```
Device# show flow record

flow record FLOW-RECORD-2:
  Description:      Used for basic IPv6 traffic analysis
  No. of users:    1
  Total field space: 53 bytes
  Fields:
    match ipv6 destination address
    collect counter bytes
    collect counter packets
flow record FLOW-RECORD-1:
  Description:      Used for basic IPv4 traffic analysis
  No. of users:    1
  Total field space: 29 bytes
  Fields:
    match ipv4 destination address
    collect counter bytes
    collect counter packets
```

Verifying the Flow Record Configuration

Perform this optional task to verify the configuration commands that you entered.

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 show running-config flow record

The **show running-config flow record** command shows the configuration commands of the flow monitor that you specify.

Example:

```
Device# show running-config flow record

Current configuration:
!
flow record FLOW-RECORD-2
description Used for basic IPv6 traffic analysis
match ipv6 destination address
collect counter bytes
collect counter packets
!
flow record FLOW-RECORD-1
description Used for basic IPv4 traffic analysis
match ipv4 destination address
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
```

Configuring a Flow Monitor for IPv4 or IPv6 Traffic Using the Predefined Record

To configure a flow monitor for IPv4/IPv6 traffic using the Flexible NetFlow "NetFlow IPv4/IPv6 original input" predefined record for the flow monitor, perform the following required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.



Note

You must remove a flow monitor from all of the interfaces to which you have applied it before you can modify the **record** format of the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record netflow** {*ipv4* | *ipv6*} **original-input**
6. **end**
7. **show flow monitor** [[*name*] *monitor-name* [**cache** [**format** {*csv* | *record* | *table*}]]][**statistics**]]

8. show running-config flow monitor *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: Device(config-flow-monitor)# description Used for monitoring IPv4 traffic | (Optional) Creates a description for the flow monitor. |
| Step 5 | record netflow {ipv4 ipv6} original-input Example: Device(config-flow-monitor)# record netflow ipv4 original-input | Specifies the record for the flow monitor. |
| Step 6 | end Example: Device(config-flow-monitor)# end | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 7 | show flow monitor [[name] <i>monitor-name</i> [cache [format {csv record table}]]][statistics]] Example: Device# show flow monitor FLOW-MONITOR-2 cache | (Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. |
| Step 8 | show running-config flow monitor <i>monitor-name</i> Example: Device# show flow monitor FLOW_MONITOR-1 | (Optional) Displays the configuration of the specified flow monitor. |

Configuring a Flow Exporter for the Flow Monitor

Perform this optional task to configure a flow exporter for the flow monitor in order to export the data that is collected by Flexible NetFlow to a remote system for further analysis and storage.

Flow exporters are used to send the data that you collect with Flexible NetFlow to a remote system such as a NetFlow Collection Engine. Exporters use UDP as the transport protocol and use the Version 9 export format.



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 either an IPv4 or IPv6 address.



Note When you configure an exporter, configure the exporter in such a way that the source interface is defined as a WAN interface. This configuration helps you prevent any unpredictable behavior because the NAT is not applied on the packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **transport udp** *udp-port*
8. **exit**
9. **flow monitor** *flow-monitor-name*
10. **exporter** *exporter-name*
11. **end**
12. **show flow exporter** *exporter-name*
13. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|----------------|---|---|
| | Device# configure terminal | |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates a flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: Device(config-flow-exporter)# description Exports to datacenter | (Optional) Creates a description for the flow exporter. |
| Step 5 | destination { <i>hostname</i> <i>ip-address</i> } [vrf <i>vrf-name</i>] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the hostname or IP address of the system to which the exporter sends data. Note You can export to a destination using either an IPv4 or IPv6 address. |
| Step 6 | export-protocol { netflow-v5 netflow-v9 ipfix } Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. <ul style="list-style-type: none"> Default: netflow-v9. |
| Step 7 | transport udp <i>udp-port</i> Example: Device(config-flow-exporter)# transport udp 65 | Configures UDP as the transport protocol and specifies the UDP port on which the destination system is listening for exported Flexible NetFlow traffic. |
| Step 8 | exit Example: Device(config-flow-exporter)# exit | Exits Flexible NetFlow flow exporter configuration mode and returns to global configuration mode. |
| Step 9 | flow monitor <i>flow-monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Enters Flexible NetFlow flow monitor configuration mode for the flow monitor that you created previously. |
| Step 10 | exporter <i>exporter-name</i> Example: Device(config-flow-monitor)# exporter EXPORTER-1 | Specifies the name of an exporter that you created previously. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 11 | end Example: Device(config-flow-monitor)# end | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 12 | show flow exporter <i>exporter-name</i> Example: Device# show flow exporter FLOW_EXPORTER-1 | (Optional) Displays the current status of the specified flow exporter. |
| Step 13 | show running-config flow exporter <i>exporter-name</i> Example: Device<# show running-config flow exporter FLOW_EXPORTER-1 | (Optional) Displays the configuration of the specified flow exporter. |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {*timeout* {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]

11. show running-config flow monitor *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre># configure terminal</pre> | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: <pre>(config)# flow monitor FLOW-MONITOR-1</pre> | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: <pre>(config-flow-monitor)# description Used for basic ipv4 traffic analysis</pre> | (Optional) Creates a description for the flow monitor. |
| Step 5 | record {<i>record-name</i>} Example: <pre>(config-flow-monitor)# record FLOW-RECORD-1</pre> | Specifies the record for the flow monitor. |
| Step 6 | cache {<i>timeout</i> {<i>active</i>} <i>seconds</i> <i>type</i> { normal } } Example: | <ul style="list-style-type: none"> • type normal—Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: <pre>(config-flow-monitor)# exporter EXPORTER-1</pre> | (Optional) Specifies the name of an exporter that was created previously. |
| Step 9 | end Example: <pre>(config-flow-monitor)# end</pre> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 10 | show flow monitor [[<i>name</i>] <i>monitor-name</i> [cache [<i>format</i> { <i>csv</i> <i>record</i> <i>table</i> }]]] Example: <pre># show flow monitor FLOW-MONITOR-2 cache</pre> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <pre># show running-config flow monitor FLOW_MONITOR-1</pre> | (Optional) Displays the configuration of the specified flow monitor. |

Displaying the Current Status of a Flow Monitor

Perform this optional task to display the current status of a flow monitor.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** *monitor-name*

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 show flow monitor *monitor-name*

The **show flow monitor** command shows the current status of the flow monitor that you specify.

Example:

```
Device# show flow monitor FLOW-MONITOR-1

Flow Monitor FLOW-MONITOR-1:
  Description:      Used for basic ipv4 traffic analysis
  Flow Record:     FLOW-RECORD-1
  Flow Exporter:   EXPORTER-1
  Cache:
    Type:          normal
    Status:        allocated
    Size:          1000 entries / 50052 bytes
    Inactive Timeout: 15 secs
    Active Timeout: 1800 secs
    Update Timeout: 1800 secs
```

Displaying the Data in the Flow Monitor Cache

Perform this optional task to display the data in the flow monitor cache.

Before you begin

The interface on which you applied the input flow monitor must be receiving traffic that meets the criteria defined by the NetFlow original record before you can display the flows in the flow monitor cache.

SUMMARY STEPS

1. **enable**
2. **show flow monitor name *monitor-name* cache format record**

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 show flow monitor name *monitor-name* cache format record

The **show flow monitor name *monitor-name* cache format record** command string displays the status, statistics, and flow data in the cache for a flow monitor.

Example:

```
Device# show flow monitor name FLOW-MONITOR-1 cache format record

Cache type:                               Normal
Cache size:                               1000
Current entries:                           4
High Watermark:                            4
Flows added:                               101
Flows aged:                                97
- Active timeout ( 1800 secs)              3
- Inactive timeout ( 15 secs)              94
- Event aged                               0
- Watermark aged                           0
- Emergency aged                           0
IPV4 DESTINATION ADDRESS: 172.16.10.5
ipv4 source address:                       10.10.11.1
trns source port:                           25
trns destination port:                      25
counter bytes:                              72840
counter packets:                            1821
IPV4 DESTINATION ADDRESS: 172.16.10.2
ipv4 source address:                       10.10.10.2
trns source port:                           20
trns destination port:                      20
```

```

counter bytes:          3913860
counter packets:       7326
IPV4 DESTINATION ADDRESS: 172.16.10.200
ipv4 source address:   192.168.67.6
trns source port:      0
trns destination port: 3073
counter bytes:         51072
counter packets:       1824

```

Device# **show flow monitor name FLOW-MONITOR-2 cache format record**

```

Cache type:                Normal
Cache size:                 1000
Current entries:            2
High Watermark:            3
Flows added:                95
Flows aged:                93
- Active timeout ( 1800 secs) 0
- Inactive timeout ( 15 secs) 93
- Event aged                 0
- Watermark aged             0
- Emergency aged             0
IPV6 DESTINATION ADDRESS: 2001:DB8:4:ABCD::2
ipv6 source address:       2001:DB8:1:ABCD::1
trns source port:          33572
trns destination port:     23
counter bytes:              19140
counter packets:           349
IPV6 DESTINATION ADDRESS: FF02::9
ipv6 source address:       FE80::A8AA:BBFF:FEBB:CC03
trns source port:          521
trns destination port:     521
counter bytes:              92
counter packets:           1

```

Verifying the Flow Monitor Configuration

Perform this optional task to verify the configuration commands that you entered.

SUMMARY STEPS

1. **enable**
2. **show running-config flow monitor**

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```

Device> enable
Device#

```

Step 2 **show running-config flow monitor**

The **show running-config flow monitor** command shows the configuration commands of the flow monitor that you specify.

Example:

```
Device# show running-config flow monitor FLOW-MONITOR-1

Current configuration:
!
flow monitor FLOW-MONITOR-1
  description Used for basic ipv4 traffic analysis
  record FLOW-RECORD-1
  exporter EXPORTER-1
  cache entries 1000
!
```

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: | Specifies an interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device(config)# interface GigabitEthernet 0/0/0 | |
| Step 4 | <p>{ip ipv6} flow monitor <i>monitor-name</i> {input output}</p> <p>Example:</p> <pre>Device(config-if)# ip flow monitor FLOW-MONITOR-1 input</pre> | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | <p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | <p>show flow interface <i>type number</i></p> <p>Example:</p> <pre>Device# show flow interface GigabitEthernet 0/0/0</pre> | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |
| Step 8 | <p>show flow monitor name <i>monitor-name</i> cache format record</p> <p>Example:</p> <pre>Device# show flow monitor name FLOW_MONITOR-1 cache format record</pre> | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Verifying That Flexible NetFlow Is Enabled on an Interface

Perform this optional task to verify that Flexible NetFlow is enabled on an interface.

SUMMARY STEPS

1. **enable**
2. **show flow interface *type number***

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```


Step 2 `show flow interface type number`

The `show flow interface` command verifies that Flexible NetFlow is enabled on an interface.

Example:

```
Device# show flow interface GigabitEthernet 0/0/0

Interface GigabitEthernet0/0/0
  FNF: monitor:      FLOW-MONITOR-1
      direction:    Input
      traffic(ip):   on
  FNF: monitor:      FLOW-MONITOR-2
      direction:    Input
      traffic(ipv6): on
Device# show flow interface GigabitEthernet 1/0/0
Interface GigabitEthernet1/0/0
  FNF: monitor:      FLOW-MONITOR-1
      direction:    Output
      traffic(ip):   on
  FNF: monitor:      FLOW-MONITOR-2
      direction:    Input
      traffic(ipv6): on
```

Configuration Examples for Flexible Netflow

Example: Configuring a Flexible NetFlow Predefined Record for IPv4 Traffic

The following example shows how to configure a flow monitor using the Flexible NetFlow "BGP ToS next-hop" predefined record to monitor IPv4 traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 bgp-nexthop-tos
 exit
!
ip cef
!
interface Ethernet 0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

Example: Configuring a Flexible NetFlow Predefined Record for IPv6 Traffic

The following example shows how to configure a flow monitor using the Flexible NetFlow "source prefix" predefined record to monitor IPv6 traffic.

This sample starts in global configuration mode:

```
!
```

Example: Configuring a Normal Flow Record Cache with a Limited Number of Flows

```

flow monitor FLOW-MONITOR-2
 record netflow ipv6 source-prefix
 exit
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 input
!

```

Example: Configuring a Normal Flow Record Cache with a Limited Number of Flows

The following example is designed to monitor the type of service (ToS) field usage on all interfaces in the router. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This example starts in global configuration mode.

```

!
flow record QOS_RECORD
 description UD: Flow Record to monitor the use of TOS within this router/network
 match interface input
 match interface output
 match ipv4 tos
 collect counter packets
 collect counter bytes
 exit
!
flow monitor QOS_MONITOR
 description UD: Flow Monitor which watches the limited combinations of interface and TOS
 record QOS_RECORD
 cache type normal
 cache entries 8192 ! 2^5 (combos of interfaces) * 256 (values of TOS)
 exit
!
interface GigabitEthernet0/0/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface GigabitEthernet0/1/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface GigabitEthernet0/2/0
 ip flow monitor QOS_MONITOR input
 exit
!

```

The display from the **show flow monitor** command shows the current status of the cache.

```

Router# show flow monitor QOS_MONITOR cache

Cache type:           Normal
Cache size:           8192
Current entries:      2
High Watermark:       2
Flows added:          2
Updates sent          ( 1800 secs) 0

```

Example: Configuring a Customized Flow Record Cache for Monitoring IPv6 Traffic

The following example creates a customized flow record cache for monitoring IPv6 traffic.

This example starts in global configuration mode.

```
!  
ip cef  
ipv6 cef  
!  
flow record FLOW-RECORD-2  
  description Used for basic IPv6 traffic analysis  
  match ipv6 destination address  
  collect counter bytes  
  collect counter packets  
!  
flow monitor FLOW-MONITOR-2  
  description Used for basic IPv6 traffic analysis  
  record FLOW-RECORD-2  
  cache entries 1000  
!  
interface GigabitEthernet0/0/0  
  ipv6 address 2001:DB8:2:ABCD::2/48  
  ipv6 flow monitor FLOW-MONITOR-2 input  
!  
interface GigabitEthernet1/0/0  
  ipv6 address 2001:DB8:3:ABCD::1/48  
  ipv6 flow monitor FLOW-MONITOR-2 output  
!
```

Example: Configuring a Permanent Flow Record Cache with a Limited Number of Flows

The following example is designed to monitor the type of service (ToS) field usage on all interfaces in the router. An exporter is not configured because this example is intended to be used to capture additional data for analysis on the router using the **show flow monitor** command.

This example starts in global configuration mode.

```
!  
ip cef  
!  
flow record QOS_RECORD  
  description UD: Flow Record to monitor the use of TOS within this router/network  
  match interface input  
  match interface output  
  match ipv4 tos  
  collect counter packets  
  collect counter bytes  
  exit  
!  
flow monitor QOS_MONITOR  
  description UD: Flow Monitor which watches the limited combinations of interface and TOS  
  record QOS_RECORD  
  cache type permanent  
  cache entries 8192 ! 2^5 (combos of interfaces) * 256 (values of TOS)  
  exit
```

```

!
interface ethernet0/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface ethernet0/1
 ip flow monitor QOS_MONITOR input
 exit
!
interface ethernet0/2
 ip flow monitor QOS_MONITOR input
 exit
!
interface serial2/0
 ip flow monitor QOS_MONITOR input
 exit
!
interface serial2/1
 ip flow monitor QOS_MONITOR input
!

```

The display from the **show flow monitor** command shows the current status of the cache.

```

Router# show flow monitor QOS_MONITOR cache
Cache type:                Permanent
Cache size:                8192
Current entries:          2
High Watermark:           2
Flows added:               2
Updates sent ( 1800 secs) 0

```

Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

The following example shows how to configure Flexible NetFlow egress accounting for IPv4 and IPv6 traffic.

This example starts in global configuration mode.

```

!
flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow record v6_r1
 match ipv6 traffic-class
 match ipv6 protocol
 match ipv6 source address
 match ipv6 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow monitor FLOW-MONITOR-1

```

```

    record v4_r1
    exit
    !
    !
    flow monitor FLOW-MONITOR-2
    record v6_r1
    exit
    !
    ip cef
    ipv6 cef
    !
    interface GigabitEthernet0/0/0
    ip address 172.16.6.2 255.255.255.0
    ipv6 address 2001:DB8:2:ABCD::2/48
    ip flow monitor FLOW-MONITOR-1 output
    ipv6 flow monitor FLOW-MONITOR-2 output
    !

```

Example: Configuring Flexible NetFlow Subinterface Support

The following example shows how to configure Flexible NetFlow subinterface support for IPv4 traffic.

This example starts in global configuration mode.

```

!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
ip cef
!
interface Ethernet0/0.1
ip address 172.16.6.2 255.255.255.0
ip flow monitor FLOW-MONITOR-1 input
!

```

The following example shows how to configure Flexible NetFlow to emulate NetFlow subinterface support for IPv6 traffic.

This sample starts in global configuration mode:

```

!
flow record v6_r1
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long

```

```

collect timestamp absolute first
collect timestamp absolute last
!
flow monitor FLOW-MONITOR-2
  record v6_r1
  exit
!
ip cef
ipv6 cef
!
interface Ethernet0/0.1
  ipv6 address 2001:DB8:2:ABCD::2/48
  ipv6 flow monitor FLOW-MONITOR-2 input
!

```

Example: Configuring Flexible NetFlow Multiple Export Destinations

The following example shows how to configure Flexible NetFlow multiple export destinations.

This example starts in global configuration mode.

```

!
flow exporter EXPORTER-1
  destination 172.16.10.2
  transport udp 90
  exit
!
flow exporter EXPORTER-2
  destination 172.16.10.3
  transport udp 90
  exit
!
flow monitor FLOW-MONITOR-1
  record netflow-original
  exporter EXPORTER-2
  exporter EXPORTER-1
  exit
!
ip cef
!
interface GigabitEthernet0/0/0
  ip address 172.16.6.2 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 input
!

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 19: Feature Information for Flexible NetFlow

| Feature Name | Releases | Feature Information |
|------------------|---|--|
| Flexible NetFlow | 12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1 Cisco IOS XE Release 3.1S | <p>Flexible NetFlow is introduced.</p> <p>Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.</p> <p>The following commands were introduced or modified: cache (Flexible NetFlow), clear flow exporter, clear flow monitor, clear sampler, collect counter, collect flow, collect interface, collect ipv4, collect ipv4 destination, collect ipv4 fragmentation, collect ipv4 section, collect ipv4 source, collect ipv4 total-length, collect ipv4 ttl, collect routing, collect timestamp sys-uptime, collect transport, collect transport icmp ipv4, collect transport tcp, collect transport udp, debug flow exporter, debug flow monitor, debug flow record, debug sampler, description (Flexible NetFlow), destination, dscp (Flexible NetFlow), exporter, flow exporter, flow monitor, flow platform, flow record, ip flow monitor, match flow, match interface (Flexible NetFlow), match ipv4, match ipv4 destination, match ipv4 fragmentation, match ipv4 section, match ipv4 source, match ipv4 total-length, match ipv4 ttl, match routing, match transport, match transport icmp ipv4, match transport tcp, match transport udp, mode (Flexible NetFlow), option (Flexible NetFlow), record, sampler, show flow exporter, show flow interface, show flow monitor, show flow record, show sampler, source (Flexible NetFlow), statistics packet, template data timeout, transport (Flexible NetFlow).</p> |



CHAPTER 3

Flexible NetFlow—IPv4 Unicast Flows

The Flexible Netflow—IPv4 Unicast Flows feature enables Flexible NetFlow to monitor IPv4 traffic.

- [Finding Feature Information, on page 53](#)
- [Information About Flexible NetFlow IPv4 Unicast Flows, on page 53](#)
- [How to Configure Flexible NetFlow IPv4 Unicast Flows, on page 53](#)
- [Configuration Examples for Flexible NetFlow IPv4 Unicast Flows, on page 64](#)
- [Feature Information for Flexible NetFlow - IPv4 Unicast Flows, on page 66](#)

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.

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

Information About Flexible NetFlow IPv4 Unicast Flows

Flexible NetFlow—IPv4 Unicast Flows Overview

This feature enables Flexible NetFlow to monitor IPv4 traffic.

How to Configure Flexible NetFlow IPv4 Unicast Flows

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} address
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {source | destination} group-tag
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **show running-config flow record** *record-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow record <i>record-name</i> Example: Device(config)# flow record FLOW-RECORD-1 | Creates a flow record and enters Flexible NetFlow flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record. |
| Step 4 | description <i>description</i> Example: Device(config-flow-record)# description Used for basic traffic analysis | (Optional) Creates a description for the flow record. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | <p>match {ip ipv6} {destination source} address</p> <p>Example:</p> <pre>Device(config-flow-record)# match ipv4 destination address</pre> | <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields.</p> |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | <p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag Device(config-flow-record)# match flow cts destination group-tag</pre> | <p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |
| Step 8 | <p>collect interface {input output}</p> <p>Example:</p> <pre>Device(config-flow-record)# collect interface input</pre> | <p>Configures the input interface as a nonkey field for the record.</p> <p>Note This example configures the input interface as a nonkey field for the record.</p> |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | end Example: <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | show flow record <i>record-name</i> Example: <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | show running-config flow record <i>record-name</i> Example: <pre>Device# show running-config flow record FLOW_RECORD-1</pre> | (Optional) Displays the configuration of the specified flow record. |

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**

15. `show flow exporter exporter-name`
16. `show running-config flow exporter exporter-name`

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: <pre>Device> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre>Device# configure terminal</pre> | Enters global configuration mode. |
| Step 3 | flow exporter exporter-name Example: <pre>Device(config)# flow exporter EXPORTER-1</pre> | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow exporter. |
| Step 4 | description description Example: <pre>Device(config-flow-exporter)# description Exports to the datacenter</pre> | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination {ip-address hostname} [vrf vrf-name] Example: <pre>Device(config-flow-exporter)# destination 172.16.10.2</pre> | Specifies the IP address or hostname of the destination system for the exporter. <p>Note You can export to a destination using either an IPv4 or IPv6 address.</p> |
| Step 6 | export-protocol {netflow-v5 netflow-v9 ipfix} Example: <pre>Device(config-flow-exporter)# export-protocol netflow-v9</pre> | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none"> • Default: netflow-v9. |
| Step 7 | dscp dscp Example: <pre>Device(config-flow-exporter)# dscp 63</pre> | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none"> • The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |
| Step 8 | source interface-type interface-number Example: <pre>Device(config-flow-exporter)# source ethernet 0/0</pre> | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 9 | <p>option {exporter-stats interface-table sampler-table vrf-table} [timeout <i>seconds</i>]</p> <p>Example:</p> <pre>Device(config-flow-exporter)# option exporter-stats timeout 120</pre> | <p>(Optional) Configures options data parameters for the exporter.</p> <ul style="list-style-type: none"> You can configure all three options concurrently. The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |
| Step 10 | <p>output-features</p> <p>Example:</p> <pre>Device(config-flow-exporter)# output-features</pre> | <p>(Optional) Enables sending export packets using quality of service (QoS) and encryption.</p> |
| Step 11 | <p>template data timeout <i>seconds</i></p> <p>Example:</p> <pre>Device(config-flow-exporter)# template data timeout 120</pre> | <p>(Optional) Configures resending of templates based on a timeout.</p> <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |
| Step 12 | <p>transport udp <i>udp-port</i></p> <p>Example:</p> <pre>Device(config-flow-exporter)# transport udp 650</pre> | <p>Specifies the UDP port on which the destination system is listening for exported datagrams.</p> <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | <p>ttl <i>seconds</i></p> <p>Example:</p> <pre>Device(config-flow-exporter)# ttl 15</pre> | <p>(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter.</p> <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | <p>end</p> <p>Example:</p> <pre>Device(config-flow-exporter)# end</pre> | <p>Exits flow exporter configuration mode and returns to privileged EXEC mode.</p> |
| Step 15 | <p>show flow exporter <i>exporter-name</i></p> <p>Example:</p> <pre>Device# show flow exporter FLOW_EXPORTER-1</pre> | <p>(Optional) Displays the current status of the specified flow exporter.</p> |
| Step 16 | <p>show running-config flow exporter <i>exporter-name</i></p> <p>Example:</p> <pre>Device# show running-config flow exporter FLOW_EXPORTER-1</pre> | <p>(Optional) Displays the configuration of the specified flow exporter.</p> |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {**timeout** {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: <pre>> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre># configure terminal</pre> | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code>(config)# flow monitor FLOW-MONITOR-1</code> | <ul style="list-style-type: none"> This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: <code>(config-flow-monitor)# description Used for basic ipv4 traffic analysis</code> | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: <code>(config-flow-monitor)# record FLOW-RECORD-1</code> | Specifies the record for the flow monitor. |
| Step 6 | cache { <i>timeout</i> { <i>active</i> } <i>seconds</i> type { normal } Example: | <ul style="list-style-type: none"> type normal—Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: <code>(config-flow-monitor)# exporter EXPORTER-1</code> | (Optional) Specifies the name of an exporter that was created previously. |
| Step 9 | end Example: <code>(config-flow-monitor)# end</code> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[<i>name</i>] <i>monitor-name</i> [cache [format { <i>csv</i> <i>record</i> <i>table</i> }]]] Example: <code># show flow monitor FLOW-MONITOR-2 cache</code> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <code># show running-config flow monitor FLOW_MONITOR-1</code> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 4 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | show flow interface <i>type number</i> Example: Device# show flow interface GigabitEthernet 0/0/0 | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 8 | show flow monitor name <i>monitor-name</i> cache format record Example: Device# show flow monitor name FLOW_MONITOR-1 cache format record | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuring and Enabling Flexible NetFlow with Data Export

You must create a flow monitor to configure the types of traffic for which you want to export the cache data. You must enable the flow monitor by applying it to at least one interface to start exporting data. To configure and enable Flexible NetFlow with data export, perform this required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.



Note You must remove a flow monitor from all of the interfaces to which you have applied it before you can modify the **record** format of the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor *monitor-name***
4. **record {*record-name* | netflow-original | netflow {ipv4 | ipv6 record [*peer*] } }**
5. **exporter *exporter-name***
6. **exit**
7. **interface *type number***
8. **{ip | ipv6} flow monitor *monitor-name* {input | output}**
9. **end**
10. **show flow monitor [[*name*] *monitor-name* [cache [format {csv | record | table}]]][statistics]]**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| | Device# configure terminal | |
| Step 3 | flow monitor <i>monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> This command also allows you to modify an existing flow monitor. |
| Step 4 | record { <i>record-name</i> netflow-original netflow { ipv4 ipv6 <i>record</i> [peer] }} Example: Device(config-flow-monitor)# record netflow ipv4 original-input | Specifies the record for the flow monitor. |
| Step 5 | exporter <i>exporter-name</i> Example: Device(config-flow-monitor)# exporter EXPORTER-1 | Specifies the name of an exporter that you created previously. |
| Step 6 | exit Example: Device(config-flow-monitor)# exit | Exits Flexible NetFlow flow monitor configuration mode and returns to global configuration mode. |
| Step 7 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 8 | { ip ipv6 } flow monitor <i>monitor-name</i> { input output } Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. |
| Step 9 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[name] <i>monitor-name</i> [cache [format { csv record table }]]][statistics]] Example: Device# show flow monitor FLOW-MONITOR-2 cache | (Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. This will verify data export is enabled for the flow monitor cache. |

Configuration Examples for Flexible NetFlow IPv4 Unicast Flows

Example: Configuring Multiple Export Destinations

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv4 or IPv6 traffic.

This sample starts in global configuration mode:

```

!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow exporter EXPORTER-2
 destination 172.16.10.3
 transport udp 90
 exit
!
flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow record v6_r1
 match ipv6 traffic-class
 match ipv6 protocol
 match ipv6 source address
 match ipv6 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!

flow monitor FLOW-MONITOR-1
 record v4_r1
 exporter EXPORTER-2
 exporter EXPORTER-1
!
!
flow monitor FLOW-MONITOR-2
 record v6_r1
 exporter EXPORTER-2
 exporter EXPORTER-1
!
ip cef
!
interface GigabitEthernet1/0/0
 ip address 172.16.6.2 255.255.255.0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ip flow monitor FLOW-MONITOR-1 input

```

```
ipv6 flow monitor FLOW-MONITOR-2 input
!
```

The following display output shows that the flow monitor is exporting data to the two exporters:

```
Device# show flow monitor FLOW-MONITOR-1
Flow Monitor FLOW-MONITOR-1:
  Description:      User defined
  Flow Record:     v4_r1
  Flow Exporter:   EXPORTER-1
                  EXPORTER-2

Cache:
  Type:            normal (Platform cache)
  Status:         allocated
  Size:           4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
  Update Timeout:  1800 secs
```

Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

The following example shows how to configure Flexible NetFlow egress accounting for IPv4 and IPv6 traffic.

This example starts in global configuration mode.

```
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow record v6_r1
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
!
flow monitor FLOW-MONITOR-2
record v6_r1
exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet0/0/0
```

```

ip address 172.16.6.2 255.255.255.0
ipv6 address 2001:DB8:2:ABCD::2/48
ip flow monitor FLOW-MONITOR-1 output
ipv6 flow monitor FLOW-MONITOR-2 output
!

```

Feature Information for Flexible NetFlow - IPv4 Unicast Flows

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 20: Feature Information for Flexible NetFlow - IPv4 Unicast Flows

| Feature Name | Releases | Feature Information |
|---------------------------------------|---|---|
| Flexible NetFlow - IPv4 Unicast Flows | 12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1 Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2SE | Enables Flexible NetFlow to monitor IPv4 traffic. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: collect routing, debug flow record, collect ipv4, collect ipv4 destination, collect ipv4 fragmentation, collect ipv4 section, collect ipv4 source, ip flow monitor, match ipv4, match ipv4 destination, match ipv4 fragmentation, match ipv4 section, match ipv4 source, match routing, record, show flow monitor, show flow record. |



CHAPTER 4

Flexible NetFlow—IPv6 Unicast Flows

The Flexible NetFlow—IPv6 Unicast Flows feature enables Flexible NetFlow to monitor IPv6 traffic.

- [Finding Feature Information, on page 67](#)
- [Information About Flexible NetFlow IPv6 Unicast Flows, on page 67](#)
- [How to Configure Flexible NetFlow IPv6 Unicast Flows, on page 67](#)
- [Configuration Examples for Flexible NetFlow IPv6 Unicast Flows, on page 78](#)
- [Feature Information for Flexible NetFlow - IPv6 Unicast Flows, on page 80](#)

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.

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

Information About Flexible NetFlow IPv6 Unicast Flows

Flexible NetFlow IPv6 Unicast Flows Overview

This feature enables Flexible NetFlow to monitor IPv6 traffic.

How to Configure Flexible NetFlow IPv6 Unicast Flows

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} address
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {source | destination} group-tag
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **show running-config flow record** *record-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow record <i>record-name</i> Example: Device(config)# flow record FLOW-RECORD-1 | Creates a flow record and enters Flexible NetFlow flow record configuration mode. • This command also allows you to modify an existing flow record. |
| Step 4 | description <i>description</i> Example: Device(config-flow-record)# description Used for basic traffic analysis | (Optional) Creates a description for the flow record. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 5 | <p>match {ip ipv6} {destination source} address</p> <p>Example:</p> <pre>Device(config-flow-record)# match ipv4 destination address</pre> | <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields.</p> |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | <p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag Device(config-flow-record)# match flow cts destination group-tag</pre> | <p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |
| Step 8 | <p>collect interface {input output}</p> <p>Example:</p> <pre>Device(config-flow-record)# collect interface input</pre> | <p>Configures the input interface as a nonkey field for the record.</p> <p>Note This example configures the input interface as a nonkey field for the record.</p> |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | end Example: <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | show flow record <i>record-name</i> Example: <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | show running-config flow record <i>record-name</i> Example: <pre>Device# show running-config flow record FLOW_RECORD-1</pre> | (Optional) Displays the configuration of the specified flow record. |

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**

15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: Device(config-flow-exporter)# description Exports to the datacenter | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination { <i>ip-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the IP address or hostname of the destination system for the exporter. <p>Note You can export to a destination using either an IPv4 or IPv6 address.</p> |
| Step 6 | export-protocol { netflow-v5 netflow-v9 ipfix } Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none"> • Default: netflow-v9. |
| Step 7 | dscp <i>dscp</i> Example: Device(config-flow-exporter)# dscp 63 | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none"> • The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |
| Step 8 | source <i>interface-type interface-number</i> Example: Device(config-flow-exporter)# source ethernet 0/0 | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 9 | <p>option {exporter-stats interface-table sampler-table vrf-table} [timeout <i>seconds</i>]</p> <p>Example:</p> <pre>Device(config-flow-exporter)# option exporter-stats timeout 120</pre> | <p>(Optional) Configures options data parameters for the exporter.</p> <ul style="list-style-type: none"> You can configure all three options concurrently. The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |
| Step 10 | <p>output-features</p> <p>Example:</p> <pre>Device(config-flow-exporter)# output-features</pre> | <p>(Optional) Enables sending export packets using quality of service (QoS) and encryption.</p> |
| Step 11 | <p>template data timeout <i>seconds</i></p> <p>Example:</p> <pre>Device(config-flow-exporter)# template data timeout 120</pre> | <p>(Optional) Configures resending of templates based on a timeout.</p> <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |
| Step 12 | <p>transport udp <i>udp-port</i></p> <p>Example:</p> <pre>Device(config-flow-exporter)# transport udp 650</pre> | <p>Specifies the UDP port on which the destination system is listening for exported datagrams.</p> <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | <p>ttl <i>seconds</i></p> <p>Example:</p> <pre>Device(config-flow-exporter)# ttl 15</pre> | <p>(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter.</p> <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | <p>end</p> <p>Example:</p> <pre>Device(config-flow-exporter)# end</pre> | <p>Exits flow exporter configuration mode and returns to privileged EXEC mode.</p> |
| Step 15 | <p>show flow exporter <i>exporter-name</i></p> <p>Example:</p> <pre>Device# show flow exporter FLOW_EXPORTER-1</pre> | <p>(Optional) Displays the current status of the specified flow exporter.</p> |
| Step 16 | <p>show running-config flow exporter <i>exporter-name</i></p> <p>Example:</p> <pre>Device# show running-config flow exporter FLOW_EXPORTER-1</pre> | <p>(Optional) Displays the configuration of the specified flow exporter.</p> |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {**timeout** {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: > enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: # configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code>(config)# flow monitor FLOW-MONITOR-1</code> | <ul style="list-style-type: none"> This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: <code>(config-flow-monitor)# description Used for basic ipv4 traffic analysis</code> | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: <code>(config-flow-monitor)# record FLOW-RECORD-1</code> | Specifies the record for the flow monitor. |
| Step 6 | cache { <i>timeout</i> { <i>active</i> } <i>seconds</i> type { normal } Example: | <ul style="list-style-type: none"> type normal—Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: <code>(config-flow-monitor)# exporter EXPORTER-1</code> | (Optional) Specifies the name of an exporter that was created previously. |
| Step 9 | end Example: <code>(config-flow-monitor)# end</code> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[<i>name</i>] <i>monitor-name</i> [cache [format { <i>csv</i> <i>record</i> <i>table</i> }]]] Example: <code># show flow monitor FLOW-MONITOR-2 cache</code> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <code># show running-config flow monitor FLOW_MONITOR-1</code> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 4 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | show flow interface <i>type number</i> Example: Device# show flow interface GigabitEthernet 0/0/0 | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 8 | show flow monitor name <i>monitor-name</i> cache format record Example: Device# show flow monitor name FLOW_MONITOR-1 cache format record | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuring and Enabling Flexible NetFlow with Data Export

You must create a flow monitor to configure the types of traffic for which you want to export the cache data. You must enable the flow monitor by applying it to at least one interface to start exporting data. To configure and enable Flexible NetFlow with data export, perform this required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.



Note You must remove a flow monitor from all of the interfaces to which you have applied it before you can modify the **record** format of the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor *monitor-name***
4. **record {*record-name* | netflow-original | netflow {ipv4 | ipv6 record [*peer*] } }**
5. **exporter *exporter-name***
6. **exit**
7. **interface *type number***
8. **{ip | ipv6} flow monitor *monitor-name* {input | output}**
9. **end**
10. **show flow monitor [[*name*] *monitor-name* [cache [format {csv | record | table}]]][statistics]]**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| | Device# configure terminal | |
| Step 3 | flow monitor <i>monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor. |
| Step 4 | record { <i>record-name</i> netflow-original netflow { ipv4 ipv6 <i>record</i> [peer] }} Example: Device(config-flow-monitor)# record netflow ipv4 original-input | Specifies the record for the flow monitor. |
| Step 5 | exporter <i>exporter-name</i> Example: Device(config-flow-monitor)# exporter EXPORTER-1 | Specifies the name of an exporter that you created previously. |
| Step 6 | exit Example: Device(config-flow-monitor)# exit | Exits Flexible NetFlow flow monitor configuration mode and returns to global configuration mode. |
| Step 7 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 8 | {ip ipv6} flow monitor <i>monitor-name</i> { input output } Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. |
| Step 9 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[name] <i>monitor-name</i> [cache [format { csv record table }]]][statistics]] Example: Device# show flow monitor FLOW-MONITOR-2 cache | (Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. This will verify data export is enabled for the flow monitor cache. |

Configuration Examples for Flexible NetFlow IPv6 Unicast Flows

Example: Configuring Multiple Export Destinations

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv4 or IPv6 traffic.

This sample starts in global configuration mode:

```

!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow exporter EXPORTER-2
 destination 172.16.10.3
 transport udp 90
 exit
!
flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow record v6_r1
 match ipv6 traffic-class
 match ipv6 protocol
 match ipv6 source address
 match ipv6 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!

flow monitor FLOW-MONITOR-1
 record v4_r1
 exporter EXPORTER-2
 exporter EXPORTER-1
!
!
flow monitor FLOW-MONITOR-2
 record v6_r1
 exporter EXPORTER-2
 exporter EXPORTER-1
!
ip cef
!
interface GigabitEthernet1/0/0
 ip address 172.16.6.2 255.255.255.0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ip flow monitor FLOW-MONITOR-1 input

```

```
ipv6 flow monitor FLOW-MONITOR-2 input
!
```

The following display output shows that the flow monitor is exporting data to the two exporters:

```
Device# show flow monitor FLOW-MONITOR-1
Flow Monitor FLOW-MONITOR-1:
  Description:      User defined
  Flow Record:     v4_r1
  Flow Exporter:   EXPORTER-1
                  EXPORTER-2

Cache:
  Type:            normal (Platform cache)
  Status:         allocated
  Size:           4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
  Update Timeout:  1800 secs
```

Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

The following example shows how to configure Flexible NetFlow egress accounting for IPv4 and IPv6 traffic.

This example starts in global configuration mode.

```
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow record v6_r1
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
record v4_r1
exit
!
!
flow monitor FLOW-MONITOR-2
record v6_r1
exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet0/0/0
```

```

ip address 172.16.6.2 255.255.255.0
ipv6 address 2001:DB8:2:ABCD::2/48
ip flow monitor FLOW-MONITOR-1 output
ipv6 flow monitor FLOW-MONITOR-2 output
!

```

Feature Information for Flexible NetFlow - IPv6 Unicast Flows

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 21: Feature Information for Flexible NetFlow - IPv6 Unicast Flows

| Feature Name | Releases | Feature Information |
|---------------------------------------|----------------------------|--|
| Flexible NetFlow - IPv6 Unicast Flows | 12.2(33)SRE | Enables Flexible NetFlow to monitor IPv6 traffic. |
| | 12.2(50)SY | Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. |
| | 12.4(20)T | |
| | 15.0(1)SY | The following commands were introduced or modified: collect routing , debug flow record , match routing , record , show flow monitor , show flow record , collect ipv6 , collect ipv6 destination , collect ipv6 extension map , collect ipv6 fragmentation , collect ipv6 hop-limit , collect ipv6 length , collect ipv6 section , collect ipv6 source , collect transport icmp ipv6 , ipv6 flow monitor , match ipv6 , match ipv6 destination , match ipv6 extension map , match ipv6 fragmentation , match ipv6 hop-limit , match ipv6 length , match ipv6 section , match ipv6 source , match transport icmp ipv6 . |
| | 15.0(1)SY1 | |
| | Cisco IOS XE Release 3.2SE | |
| Cisco IOS XE Release 3.3S | | |



CHAPTER 5

Flexible NetFlow—MPLS Egress NetFlow

The Flexible NetFlow--MPLS Egress NetFlow feature allows you to capture IP flow information for packets undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS packets and are transmitted as IP packets.

- [Finding Feature Information, on page 81](#)
- [Information About Flexible NetFlow MPLS Egress NetFlow , on page 81](#)
- [How to Configure Flexible NetFlow MPLS Egress NetFlow , on page 83](#)
- [Configuration Examples for Flexible NetFlow MPLS Egress NetFlow , on page 88](#)
- [Additional References, on page 89](#)
- [Feature Information for Flexible NetFlow - MPLS Egress NetFlow , on page 90](#)

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.

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

Information About Flexible NetFlow MPLS Egress NetFlow

Flexible NetFlow MPLS Egress NetFlow

The Flexible NetFlow - MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN. The Flexible NetFlow - MPLS Egress NetFlow feature is enabled by applying a flow monitor in output (egress) mode on the provider edge (PE) to customer edge (CE) interface of the provider's network.

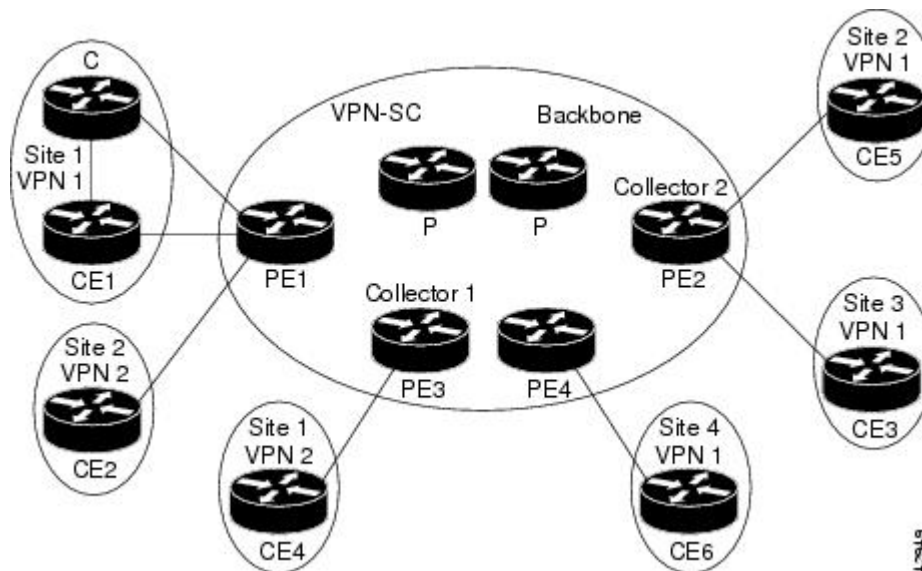
The figure below shows a sample MPLS VPN network topology that includes four VPN 1 sites and two VPN 2 sites. If the Flexible NetFlow - MPLS Egress NetFlow is enabled on an outgoing PE interface by applying

a flow monitor in output mode, IP flow information for packets that arrive at the PE as MPLS packets (from an MPLS VPN) and that are transmitted as IP packets to the PE router is captured. For example:

- To capture the flow of traffic going to site 2 of VPN 1 from any remote VPN 1 sites, you enable a flow monitor in output mode on link PE2-CE5 of provider edge router PE2.
- To capture the flow of traffic going to site 1 of VPN 2 from any remote VPN 2 site, you enable a flow monitor in output mode on link PE3-CE4 of the provider edge router PE3.

The flow data is stored in the Flexible NetFlow cache. You can use the **show flow monitor** *monitor-name* *cache* command to display the flow data in the cache.

Figure 7: Sample MPLS VPN Network Topology with Flexible NetFlow--MPLS Egress NetFlow Feature



If you configure a Flexible NetFlow exporter for the flow monitors you use for the Flexible NetFlow - MPLS Egress NetFlow feature, the PE routers will export the captured flows to the configured collector devices in the provider network. Applications such as the Network Data Analyzer or the VPN Solution Center (VPN-SC) can gather information from the captured flows and compute and display site-to-site VPN traffic statistics.

Limitations

When using Flexible NetFlow to monitor outbound traffic on a router at the edge of an MPLS cloud, for IP traffic that leaves over a VRF, the following fields are not collected and have a value of 0:

- destination mask
- destination prefix
- destination AS numbers
- destination BGP traffic index
- nexthop
- BGP nexthop

How to Configure Flexible NetFlow MPLS Egress NetFlow

Configuring a Flow Exporter for the Flow Monitor

Perform this optional task to configure a flow exporter for the flow monitor in order to export the data that is collected by Flexible NetFlow to a remote system for further analysis and storage.

Flow exporters are used to send the data that you collect with Flexible NetFlow to a remote system such as a NetFlow Collection Engine. Exporters use UDP as the transport protocol and use the Version 9 export format.



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 either an IPv4 or IPv6 address.



Note When you configure an exporter, configure the exporter in such a way that the source interface is defined as a WAN interface. This configuration helps you prevent any unpredictable behavior because the NAT is not applied on the packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **transport udp** *udp-port*
8. **exit**
9. **flow monitor** *flow-monitor-name*
10. **exporter** *exporter-name*
11. **end**
12. **show flow exporter** *exporter-name*
13. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|----------------|---|---|
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates a flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: Device(config-flow-exporter)# description Exports to datacenter | (Optional) Creates a description for the flow exporter. |
| Step 5 | destination { <i>hostname</i> <i>ip-address</i> } [vrf <i>vrf-name</i>] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the hostname or IP address of the system to which the exporter sends data. Note You can export to a destination using either an IPv4 or IPv6 address. |
| Step 6 | export-protocol { netflow-v5 netflow-v9 ipfix } Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. <ul style="list-style-type: none"> Default: netflow-v9. |
| Step 7 | transport udp <i>udp-port</i> Example: Device(config-flow-exporter)# transport udp 65 | Configures UDP as the transport protocol and specifies the UDP port on which the destination system is listening for exported Flexible NetFlow traffic. |
| Step 8 | exit Example: Device(config-flow-exporter)# exit | Exits Flexible NetFlow flow exporter configuration mode and returns to global configuration mode. |
| Step 9 | flow monitor <i>flow-monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Enters Flexible NetFlow flow monitor configuration mode for the flow monitor that you created previously. |
| Step 10 | exporter <i>exporter-name</i> Example: | Specifies the name of an exporter that you created previously. |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code>Device(config-flow-monitor)# exporter EXPORTER-1</code> | |
| Step 11 | end Example: <code>Device(config-flow-monitor)# end</code> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 12 | show flow exporter <i>exporter-name</i> Example: <code>Device# show flow exporter FLOW_EXPORTER-1</code> | (Optional) Displays the current status of the specified flow exporter. |
| Step 13 | show running-config flow exporter <i>exporter-name</i> Example: <code>Device<# show running-config flow exporter FLOW_EXPORTER-1</code> | (Optional) Displays the configuration of the specified flow exporter. |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {*timeout* {**active**} *seconds* | **type** { **normal** } }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.

8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: > enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: # configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: (config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: (config-flow-monitor)# description Used for basic ipv4 traffic analysis | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: (config-flow-monitor)# record FLOW-RECORD-1 | Specifies the record for the flow monitor. |
| Step 6 | cache { <i>timeout</i> { <i>active</i> } <i>seconds</i> type { normal } Example: | • type normal —Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: (config-flow-monitor)# exporter EXPORTER-1 | (Optional) Specifies the name of an exporter that was created previously. |
| Step 9 | end Example: | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| | <code>(config-flow-monitor)# end</code> | |
| Step 10 | show flow monitor <i>[[name] monitor-name [cache [format {csv record table}]]]</i> Example: <code># show flow monitor FLOW-MONITOR-2 cache</code> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <code># show running-config flow monitor FLOW_MONITOR-1</code> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name {input | output}*
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name cache format record*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: <code>Device> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <code>Device# configure terminal</code> | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: | Specifies an interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device(config)# interface GigabitEthernet 0/0/0 | |
| Step 4 | <p>{ip ipv6} flow monitor <i>monitor-name</i> {input output}</p> <p>Example:</p> <pre>Device(config-if)# ip flow monitor FLOW-MONITOR-1 input</pre> | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | <p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | <p>show flow interface <i>type number</i></p> <p>Example:</p> <pre>Device# show flow interface GigabitEthernet 0/0/0</pre> | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |
| Step 8 | <p>show flow monitor name <i>monitor-name</i> cache format record</p> <p>Example:</p> <pre>Device# show flow monitor name FLOW_MONITOR-1 cache format record</pre> | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuration Examples for Flexible NetFlow MPLS Egress NetFlow

Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

The following example shows how to configure Flexible NetFlow egress accounting for IPv4 and IPv6 traffic. This example starts in global configuration mode.

```
!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
```

```

match transport destination-port
collect counter bytes long
collect counter packets long
!
flow record v6_r1
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
  record v4_r1
  exit
!
!
flow monitor FLOW-MONITOR-2
  record v6_r1
  exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet0/0/0
 ip address 172.16.6.2 255.255.255.0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ip flow monitor FLOW-MONITOR-1 output
 ipv6 flow monitor FLOW-MONITOR-2 output
!

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow - MPLS Egress NetFlow

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 22: Feature Information for Flexible NetFlow - MPLS Egress NetFlow

| Feature Name | Releases | Feature Information |
|--|--|---|
| Flexible NetFlow - MPLS Egress NetFlow | 12.2(33)SRE 12.2(50)SY 12.4(22)T 15.0(1)SY 15.0(1)SY1 Cisco IOS XE Release 3.1S | The Flexible NetFlow--MPLS Egress NetFlow feature allows you to capture IP flow information for packets undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS packets and are transmitted as IP packets. Support for this feature was added for Cisco 7200 and 7300 NPE series routers in Cisco IOS Release 12.2(33)SRE. No commands were introduced or modified by this feature. |



CHAPTER 6

Flexible NetFlow v9 Export Format

This feature enables sending export packets using the Version 9 export format.

- [Finding Feature Information, on page 91](#)
- [Prerequisites for Flexible NetFlow v9 Export Format, on page 91](#)
- [Information About Flexible NetFlow v9 Export Format, on page 91](#)
- [How to Configure Flexible NetFlow v9 Export Format, on page 92](#)
- [Configuration Examples for Flexible NetFlow v9 Export Format, on page 95](#)
- [Additional Reference for Flexible NetFlow v9 Export Format, on page 95](#)
- [Feature Information for Flexible NetFlow - NetFlow v9 Export Format, on page 97](#)

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.

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

Prerequisites for Flexible NetFlow v9 Export Format

- The networking device must be running a Cisco release that supports Flexible NetFlow.

Information About Flexible NetFlow v9 Export Format

Flow Exporters

Flow exporters are created as separate components in a router's configuration. Exporters are assigned to flow monitors to export the data from the flow monitor cache to a remote system such as a NetFlow collector. Flow monitors can support more than one exporter. Each exporter can be customized to meet the requirements of

the flow monitor or monitors in which it is used and the NetFlow collector systems to which it is exporting data.

Benefits of Flexible NetFlow Flow Exporters

Flexible NetFlow allows you to configure many different flow exporters, depending on your requirements. Some of the benefits of Flexible NetFlow flow exporters are as follows:

- Using flow exporters, you can create an exporter for every type of traffic that you want to analyze so that you can send each type of traffic to a different NetFlow collector. Original NetFlow sends the data in a cache for all of the analyzed traffic to a maximum of two export destinations.
- Flow exporters support up to ten exporters per flow monitor. Original NetFlow is limited to only two export destinations per cache.
- Flow exporters can use both TCP and UDP for export.
- Depending on your release, flow exporters can use class of service (CoS) in the packets that are sent to export destinations to help ensure that the packets are given the correct priority throughout the network. Original NetFlow exporters do not use CoS in the packets that are sent to export destinations.
- Depending on your release, flow exporter traffic can be encrypted.

How to Configure Flexible NetFlow v9 Export Format

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**

11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**
15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: Device(config-flow-exporter)# description Exports to the datacenter | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination { <i>ip-address</i> <i>hostname</i> } [<i>vrf vrf-name</i>] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the IP address or hostname of the destination system for the exporter. <p>Note You can export to a destination using either an IPv4 or IPv6 address.</p> |
| Step 6 | export-protocol { <i>netflow-v5</i> <i>netflow-v9</i> <i>ipfix</i> } Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none"> • Default: netflow-v9. |
| Step 7 | dscp <i>dscp</i> Example: Device(config-flow-exporter)# dscp 63 | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none"> • The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 8 | source <i>interface-type interface-number</i> Example: Device(config-flow-exporter)# source ethernet 0/0 | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |
| Step 9 | option { exporter-stats interface-table sampler-table vrf-table } [timeout <i>seconds</i>] Example: Device(config-flow-exporter)# option exporter-stats timeout 120 | (Optional) Configures options data parameters for the exporter. <ul style="list-style-type: none"> You can configure all three options concurrently. The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |
| Step 10 | output-features Example: Device(config-flow-exporter)# output-features | (Optional) Enables sending export packets using quality of service (QoS) and encryption. |
| Step 11 | template data timeout <i>seconds</i> Example: Device(config-flow-exporter)# template data timeout 120 | (Optional) Configures resending of templates based on a timeout. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |
| Step 12 | transport udp <i>udp-port</i> Example: Device(config-flow-exporter)# transport udp 650 | Specifies the UDP port on which the destination system is listening for exported datagrams. <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | ttl <i>seconds</i> Example: Device(config-flow-exporter)# ttl 15 | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | end Example: Device(config-flow-exporter)# end | Exits flow exporter configuration mode and returns to privileged EXEC mode. |
| Step 15 | show flow exporter <i>exporter-name</i> Example: Device# show flow exporter FLOW_EXPORTER-1 | (Optional) Displays the current status of the specified flow exporter. |
| Step 16 | show running-config flow exporter <i>exporter-name</i> Example: | (Optional) Displays the configuration of the specified flow exporter. |

| | Command or Action | Purpose |
|--|---|---------|
| | Device# show running-config flow exporter FLOW_EXPORTER-1 | |

Configuration Examples for Flexible NetFlow v9 Export Format

Example: Configuring NetFlow v9 Export Format

The following example shows how to configure version 9 export for Flexible NetFlow.

This example starts in global configuration mode.

```

!
flow exporter EXPORTER-1
 destination 172.16.10.2
 export-protocol netflow-v9
 transport udp 90
 exit
!
flow record v4_r1
 match ipv4 tos
 match ipv4 protocol
 match ipv4 source address
 match ipv4 destination address
 match transport source-port
 match transport destination-port
 collect counter bytes long
 collect counter packets long
!
flow monitor FLOW-MONITOR-1
 record v4_r1
 exporter EXPORTER-1
!
ip cef
!
interface GigabitEthernet 0/0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!

```

Additional Reference for Flexible NetFlow v9 Export Format

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | Flexible NetFlow Configuration Guide |

| Related Topic | Document Title |
|---------------------------|---|
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards

| Standard | Title |
|----------|-------|
| None | — |

MIBs

| MIB | MIBs Link |
|------|--|
| None | 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 |

RFCs

| RFC | Title |
|----------|--|
| RFC 3954 | <i>Cisco Systems NetFlow Services Export Version 9</i> |

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/cisco/web/support/index.html |

Feature Information for Flexible NetFlow - NetFlow v9 Export Format

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 23: Feature Information for Flexible NetFlow - NetFlow v9 Export Format

| Feature Name | Releases | Feature Information |
|---|---|---|
| Flexible NetFlow - NetFlow v9 Export Format | 12.2(33)SRE 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1 Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2SE | This feature enables sending export packets using the Version 9 export format. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: export-protocol . |



CHAPTER 7

Flexible NetFlow Output Features on Data Export

This feature enables sending export packets using Quality of Service (QoS) and encryption.

- [Finding Feature Information, on page 99](#)
- [Prerequisites for Flexible NetFlow Output Features on Data Export , on page 99](#)
- [Information About Flexible NetFlow Output Features on Data Export, on page 100](#)
- [How to Configure Flexible NetFlow Output Features on Data Export , on page 101](#)
- [Configuration Examples for Flexible NetFlow Output Features on Data Export , on page 107](#)
- [Additional References, on page 108](#)
- [Feature Information for Flexible NetFlow—Output Features on Data Export, on page 109](#)

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.

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

Prerequisites for Flexible NetFlow Output Features on Data Export

- The networking device must be running a Cisco release that supports Flexible NetFlow.

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.

Information About Flexible NetFlow Output Features on Data Export

Flow Exporters

Flow exporters are created as separate components in a router's configuration. Exporters are assigned to flow monitors to export the data from the flow monitor cache to a remote system such as a NetFlow collector. Flow monitors can support more than one exporter. Each exporter can be customized to meet the requirements of the flow monitor or monitors in which it is used and the NetFlow collector systems to which it is exporting data.

Benefits of Flexible NetFlow Flow Exporters

Flexible NetFlow allows you to configure many different flow exporters, depending on your requirements. Some of the benefits of Flexible NetFlow flow exporters are as follows:

- Using flow exporters, you can create an exporter for every type of traffic that you want to analyze so that you can send each type of traffic to a different NetFlow collector. Original NetFlow sends the data in a cache for all of the analyzed traffic to a maximum of two export destinations.
- Flow exporters support up to ten exporters per flow monitor. Original NetFlow is limited to only two export destinations per cache.
- Flow exporters can use both TCP and UDP for export.
- Depending on your release, flow exporters can use class of service (CoS) in the packets that are sent to export destinations to help ensure that the packets are given the correct priority throughout the network. Original NetFlow exporters do not use CoS in the packets that are sent to export destinations.
- Depending on your release, flow exporter traffic can be encrypted.

How to Configure Flexible NetFlow Output Features on Data Export

Restrictions

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. Flow exporters are added to flow monitors to enable data export from the flow monitor cache.



Note Only the keywords and arguments required for the Flexible NetFlow commands used in these tasks are explained in these tasks. For information about the other keywords and arguments available for these Flexible NetFlow commands, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**
15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none">• This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: Device(config-flow-exporter)# description Exports to the datacenter | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination {<i>ip-address</i> <i>hostname</i>} [vrf <i>vrf-name</i>] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the IP address or hostname of the destination system for the exporter. Note You can export to a destination using either an IPv4 or IPv6 address. |
| Step 6 | export-protocol {netflow-v5 netflow-v9 ipfix} Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none">• Default: netflow-v9. |
| Step 7 | dscp <i>dscp</i> Example: Device(config-flow-exporter)# dscp 63 | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none">• The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |
| Step 8 | source <i>interface-type interface-number</i> Example: Device(config-flow-exporter)# source ethernet 0/0 | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |
| Step 9 | option {exporter-stats interface-table sampler-table vrf-table} [timeout <i>seconds</i>] | (Optional) Configures options data parameters for the exporter. |

| | Command or Action | Purpose |
|----------------|---|--|
| | Example: <pre>Device(config-flow-exporter)# option exporter-stats timeout 120</pre> | <ul style="list-style-type: none"> You can configure all three options concurrently. The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |
| Step 10 | output-features Example: <pre>Device(config-flow-exporter)# output-features</pre> | (Optional) Enables sending export packets using quality of service (QoS) and encryption. |
| Step 11 | template data timeout seconds Example: <pre>Device(config-flow-exporter)# template data timeout 120</pre> | (Optional) Configures resending of templates based on a timeout. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |
| Step 12 | transport udp udp-port Example: <pre>Device(config-flow-exporter)# transport udp 650</pre> | Specifies the UDP port on which the destination system is listening for exported datagrams. <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | ttl seconds Example: <pre>Device(config-flow-exporter)# ttl 15</pre> | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | end Example: <pre>Device(config-flow-exporter)# end</pre> | Exits flow exporter configuration mode and returns to privileged EXEC mode. |
| Step 15 | show flow exporter exporter-name Example: <pre>Device# show flow exporter FLOW_EXPORTER-1</pre> | (Optional) Displays the current status of the specified flow exporter. |
| Step 16 | show running-config flow exporter exporter-name Example: <pre>Device# show running-config flow exporter FLOW_EXPORTER-1</pre> | (Optional) Displays the configuration of the specified flow exporter. |

Displaying the Current Status of a Flow Exporter

To display the current status of a flow exporter, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show flow exporter** [export-ids {netflow-v5| netflow-v9} | [name] *exporter-name* [statistics | templates]]

DETAILED STEPS

Step 1 enable

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 show flow exporter [export-ids {netflow-v5| netflow-v9} | [name] *exporter-name* [statistics | templates]]

The **show flow exporter** command shows the current status of the flow exporter that you specify.

Example:

```
Device# show flow exporter EXPORTER-1
Flow Exporter EXPORTER-1:
  Description:           Exports to the datacenter
  Export protocol:       NetFlow Version 9
  Transport Configuration:
    Destination IP address: 172.16.10.2
    Source IP address:     172.16.6.2
    Source Interface:      GigabitEthernet1/0/0
    Transport Protocol:    UDP
    Destination Port:      650
    Source Port:           55864
    DSCP:                  0x3F
    TTL:                   15
    Output Features:       Used
  Options Configuration:
    exporter-stats (timeout 120 seconds)
    interface-table (timeout 120 seconds)
    sampler-table (timeout 120 seconds)
```

Verifying the Flow Exporter Configuration

To verify the configuration commands that you entered, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 **show running-config flow exporter *exporter-name***

The **show running-config flow exporter** command shows the configuration commands of the flow exporter that you specify.

Example:

```
Device# show running-config flow exporter EXPORTER-1
Building configuration...
Current configuration:
!
flow exporter EXPORTER-1
  description Exports to the datacenter
  destination 172.16.10.2
  source GigabitEthernet1/0/0
  dscp 63
  ttl 15
  transport udp 650
  template data timeout 120
  option exporter-stats timeout 120
  option interface-table timeout 120
  option sampler-table timeout 120
!
end
```

Configuring and Enabling Flexible NetFlow with Data Export

You must create a flow monitor to configure the types of traffic for which you want to export the cache data. You must enable the flow monitor by applying it to at least one interface to start exporting data. To configure and enable Flexible NetFlow with data export, perform this required task.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.



Note You must remove a flow monitor from all of the interfaces to which you have applied it before you can modify the **record** format of the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6** *record* [**peer**] }}
5. **exporter** *exporter-name*
6. **exit**
7. **interface** *type number*
8. {**ip** | **ipv6**} **flow monitor** *monitor-name* {**input** | **output**}
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]]

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor. |
| Step 4 | record { <i>record-name</i> netflow-original netflow { ipv4 ipv6 <i>record</i> [peer] }} Example: Device(config-flow-monitor)# record netflow ipv4 original-input | Specifies the record for the flow monitor. |
| Step 5 | exporter <i>exporter-name</i> Example: Device(config-flow-monitor)# exporter EXPORTER-1 | Specifies the name of an exporter that you created previously. |
| Step 6 | exit Example: Device(config-flow-monitor)# exit | Exits Flexible NetFlow flow monitor configuration mode and returns to global configuration mode. |

| | Command or Action | Purpose |
|---------|---|--|
| Step 7 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 8 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. |
| Step 9 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[name] monitor-name [cache [format {csv record table}]]][statistics]] Example: Device# show flow monitor FLOW-MONITOR-2 cache | (Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. This will verify data export is enabled for the flow monitor cache. |

Configuration Examples for Flexible NetFlow Output Features on Data Export

Example: Configuring Sending Export Packets Using QoS

The following example shows how to enable QoS on Flexible Netflow export packets.



Note The Flexible NetFlow export packets are transmitted using QoS on Ethernet interface 0/1 (the interface on which the destination is reachable) to the destination host (IP address 10.0.1.2).

This sample starts in global configuration mode:

```

!
flow record FLOW-RECORD-1
  match ipv4 source address
  collect counter packets
!
flow exporter FLOW-EXPORTER-1
  destination 10.0.1.2
  output-features
  dscp 18
!

```

```

flow monitor FLOW-MONITOR-1
  record FLOW-RECORD-1
  exporter FLOW-EXPORTER-1
  cache entries 1024
!
ip cef
!
class-map match-any COS3
!
policy-map PH_LABS_FRL_64k_16k_16k_8k_8k
  class COS3
    bandwidth percent 2
    random-detect dscp-based
    random-detect exponential-weighting-constant 1
    random-detect dscp 18 200 300 10
!
interface Ethernet 0/0
  ip address 10.0.0.1 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 input
!
interface Ethernet 0/1
  ip address 10.0.1.1 255.255.255.0
  service-policy output PH_LABS_FRL_64k_16k_16k_8k_8k
!

```

The following display output shows that the flow monitor is exporting data using output feature support that enables the exported data to use QoS:

```

Device# show flow monitor FLOW-MONITOR-1
Flow Exporter FLOW-EXPORTER-1:
  Description:          User defined
  Transport Configuration:
    Destination IP address: 10.0.1.2
    Source IP address:     10.0.0.1
    Transport Protocol:    UDP
    Destination Port:      9995
    Source Port:           56750
    DSCP:                  0x12
    TTL:                   255
    Output Features:       Used

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow—Output Features on Data Export

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 24: Feature Information for Flexible NetFlow—Output Features on Data Export

| Feature Name | Releases | Feature Information |
|---|--|---|
| Flexible NetFlow—Output Features on Data Export | 12.4(20)T Cisco IOS XE Release 3.1S | Enables sending export packets using QoS and encryption. The following command was introduced: output-features . |



CHAPTER 8

Flexible NetFlow NetFlow V5 Export Protocol

The Flexible Netflow NetFlow V5 Export Protocol feature enables sending export packets using the Version 5 export protocol.

Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE.

- [Finding Feature Information, on page 111](#)
- [Restrictions for Flexible NetFlow NetFlow V5 Export Protocol, on page 111](#)
- [Information about Flexible NetFlow NetFlow V5 Export Protocol, on page 112](#)
- [How to Configure Flexible NetFlow NetFlow V5 Export Protocol, on page 112](#)
- [Configuration Examples for Flexible NetFlow NetFlow V5 Export Protocol, on page 114](#)
- [Additional References, on page 115](#)
- [Feature Information for Flexible NetFlow NetFlow V5 Export Protocol, on page 116](#)

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.

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

Restrictions for Flexible NetFlow NetFlow V5 Export Protocol

- The NetFlow Version 5 export protocol that was first shipped in Cisco IOS Release 12.4(22)T is supported for flow monitors that use only the following Flexible NetFlow predefined records: netflow-original, original input, and original output.

Information about Flexible NetFlow NetFlow V5 Export Protocol

Flexible NetFlow V5 Export Protocol Overview

This feature enables sending export packets using the Version 5 export protocol.

How to Configure Flexible NetFlow NetFlow V5 Export Protocol

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**
15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--------------------------------------|---|
| Step 1 | enable Example: | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------------|--|--|
| | Device> enable | |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter exporter-name Example: Device(config)# flow exporter EXPORTER-1 | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow exporter. |
| Step 4 | description description Example: Device(config-flow-exporter)# description Exports to the datacenter | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination {ip-address hostname} [vrf vrf-name] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the IP address or hostname of the destination system for the exporter. Note You can export to a destination using either an IPv4 or IPv6 address. |
| Step 6 | export-protocol {netflow-v5 netflow-v9 ipfix} Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none"> • Default: netflow-v9. |
| Step 7 | dscp dscp Example: Device(config-flow-exporter)# dscp 63 | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none"> • The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |
| Step 8 | source interface-type interface-number Example: Device(config-flow-exporter)# source ethernet 0/0 | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |
| Step 9 | option {exporter-stats interface-table sampler-table vrf-table} [timeout seconds] Example: Device(config-flow-exporter)# option exporter-stats timeout 120 | (Optional) Configures options data parameters for the exporter. <ul style="list-style-type: none"> • You can configure all three options concurrently. • The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 10 | output-features Example: Device(config-flow-exporter)# output-features | (Optional) Enables sending export packets using quality of service (QoS) and encryption. |
| Step 11 | template data timeout seconds Example: Device(config-flow-exporter)# template data timeout 120 | (Optional) Configures resending of templates based on a timeout. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |
| Step 12 | transport udp udp-port Example: Device(config-flow-exporter)# transport udp 650 | Specifies the UDP port on which the destination system is listening for exported datagrams. <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | ttl seconds Example: Device(config-flow-exporter)# ttl 15 | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | end Example: Device(config-flow-exporter)# end | Exits flow exporter configuration mode and returns to privileged EXEC mode. |
| Step 15 | show flow exporter exporter-name Example: Device# show flow exporter FLOW_EXPORTER-1 | (Optional) Displays the current status of the specified flow exporter. |
| Step 16 | show running-config flow exporter exporter-name Example: Device# show running-config flow exporter FLOW_EXPORTER-1 | (Optional) Displays the configuration of the specified flow exporter. |

Configuration Examples for Flexible NetFlow NetFlow V5 Export Protocol

Example: Configuring Version 5 Export

The following example shows how to configure version 5 export for Flexible NetFlow.

This sample starts in global configuration mode:

```

!
flow exporter EXPORTER-1
 destination 172.16.10.2
 export-protocol netflow-v5
 transport udp 90
 exit
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exporter EXPORTER-1
!
ip cef
!
interface Ethernet 0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow NetFlow V5 Export Protocol

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 25: Feature Information for Flexible NetFlow NetFlow V5 Export Protocol

| Feature Name | Releases | Feature Information |
|--|--|--|
| Flexible NetFlow--NetFlow V5 Export Protocol | 12.2(33)SRE 12.2(50)SY 12.4(22)T 15.0(1)SY 15.0(1)SY1 Cisco IOS XE Release 3.1S | Enables sending export packets using the Version 5 export protocol. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following command was introduced: export-protocol. |



CHAPTER 9

Using Flexible NetFlow Flow Sampling

This document contains information about and instructions for configuring sampling to reduce the CPU overhead of analyzing traffic with Flexible NetFlow.

NetFlow is a Cisco technology that provides statistics on packets flowing through a router. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides data to support 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.

- [Finding Feature Information, on page 117](#)
- [Prerequisites for Using Flexible NetFlow Flow Sampling, on page 117](#)
- [Restrictions for Using Flexible NetFlow Flow Sampling, on page 118](#)
- [Information About Flexible NetFlow Flow Sampling, on page 118](#)
- [How to Configure Flexible NetFlow Flow Sampling, on page 118](#)
- [Configuration Examples for Flexible NetFlow Flow Sampling, on page 122](#)
- [Additional References, on page 124](#)
- [Feature Information for Flexible NetFlow Flow Sampling, on page 124](#)

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.

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

Prerequisites for Using Flexible NetFlow Flow Sampling

- The networking device must be running a Cisco release that supports Flexible NetFlow.

Restrictions for Using Flexible NetFlow Flow Sampling

Information About Flexible NetFlow Flow Sampling

Flow Samplers

Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running by limiting the number of packets that are selected for analysis.

Flow sampling exchanges monitoring accuracy for router performance. When you apply a sampler to a flow monitor, the overhead load on the router of running the flow monitor is reduced because the number of packets that the flow monitor must analyze is reduced. The reduction in the number of packets that are analyzed by the flow monitor causes a corresponding reduction in the accuracy of the information stored in the flow monitor's cache.

Samplers are combined with flow monitors when they are applied to an interface with the **ip flow monitor** command.

How to Configure Flexible NetFlow Flow Sampling

Flow sampling reduces the CPU overhead of analyzing traffic with Flexible NetFlow by reducing the number of packets that are analyzed.



Note Only the keywords and arguments required for the Flexible NetFlow commands used in these tasks are explained in these tasks. For information about the other keywords and arguments available for these Flexible NetFlow commands, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Configuring a Flow Monitor

Samplers are applied to an interface in conjunction with a flow monitor. You must create a flow monitor to configure the types of traffic that you want to analyze before you can enable sampling. Perform this required task to configure a flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. The record format can be one of the predefined record formats, or an advanced user may create his or her own record format using the **collect** and **match** commands in Flexible NetFlow flow record configuration mode.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: Device(config-flow-monitor)# description Used for basic traffic analysis | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> netflow-original netflow { ipv4 ipv6 } <i>record</i> [peer]} | Specifies the record for the flow monitor. |
| Step 6 | end Example: Device(config-flow-monitor)# end | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |

Perform this required task to configure and enable a flow sampler.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sampler** *sampler-name*
4. **description** *description*
5. **mode** {random} 1 out-of *window-size*
6. **exit**
7. **interface** *type number*
8. {ip | ipv6} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**}
9. **end**
10. **show sampler** *sampler-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | sampler <i>sampler-name</i> Example: Device(config)# sampler SAMPLER-1 | Creates a sampler and enters sampler configuration mode. • This command also allows you to modify an existing sampler. |
| Step 4 | description <i>description</i> Example: Device(config-sampler)# description Sample at 50% | (Optional) Creates a description for the flow sampler. |
| Step 5 | mode {random} 1 out-of <i>window-size</i> Example: Device(config-sampler)# mode random 1 out-of 2 | Specifies the sampler mode and the flow sampler window size. • The range for the <i>window-size</i> argument is from . |
| Step 6 | exit Example: Device(config-sampler)# exit | Exits sampler configuration mode and returns to global configuration mode. |
| Step 7 | interface <i>type number</i> Example: | Specifies an interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|----------------|--|---|
| | Device(config)# interface GigabitEthernet 0/0/0 | |
| Step 8 | <p>{ip ipv6} flow monitor <i>monitor-name</i> [[sampler] <i>sampler-name</i>] {input output}</p> <p>Example:</p> <pre>Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input</pre> | Assigns the flow monitor and the flow sampler that you created to the interface to enable sampling. |
| Step 9 | <p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 10 | <p>show sampler <i>sampler-name</i></p> <p>Example:</p> <pre>Device# show sampler SAMPLER-1</pre> | Displays the status and statistics of the flow sampler that you configured and enabled. |

Displaying the Status and Statistics of the Flow Sampler Configuration

To display the status and statistics of the flow sampler that you configured and enabled, perform the following optional task.

SUMMARY STEPS

1. **enable**
2. **show sampler *sampler-name***

DETAILED STEPS

Step 1 **enable**

The **enable** command enters privileged EXEC mode (enter the password if prompted).

Example:

```
Device> enable
Device#
```

Step 2 **show sampler *sampler-name***

The **show sampler** command shows the current status of the sampler that you specify.

Example:

```
Device# show sampler SAMPLER-1
Sampler SAMPLER-1:
ID:                2
```

```

Description:    Sample at 50%
Type:          random
Rate:         1 out of 2
Samples:      2482
Requests:     4964
Users (1):
  flow monitor FLOW-MONITOR-1 (ip,Et0/0,I  2482 out of 4964

```

Configuration Examples for Flexible NetFlow Flow Sampling

Example: Configuring and Enabling a Random Sampler for IPv4 Traffic

The following example shows how to configure and enable random sampling for IPv4 output traffic.

This example starts in global configuration mode.

```

!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!
flow monitor FLOW-MONITOR-1
  record v4_r1
  exit
!
sampler SAMPLER-1
  mode random 1 out-of 2
  exit
!
ip cef
!
interface GigabitEthernet 0/0/0
  ip address 172.16.6.2 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 output
!

```

The following example shows how to configure and enable random sampling for IPv4 input traffic.

This example starts in global configuration mode.

```

!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long

```

```

!
flow monitor FLOW-MONITOR-1
  record v4_r1
  exit
!
sampler SAMPLER-1
  mode random 1 out-of 2
  exit
!
ip cef
!
interface GigabitEthernet 0/0/0
  ip address 172.16.6.2 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
!

```

Example: Adding a Sampler to a Flow Monitor When a Flow Monitor Is Already Enabled

The following example shows what happens when you try to add a sampler to a flow monitor that has already been enabled on an interface without a sampler:

```

Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.

```

The following example shows how to remove the flow monitor from the interface so that it can be enabled with the sampler:

```

Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input

```

Example: Removing a Sampler from a Flow Monitor

The following example shows what happens when you try to remove a sampler from a flow monitor on an interface by entering the **ip flow monitor** command again without the sampler keyword and argument:

```

Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.

```

The following example shows how to remove the flow monitor that was enabled with a sampler from the interface so that it can be enabled without the sampler:

```

Device(config)# interface GigabitEthernet 0/0/0
Device(config-if)# no ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
Device(config-if)# ip flow monitor FLOW-MONITOR-1 input

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow Flow Sampling

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 26: Feature Information for Flexible Netflow Flow Sampling

| Feature Name | Releases | Feature Information |
|------------------------------------|--|--|
| Flexible Netflow - Random Sampling | 12.2(50)SY 12.4(20)T Cisco IOS XE Release 3.1S Cisco IOS XE Release 3.2SE | Flow samplers are created as separate components in a router's configuration. Flow samplers are used to reduce the load on the device that is running Flexible NetFlow by limiting the number of packets that are selected for analysis. Samplers use either random or deterministic sampling techniques (modes). The following commands were introduced or modified: clear sampler , debug sampler , mode , record , sampler , show sampler . |



CHAPTER 10

Flexible NetFlow - Layer 2 Fields

The Flexible NetFlow - Layer 2 Fields feature enables collecting statistics for Layer 2 fields such as MAC addresses and virtual LAN (VLAN) IDs from traffic.

- [Finding Feature Information, on page 127](#)
- [Information About Flexible NetFlow Layer 2 Fields , on page 127](#)
- [How to Configure Flexible NetFlow Layer 2 Fields, on page 128](#)
- [Configuration Examples for Flexible NetFlow Layer 2 Fields, on page 133](#)
- [Additional References, on page 134](#)
- [Feature Information for Flexible NetFlow - Layer 2 Fields, on page 135](#)

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.

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

Information About Flexible NetFlow Layer 2 Fields

Flexible NetFlow - Layer 2 Fields Overview

The Flexible NetFlow - Layer 2 Fields feature enables collecting statistics for Layer 2 fields such as MAC addresses and virtual LAN (VLAN) IDs from traffic.

How to Configure Flexible NetFlow Layer 2 Fields

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {source | destination} **group-tag**
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **show running-config flow record** *record-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow record <i>record-name</i> Example: Device(config)# flow record FLOW-RECORD-1 | Creates a flow record and enters Flexible NetFlow flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | <p>description <i>description</i></p> <p>Example:</p> <pre>Device(config-flow-record)# description Used for basic traffic analysis</pre> | (Optional) Creates a description for the flow record. |
| Step 5 | <p>match {ip ipv6} {destination source} address</p> <p>Example:</p> <pre>Device(config-flow-record)# match ipv4 destination address</pre> | <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields.</p> |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | <p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag</pre> <pre>Device(config-flow-record)# match flow cts destination group-tag</pre> | <p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 8 | collect interface {input output} Example: <pre>Device(config-flow-record)# collect interface input</pre> | Configures the input interface as a nonkey field for the record. Note This example configures the input interface as a nonkey field for the record. |
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | end Example: <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | show flow record <i>record-name</i> Example: <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | show running-config flow record <i>record-name</i> Example: <pre>Device# show running-config flow record FLOW_RECORD-1</pre> | (Optional) Displays the configuration of the specified flow record. |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {**timeout** {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: > enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: # configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: (config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: (config-flow-monitor)# description Used for basic ipv4 traffic analysis | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: (config-flow-monitor)# record FLOW-RECORD-1 | Specifies the record for the flow monitor. |
| Step 6 | cache { timeout { active } <i>seconds</i> type { normal } Example: | • type normal —Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: | (Optional) Specifies the name of an exporter that was created previously. |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code>(config-flow-monitor)# exporter EXPORTER-1</code> | |
| Step 9 | end Example: <code>(config-flow-monitor)# end</code> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[name] <i>monitor-name</i> [cache [format { csv record table }]]] Example: <code># show flow monitor FLOW-MONITOR-2 cache</code> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <code># show running-config flow monitor FLOW_MONITOR-1</code> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* {**input** | **output**}
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <code>Device> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device# configure terminal | |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 4 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | show flow interface <i>type number</i> Example: Device# show flow interface GigabitEthernet 0/0/0 | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |
| Step 8 | show flow monitor name <i>monitor-name</i> cache format record Example: Device# show flow monitor name FLOW_MONITOR-1 cache format record | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuration Examples for Flexible NetFlow Layer 2 Fields

Example: Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics

The following example shows how to configure Flexible NetFlow for monitoring MAC and VLAN statistics.

This example starts in global configuration mode.

```
!
flow record LAYER-2-FIELDS-1
match ipv4 source address
match ipv4 destination address
match datalink dot1q vlan output
```

```

match datalink mac source address input
match datalink mac source address output
match datalink mac destination address input
match flow direction
!
exit
!
!
flow monitor FLOW-MONITOR-4
  record LAYER-2-FIELDS-1
  exit
!
ip cef
!
interface GigabitEthernet0/0/1
  ip address 172.16.6.2 255.255.255.0
  ip flow monitor FLOW-MONITOR-1 input
!

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow - Layer 2 Fields

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 27: Feature Information for Flexible NetFlow - Layer 2 Fields

| Feature Name | Releases | Feature Information |
|-----------------------------------|--|---|
| Flexible NetFlow - Layer 2 Fields | 12.2(33)SRE 12.4(22)T Cisco IOS XE Release 3.2SE | Enables collecting statistics for Layer 2 fields such as MAC addresses and virtual LAN (VLAN) IDs from traffic. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: collect datalink dot1q vlan, collect datalink mac, match datalink dot1q vlan, match datalink mac. |



CHAPTER 11

Flexible Netflow - Ingress VRF Support

The Flexible Netflow - Ingress VRF Support feature enables collecting the virtual routing and forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key or a nonkey field.

- [Finding Feature Information, on page 137](#)
- [Information About Flexible NetFlow Ingress VRF Support , on page 137](#)
- [How to Configure Flexible NetFlow Ingress VRF Support , on page 138](#)
- [Configuration Examples for Flexible NetFlow Ingress VRF Support , on page 143](#)
- [Additional References, on page 144](#)
- [Feature Information for Flexible NetFlow—Ingress VRF Support , on page 145](#)

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.

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

Information About Flexible NetFlow Ingress VRF Support

Flexible NetFlow—Ingress VRF Support Overview

This feature enables collecting the virtual routing and forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key or a nonkey field.

How to Configure Flexible NetFlow Ingress VRF Support

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {source | destination} **group-tag**
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **show running-config flow record** *record-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow record <i>record-name</i> Example: Device(config)# flow record FLOW-RECORD-1 | Creates a flow record and enters Flexible NetFlow flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | <p>description <i>description</i></p> <p>Example:</p> <pre>Device(config-flow-record)# description Used for basic traffic analysis</pre> | (Optional) Creates a description for the flow record. |
| Step 5 | <p>match {ip ipv6} {destination source} address</p> <p>Example:</p> <pre>Device(config-flow-record)# match ipv4 destination address</pre> | <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields.</p> |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | <p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag</pre> <pre>Device(config-flow-record)# match flow cts destination group-tag</pre> | <p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 8 | collect interface {input output} Example: <pre>Device(config-flow-record)# collect interface input</pre> | Configures the input interface as a nonkey field for the record. Note This example configures the input interface as a nonkey field for the record. |
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | end Example: <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | show flow record <i>record-name</i> Example: <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | show running-config flow record <i>record-name</i> Example: <pre>Device# show running-config flow record FLOW_RECORD-1</pre> | (Optional) Displays the configuration of the specified flow record. |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {**timeout** {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: > enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: # configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: (config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: (config-flow-monitor)# description Used for basic ipv4 traffic analysis | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: (config-flow-monitor)# record FLOW-RECORD-1 | Specifies the record for the flow monitor. |
| Step 6 | cache { timeout { active } <i>seconds</i> type { normal } Example: | • type normal —Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: | (Optional) Specifies the name of an exporter that was created previously. |

| | Command or Action | Purpose |
|----------------|---|---|
| | <code>(config-flow-monitor)# exporter EXPORTER-1</code> | |
| Step 9 | end Example: <code>(config-flow-monitor)# end</code> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor <i>[[name] monitor-name [cache [format {csv record table}]]]</i> Example: <code># show flow monitor FLOW-MONITOR-2 cache</code> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <code># show running-config flow monitor FLOW_MONITOR-1</code> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name {input | output}*
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name cache format record*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <code>Device> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device# configure terminal | |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 4 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | show flow interface <i>type number</i> Example: Device# show flow interface GigabitEthernet 0/0/0 | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |
| Step 8 | show flow monitor name <i>monitor-name</i> cache format record Example: Device# show flow monitor name FLOW_MONITOR-1 cache format record | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuration Examples for Flexible NetFlow Ingress VRF Support

Example: Configuring Flexible NetFlow for Ingress VRF Support

The following example configures the collection of the virtual routing and forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key field.

This example starts in global configuration mode.

```

!
flow record rm_1
match routing vrf input
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface GigabitEthernet 0/0/0
ip vrf forwarding green
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 input
!
end

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow—Ingress VRF Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 28: Feature Information for Flexible NetFlow—Ingress VRF Support

| Feature Name | Releases | Feature Information |
|---------------------------------------|--|---|
| Flexible NetFlow--Ingress VRF Support | 12.2(33)SRE 12.2(50)SY 15.0(1)M 15.0(1)SY 15.0(1)SY1 | Enables collecting the virtual routing and forwarding (VRF) ID from incoming packets on a router by applying an input flow monitor having a flow record that collects the VRF ID as a key or a nonkey field. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: collect routing, match routing, option (Flexible NetFlow), show flow monitor. |



CHAPTER 12

Flexible NetFlow NBAR Application Recognition Overview

NBAR enables creation of different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key or a nonkey field.

- [Finding Feature Information, on page 147](#)
- [Information About Flexible NetFlow NBAR Application Recognition, on page 147](#)
- [How to Configure Flexible NetFlow NBAR Application Recognition, on page 148](#)
- [Configuration Examples for Flexible NetFlow NBAR Application Recognition, on page 154](#)
- [Additional References, on page 154](#)
- [Feature Information for Flexible NetFlow NBAR Application Recognition, on page 155](#)

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.

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

Information About Flexible NetFlow NBAR Application Recognition

Flexible NetFlow NBAR Application Recognition Overview

If the predefined Flexible NetFlow records are not suitable for your traffic requirements, you can create a user-defined (custom) record using the Flexible NetFlow **collect** and **match** commands. Before you can create a customized record, you must decide the criteria that you are going to use for the key and nonkey fields.

If you want to create a customized record for detecting network attacks, you must include the appropriate key and nonkey fields in the record to ensure that the router creates the flows and captures the data that you need

to analyze the attack and respond to it. Flexible NetFlow uses Network-based Application recognition (NBAR) to create different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key field.

How to Configure Flexible NetFlow NBAR Application Recognition

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} address
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {source | destination} group-tag
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **show running-config flow record** *record-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 3 | <p>flow record <i>record-name</i></p> <p>Example:</p> <pre>Device(config)# flow record FLOW-RECORD-1</pre> | <p>Creates a flow record and enters Flexible NetFlow flow record configuration mode.</p> <ul style="list-style-type: none"> This command also allows you to modify an existing flow record. |
| Step 4 | <p>description <i>description</i></p> <p>Example:</p> <pre>Device(config-flow-record)# description Used for basic traffic analysis</pre> | (Optional) Creates a description for the flow record. |
| Step 5 | <p>match {ip ipv6} {destination source} address</p> <p>Example:</p> <pre>Device(config-flow-record)# match ipv4 destination address</pre> | <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields.</p> |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | <p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag Device(config-flow-record)# match flow cts destination group-tag</pre> | <p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> |

| | Command or Action | Purpose |
|----------------|--|--|
| | | <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |
| Step 8 | <p>collect interface {input output}</p> <p>Example:</p> <pre>Device(config-flow-record)# collect interface input</pre> | <p>Configures the input interface as a nonkey field for the record.</p> <p>Note This example configures the input interface as a nonkey field for the record.</p> |
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | <p>end</p> <p>Example:</p> <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | <p>show flow record <i>record-name</i></p> <p>Example:</p> <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | <p>show running-config flow record <i>record-name</i></p> <p>Example:</p> | (Optional) Displays the configuration of the specified flow record. |

| | Command or Action | Purpose |
|--|--|---------|
| | Device# show running-config flow record FLOW_RECORD-1 | |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {*timeout* {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: > enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: | Enters global configuration mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| | <pre># configure terminal</pre> | |
| Step 3 | flow monitor <i>monitor-name</i> Example: <pre>(config)# flow monitor FLOW-MONITOR-1</pre> | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: <pre>(config-flow-monitor)# description Used for basic ipv4 traffic analysis</pre> | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: <pre>(config-flow-monitor)# record FLOW-RECORD-1</pre> | Specifies the record for the flow monitor. |
| Step 6 | cache { <i>timeout</i> { <i>active</i> } <i>seconds</i> type { normal } Example: | <ul style="list-style-type: none"> • type normal—Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: <pre>(config-flow-monitor)# exporter EXPORTER-1</pre> | (Optional) Specifies the name of an exporter that was created previously. |
| Step 9 | end Example: <pre>(config-flow-monitor)# end</pre> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 10 | show flow monitor [[<i>name</i>] <i>monitor-name</i> [cache [<i>format</i> { <i>csv</i> <i>record</i> <i>table</i> }]]] Example: <pre># show flow monitor FLOW-MONITOR-2 cache</pre> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <pre># show running-config flow monitor FLOW_MONITOR-1</pre> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 4 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|---------------|---|---|
| Step 7 | show flow interface <i>type number</i> Example: Device# show flow interface GigabitEthernet 0/0/0 | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |
| Step 8 | show flow monitor name <i>monitor-name</i> cache format record Example: Device# show flow monitor name FLOW_MONITOR-1 cache format record | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuration Examples for Flexible NetFlow NBAR Application Recognition

Example: Configuring Flexible NetFlow for Network-Based Application Recognition

```

!
flow record rm_1
match application name
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end

```

Additional References

Related Documents

| Related Topic | Document Title |
|--------------------|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |

| Related Topic | Document Title |
|---|---|
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow NBAR Application Recognition

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 29: Feature Information for Flexible NetFlow NBAR Application Recognition

| Feature Name | Releases | Feature Information |
|--|----------|--|
| Flexible NetFlow--NBAR Application Recognition | | <p>Network-based Application recognition (NBAR) enables creation of different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key or a nonkey field.</p> <p>The following commands were introduced or modified: collect application name, match application name, option (Flexible NetFlow), show flow monitor.</p> |



CHAPTER 13

Support for ISSU and SSO

High Availability (HA) support for Flexible Netflow is introduced by providing support for both In-Service Software Upgrade (ISSU) and Stateful Switchover (SSO).

These features are enabled by default when the redundancy mode of operation is set to SSO.

- [Finding Feature Information, on page 157](#)
- [Prerequisites for Flexible Netflow High Availability, on page 157](#)
- [Information About Flexible Netflow High Availability, on page 158](#)
- [How to Configure Flexible Netflow High Availability, on page 158](#)
- [How to Verify Flexible Netflow High Availability, on page 158](#)
- [Configuration Examples for Flexible Netflow High Availability, on page 159](#)
- [Additional References, on page 162](#)
- [Feature Information for Flexible Netflow High Availability Features, on page 164](#)
- [Glossary, on page 164](#)

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.

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

Prerequisites for Flexible Netflow High Availability

- The Cisco ISSU process must be configured and working properly. See the “Cisco In-Service Software Upgrade Process” feature module for more information.
- SSO must be configured and working properly. See the “Stateful Switchover” feature module for more information.
- Nonstop Forwarding (NSF) must be configured and working properly. See the “Cisco Nonstop Forwarding” feature module for more information.

Information About Flexible Netflow High Availability

ISSU

The ISSU process allows Cisco software to be updated or otherwise modified while packet forwarding continues. In most networks, planned software upgrades are a significant cause of downtime. ISSU allows Cisco software to be modified while packet forwarding continues, which increases network availability and reduces downtime caused by planned software upgrades.

SSO

SSO refers to the implementation of Cisco software that allows applications and features to maintain a defined state between an active and standby Route Processor (RP).

In specific Cisco networking devices that support dual RPs, SSO takes advantage of RP redundancy to increase network availability. The SSO feature takes advantage of RP redundancy by establishing one of the RPs as the active RP while the other RP is designated as the standby RP, and then synchronizing critical state information between them. Following an initial synchronization between the two processors, SSO dynamically maintains RP state information between them.

A switchover from the active to the standby processor occurs when the active RP fails, is removed from the networking device, or is manually taken down for maintenance.

How to Configure Flexible Netflow High Availability

There are no configuration tasks specific to Flexible Netflow. All generalized configuration tasks for ISSU and SSO are described in the chapters referenced in the [Prerequisites for Flexible Netflow High Availability, on page 157](#).

The Flexible Netflow high availability features are enabled by default when the redundancy mode of operation is set to SSO.

How to Verify Flexible Netflow High Availability

SUMMARY STEPS

1. **enable**
2. **show redundancy** [clients | counters | history | switchover history | states]
3. **show redundancy states**
4. **show sampler broker** [detail] | [picture]
5. **show flow exporter broker** [detail] | [picture]
6. **show flow record broker** [detail] | [picture]
7. **show flow monitor broker** [detail] | [picture]

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show redundancy [clients counters history switchover history states] Example: Device# show redundancy | Displays SSO configuration information. |
| Step 3 | show redundancy states Example: Device# show redundancy states | Verifies that the device is running in SSO mode. |
| Step 4 | show sampler broker [detail] [picture] Example: Device# show sampler broker detail | Displays information about the state of the exporter broker for the Flexible Netflow sampler. |
| Step 5 | show flow exporter broker [detail] [picture] Example: Device# show flow exporter broker detail | Displays information about the state of the broker for the Flexible Netflow flow exporter. |
| Step 6 | show flow record broker [detail] [picture] Example: Device# show flow record broker detail | Displays information about the state of the broker for the Flexible Netflow flow record. |
| Step 7 | show flow monitor broker [detail] [picture] Example: Device# show flow monitor broker detail | Displays information about the state of the broker for the Flexible Netflow flow monitor. |

What to do next

Configuration Examples for Flexible Netflow High Availability

There are no configuration examples for Flexible Netflow high availability features.

All examples are for displaying the status of Flexible Netflow high availability.

Example: Displaying Detailed Status for the Sampler Broker

The following example shows the status output for the Flexible Netflow flow record broker. This output is very similar to the output for the other Flexible Netflow brokers: the sampler broker, the flow exporter broker, and the flow monitor broker.

```
Device# show flow record broker detail
Brokering for Linecard 7 (0x80)
Multicast groups :-
 0x7F801C95D000
Linecard 7 (0x80) enabled for download
Consume report for Linecard 7 (0x80) (pos 1)
24/0 completed/pending updates (all VRFs)
Update list ranges from pos 1 to pos 0 :-
1 - 24 updates
0 - 0 updates
Broker records :-
* - - Start of list
1 - - Flush
1 - Mod - Create netflow-v5
1 - Mod - Create options interface-table
1 - Mod - Create options exporter-statistics
1 - Mod - Create options vrf-id-name-table
1 - Mod - Create options sampler-table
1 - Mod - Create options applications-name
1 - Mod - Create netflow-original
1 - Mod - Create netflow ipv4 original-input
```

Example: Displaying a Status Summary for the Flow Record Broker

The following example shows a status summary output for the Flexible Netflow flow record broker. This output is very similar to the output for the other Flexible Netflow brokers: the sampler broker, the flow exporter broker, and the flow monitor broker.

```
Device# show flow record broker picture
Key:
 '['=start record, ']'=end record, 'F'=flush record, 'D'=display record
 '+<n>'=sequenve of <n> Modify update records
 '-<n>'=sequenve of <n> Delete update records
 'C<<lc>:<vrf>>'=consume record for linecard(s) <lc> and VRF(s) <vrf> <*=all>
Brokers:
[FC<7 <0x80>:*>]
```

Example: Verifying Whether SSO is Configured

The following sample output shows that SSO is configured on the device:

```
Device# show redundancy states
my state = 13 -ACTIVE
peer state = 8 -STANDBY HOT
Mode = Duplex
Unit ID = 49
Redundancy Mode (Operational) = sso
Redundancy Mode (Configured) = sso
Redundancy State = sso
Maintenance Mode = Disabled
Manual Swact = enabled
```

```

Communications = Up
  client count = 67
client_notification_TMR = 30000 milliseconds
  RF debug mask = 0x0

```

Example: Displaying which SSO Protocols and Applications are Registered

The following sample output shows a list of applications and protocols that have registered as SSO protocols or applications on the device:

```

Device# show redundancy clients
clientID = 0      clientSeq = 0      RF_INTERNAL_MSG
clientID = 29     clientSeq = 60     Redundancy Mode RF
clientID = 139    clientSeq = 62     IfIndex
clientID = 25     clientSeq = 69     CHKPT RF
clientID = 1340   clientSeq = 90     ASR1000-RP Platform
clientID = 1501   clientSeq = 91     Cat6k CWAN HA
clientID = 78     clientSeq = 95     TSPTUN HA
clientID = 305    clientSeq = 96     Multicast ISSU Conso
clientID = 304    clientSeq = 97     IP multicast RF Clie
clientID = 22     clientSeq = 98     Network RF Client
clientID = 88     clientSeq = 99     HSRP
clientID = 114    clientSeq = 100    GLBP
clientID = 1341   clientSeq = 102    ASR1000 DPIDX
clientID = 1505   clientSeq = 103    Cat6k SPA TSM
clientID = 1344   clientSeq = 110    ASR1000-RP SBC RF
clientID = 227    clientSeq = 111    SBC RF
clientID = 71     clientSeq = 112    XDR RRP RF Client
clientID = 24     clientSeq = 113    CEF RRP RF Client
clientID = 146    clientSeq = 114    BFD RF Client
clientID = 306    clientSeq = 120    MFIB RRP RF Client
clientID = 1504   clientSeq = 128    Cat6k CWAN Interface
clientID = 75     clientSeq = 130    Tableid HA
clientID = 401    clientSeq = 131    NAT HA
clientID = 402    clientSeq = 132    TPM RF client
clientID = 5      clientSeq = 135    Config Sync RF clien
clientID = 68     clientSeq = 149    Virtual Template RF
clientID = 23     clientSeq = 152    Frame Relay
clientID = 49     clientSeq = 153    HDLC
clientID = 72     clientSeq = 154    LSD HA Proc
clientID = 113    clientSeq = 155    MFI STATIC HA Proc
clientID = 20     clientSeq = 171    IPROUTING NSF RF cli
clientID = 100    clientSeq = 173    DHCP
clientID = 101    clientSeq = 174    DHCPD
clientID = 74     clientSeq = 183    MPLS VPN HA Client
clientID = 34     clientSeq = 185    SNMP RF Client
clientID = 52     clientSeq = 186    ATM
clientID = 69     clientSeq = 189    AAA
clientID = 118    clientSeq = 190    L2TP
clientID = 82     clientSeq = 191    CCM RF
clientID = 35     clientSeq = 192    History RF Client
clientID = 90     clientSeq = 204    RSVP HA Services
clientID = 70     clientSeq = 215    FH COMMON RF CLIENT
clientID = 54     clientSeq = 220    SNMP HA RF Client
clientID = 73     clientSeq = 221    LDP HA
clientID = 76     clientSeq = 222    IPRM
clientID = 57     clientSeq = 223    ARP
clientID = 50     clientSeq = 230    FH_RF_Event_Detector
clientID = 1342   clientSeq = 240    ASR1000 SpaFlow
clientID = 1343   clientSeq = 241    ASR1000 IF Flow
clientID = 83     clientSeq = 255    AC RF Client
clientID = 84     clientSeq = 257    ATOM manager

```

```

clientID = 85      clientSeq = 258      SSM
clientID = 102     clientSeq = 273      MQC QoS
clientID = 94      clientSeq = 280      Config Verify RF cli
clientID = 135     clientSeq = 289      IKE RF Client
clientID = 136     clientSeq = 290      IPSEC RF Client
clientID = 130     clientSeq = 291      CRYPTO RSA
clientID = 148     clientSeq = 296      DHCPv6 Relay
clientID = 4000    clientSeq = 303      RF_TS_CLIENT
clientID = 4005    clientSeq = 305      ISSU Test Client
clientID = 93      clientSeq = 309      Network RF 2 Client
clientID = 205     clientSeq = 311      FEC Client
clientID = 141     clientSeq = 319      DATA_DESCRIPTOR RF C
clientID = 4006    clientSeq = 322      Network Clock
clientID = 225     clientSeq = 326      VRRP
clientID = 65000   clientSeq = 336      RF_LAST_CLIENT

```

Additional References

Related Documents

| Related Topic | Document Title |
|--|---|
| In-Service Software Upgrade process conceptual and configuration information | Cisco IOS XE In Service Software Upgrade Process module |
| Nonstop Forwarding conceptual and configuration information | Cisco Nonstop Forwarding module |
| Stateful switchover conceptual and configuration information | Stateful Switchover module |
| White paper on performing In-Service Software Upgrades. | High-Availability Overview, Cisco IOS Software: Guide to Performing In-Service Software Upgrades |
| Answer to questions about the In-Service Software Upgrade product and process. | Cisco IOS In-Service Software Upgrade, Questions and Answers |
| Cisco IOS commands | Cisco IOS Master Commands List, All Releases |
| Cisco IOS High Availability commands | <i>Cisco IOS High Availability Command Reference</i> |
| Cisco IOS debug commands | <i>Cisco IOS Debug Command Reference</i> |
| SSO - BFD | "Bidirectional Forwarding Detection" chapter in the <i>IP Routing Protocols Configuration Guide</i> |
| SSO HSRP | "Configuring HSRP" chapter in the <i>IP Application Services Configuration Guide</i> |
| SSO - MPLS VPN 6VPE and 6PE SSO support | NSF/SSO and ISSU - MPLS VPN 6VPE and 6PE |
| SSO and RPR on the Cisco ASR 1000 Series Routers | <i>Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide</i> |

| Related Topic | Document Title |
|--------------------------|--|
| SSO VRRP | "Configuring VRRP" chapter in the <i>Application Services Configuration Guide</i> |
| SNMP configuration tasks | "Configuring SNMP Support" module of <i>Network Management Configuration Guide</i> |
| SNMP commands | <i>Cisco IOS Network Management Command Reference</i> |

Standards

| Standard | Title |
|---|-------|
| No new or modified standards are supported by this feature. | -- |

MIBs

| MIB | MIBs Link |
|------|--|
| None | 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 |

RFCs

| RFC | Title |
|--|--|
| No new or modified RFCs are supported by this feature. | -- |
| RFC 1907 | Management Information Base for Version 2 of the Simple Network Management Protocol |
| RFC 2571 | An Architecture for Describing SNMP Management Frameworks |
| RFC 2573 | SNMP Applications |
| RFC 2574 | User-Based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3) |
| RFC 2575 | View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) |
| RFC 2863 | The Interfaces Group MIB |
| RFC 4133 | Entity MIB (Version 3) |

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/techsupport |

Feature Information for Flexible Netflow High Availability Features

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 30: Feature Information for Flexible Netflow High Availability Features

| Feature Name | Releases | Feature Information |
|--------------------------------------|--|---|
| Flexible NetFlow: ISSU / SSO Support | Cisco IOS XE Release 3.3S 15.0(1)SY 15.0(1)SY1 | Flexible Netflow has been enhanced to support ISSU and SSO. |

Glossary

CPE --customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the service provider, installed at customer sites, and connected to the network.

ISSU --In Service Software Upgrade. ISSU is a process that allows Cisco IOS software to be updated or otherwise modified while packet forwarding continues.

RP --Route Processor. A generic term for the centralized control unit in a chassis.

SSO --Stateful Switchover. SSO refers to the implementation of Cisco IOS software that allows applications and features to maintain a defined state between an active and standby RP. When a switchover occurs, forwarding and sessions are maintained. SSO makes an RP failure undetectable to the network.



CHAPTER 14

Flexible NetFlow IPFIX Export Format

The Flexible NetFlow IPFIX Export Format feature enables sending export packets using the IPFIX export protocol. The export of extracted fields from NBAR is only supported over IPFIX.

- [Finding Feature Information](#), on page 165
- [Information About Flexible NetFlow IPFIX Export Format](#), on page 165
- [How to Configure Flexible NetFlow IPFIX Export Format](#), on page 166
- [Configuration Examples for Flexible NetFlow IPFIX Export Format](#), on page 168
- [Feature Information for Flexible NetFlow: IPFIX Export Format](#), on page 169

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.

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

Information About Flexible NetFlow IPFIX Export Format

Flexible NetFlow IPFIX Export Format Overview

IPFIX is an IETF standard based on NetFlow v9.

The Flexible NetFlow IPFIX Export Format feature enables sending export packets using the IPFIX export protocol. The export of extracted fields from NBAR is only supported over IPFIX.

How to Configure Flexible NetFlow IPFIX Export Format

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data** *timeout seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**
15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 3 | flow exporter <i>exporter-name</i> Example: <pre>Device(config)# flow exporter EXPORTER-1</pre> | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: <pre>Device(config-flow-exporter)# description Exports to the datacenter</pre> | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination { <i>ip-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] Example: <pre>Device(config-flow-exporter)# destination 172.16.10.2</pre> | Specifies the IP address or hostname of the destination system for the exporter. <p>Note You can export to a destination using either an IPv4 or IPv6 address.</p> |
| Step 6 | export-protocol { netflow-v5 netflow-v9 ipfix } Example: <pre>Device(config-flow-exporter)# export-protocol netflow-v9</pre> | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none"> Default: netflow-v9. |
| Step 7 | dscp <i>dscp</i> Example: <pre>Device(config-flow-exporter)# dscp 63</pre> | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none"> The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |
| Step 8 | source <i>interface-type interface-number</i> Example: <pre>Device(config-flow-exporter)# source ethernet 0/0</pre> | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |
| Step 9 | option { exporter-stats interface-table sampler-table vrf-table } [timeout <i>seconds</i>] Example: <pre>Device(config-flow-exporter)# option exporter-stats timeout 120</pre> | (Optional) Configures options data parameters for the exporter. <ul style="list-style-type: none"> You can configure all three options concurrently. The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |
| Step 10 | output-features Example: <pre>Device(config-flow-exporter)# output-features</pre> | (Optional) Enables sending export packets using quality of service (QoS) and encryption. |

| | Command or Action | Purpose |
|----------------|--|--|
| Step 11 | template data timeout <i>seconds</i> Example: <pre>Device(config-flow-exporter)# template data timeout 120</pre> | (Optional) Configures resending of templates based on a timeout. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |
| Step 12 | transport udp <i>udp-port</i> Example: <pre>Device(config-flow-exporter)# transport udp 650</pre> | Specifies the UDP port on which the destination system is listening for exported datagrams. <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | ttl <i>seconds</i> Example: <pre>Device(config-flow-exporter)# ttl 15</pre> | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | end Example: <pre>Device(config-flow-exporter)# end</pre> | Exits flow exporter configuration mode and returns to privileged EXEC mode. |
| Step 15 | show flow exporter <i>exporter-name</i> Example: <pre>Device# show flow exporter FLOW_EXPORTER-1</pre> | (Optional) Displays the current status of the specified flow exporter. |
| Step 16 | show running-config flow exporter <i>exporter-name</i> Example: <pre>Device# show running-config flow exporter FLOW_EXPORTER-1</pre> | (Optional) Displays the configuration of the specified flow exporter. |

Configuration Examples for Flexible NetFlow IPFIX Export Format

Example: Configuring Flexible NetFlow IPFIX Export Format

The following example shows how to configure IPFIX export format for Flexible NetFlow.

This sample starts in global configuration mode:

```
!
flow exporter EXPORTER-1
 destination 172.16.10.2
 export-protocol ipfix
```

```

transport udp 90
exit
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exporter EXPORTER-1
!
ip cef
!
interface Ethernet 0/0
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!

```

Feature Information for Flexible NetFlow: IPFIX Export Format

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 31: Feature Information for Flexible NetFlow : IPFIX Export Format

| Feature Name | Releases | Feature Information |
|--|---|---|
| Flexible NetFlow: IPFIX Export Format | 15.2(4)M Cisco IOS XE Release 3.7S 15.2(1)SY | Enables sending export packets using the IPFIX export protocol. The export of extracted fields from NBAR is only supported over IPFIX. Support for this feature was added for Cisco ASR 1000 Series Aggregation Services routers in Cisco IOS XE Release 3.7S. The following command was introduced: export-protocol . |



CHAPTER 15

Flexible Netflow Export to an IPv6 Address

The Export to an IPv6 Address feature enables Flexible NetFlow to export data to a destination using an IPv6 address.

- [Finding Feature Information, on page 171](#)
- [Information About Flexible Netflow Export to an IPv6 Address, on page 171](#)
- [How to Configure Flexible Netflow Export to an IPv6 Address, on page 171](#)
- [Configuration Examples for Flexible Netflow Export to an IPv6 Address, on page 174](#)
- [Additional References, on page 176](#)
- [Feature Information for Flexible NetFlow Export to an IPv6 Address, on page 177](#)

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.

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

Information About Flexible Netflow Export to an IPv6 Address

Flexible Netflow Export to an IPv6 Address Overview

This feature enables Flexible NetFlow to export data to a destination using an IPv6 address.

How to Configure Flexible Netflow Export to an IPv6 Address

Configuring the Flow Exporter

Perform this required task to configure the flow exporter.



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 either an IPv4 or IPv6 address.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **dscp** *dscp*
8. **source** *interface-type interface-number*
9. **option** {**exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]
10. **output-features**
11. **template data timeout** *seconds*
12. **transport udp** *udp-port*
13. **ttl** *seconds*
14. **end**
15. **show flow exporter** *exporter-name*
16. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode. • This command also allows you to modify an existing flow exporter. |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 4 | description <i>description</i> Example: <pre>Device(config-flow-exporter)# description Exports to the datacenter</pre> | (Optional) Configures a description to the exporter that will appear in the configuration and the display of the show flow exporter command. |
| Step 5 | destination { <i>ip-address</i> <i>hostname</i> } [vrf <i>vrf-name</i>] Example: <pre>Device(config-flow-exporter)# destination 172.16.10.2</pre> | Specifies the IP address or hostname of the destination system for the exporter. Note You can export to a destination using either an IPv4 or IPv6 address. |
| Step 6 | export-protocol { netflow-v5 netflow-v9 ipfix } Example: <pre>Device(config-flow-exporter)# export-protocol netflow-v9</pre> | Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. <ul style="list-style-type: none"> • Default: netflow-v9. |
| Step 7 | dscp <i>dscp</i> Example: <pre>Device(config-flow-exporter)# dscp 63</pre> | (Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. <ul style="list-style-type: none"> • The range for the <i>dscp</i> argument is from 0 to 63. Default: 0. |
| Step 8 | source <i>interface-type interface-number</i> Example: <pre>Device(config-flow-exporter)# source ethernet 0/0</pre> | (Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams. |
| Step 9 | option { exporter-stats interface-table sampler-table vrf-table } [timeout <i>seconds</i>] Example: <pre>Device(config-flow-exporter)# option exporter-stats timeout 120</pre> | (Optional) Configures options data parameters for the exporter. <ul style="list-style-type: none"> • You can configure all three options concurrently. • The range for the <i>seconds</i> argument is 1 to 86,400. Default: 600. |
| Step 10 | output-features Example: <pre>Device(config-flow-exporter)# output-features</pre> | (Optional) Enables sending export packets using quality of service (QoS) and encryption. |
| Step 11 | template data timeout <i>seconds</i> Example: <pre>Device(config-flow-exporter)# template data timeout 120</pre> | (Optional) Configures resending of templates based on a timeout. <ul style="list-style-type: none"> • The range for the <i>seconds</i> argument is 1 to 86400 (86400 seconds = 24 hours). |

| | Command or Action | Purpose |
|----------------|---|--|
| Step 12 | transport udp <i>udp-port</i> Example: Device(config-flow-exporter)# transport udp 650 | Specifies the UDP port on which the destination system is listening for exported datagrams. <ul style="list-style-type: none"> The range for the <i>udp-port</i> argument is from 1 to 65536. |
| Step 13 | ttl <i>seconds</i> Example: Device(config-flow-exporter)# ttl 15 | (Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. <ul style="list-style-type: none"> The range for the <i>seconds</i> argument is from 1 to 255. |
| Step 14 | end Example: Device(config-flow-exporter)# end | Exits flow exporter configuration mode and returns to privileged EXEC mode. |
| Step 15 | show flow exporter <i>exporter-name</i> Example: Device# show flow exporter FLOW_EXPORTER-1 | (Optional) Displays the current status of the specified flow exporter. |
| Step 16 | show running-config flow exporter <i>exporter-name</i> Example: Device# show running-config flow exporter FLOW_EXPORTER-1 | (Optional) Displays the configuration of the specified flow exporter. |

Configuration Examples for Flexible Netflow Export to an IPv6 Address

Example: Configuring Multiple Export Destinations

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv4 or IPv6 traffic. This sample starts in global configuration mode:

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv4:

```

!
flow exporter EXPORTER-1
 destination 172.16.10.2
 transport udp 90
 exit
!
flow exporter EXPORTER-2
 destination 172.16.10.3
 transport udp 90
 exit

```

```

!
flow record v4_r1
match ipv4 tos
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long

flow monitor FLOW-MONITOR-1
record v4_r1
exporter EXPORTER-2
exporter EXPORTER-1
!

ip cef
!
interface GigabitEthernet1/0/0
ip address 172.16.6.2 255.255.255.0
ip flow monitor FLOW-MONITOR-1 input
!

```

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv6:

```

!
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
exit
!
flow exporter EXPORTER-2
destination 172.16.10.3
transport udp 90
exit
!

flow record v6_r1
match ipv6 traffic-class
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
collect counter bytes long
collect counter packets long
!

!
flow monitor FLOW-MONITOR-2
record v6_r1
exporter EXPORTER-2
exporter EXPORTER-1
!
ip cef
!
interface GigabitEthernet1/0/0
ipv6 address 2001:DB8:2:ABCD::2/48
ipv6 flow monitor FLOW-MONITOR-2 input
!

```

The following display output shows that the flow monitor is exporting data to the two exporters:

```
Device# show flow monitor FLOW-MONITOR-1
Flow Monitor FLOW-MONITOR-1:
  Description:      User defined
  Flow Record:     v4_r1
  Flow Exporter:   EXPORTER-1
                  EXPORTER-2

Cache:
  Type:            normal (Platform cache)
  Status:          allocated
  Size:            4096 entries / 311316 bytes
  Inactive Timeout: 15 secs
  Active Timeout:  1800 secs
  Update Timeout:  1800 secs
```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow Export to an IPv6 Address

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 32: Feature Information for Flexible NetFlow Export to an IPv6 Address

| Feature Name | Releases | Feature Information |
|---|--|--|
| Flexible NetFlow: Export to an IPv6 Address | 15.2(2)T Cisco IOS XE Release 3.7S 15.2(1)SY | This feature enables Flexible NetFlow to export data to a destination using an IPv6 address. The following commands were introduced or modified: destination |



CHAPTER 16

Flexible Netflow—Egress VRF Support

The Flexible Netflow—Egress VRF Support feature enables collecting the virtual routing and forwarding (VRF) ID from outgoing packets on a router by applying an output flow monitor having a flow record that collects the VRF ID as a key or a nonkey field.

- [Finding Feature Information, on page 179](#)
- [Information About Flexible Netflow Egress VRF Support , on page 179](#)
- [How to Configure Flexible Netflow Egress VRF Support , on page 180](#)
- [Configuration Examples for Flexible Netflow Egress VRF Support , on page 186](#)
- [Additional References, on page 186](#)
- [Feature Information for Flexible NetFlow—Egress VRF Support, on page 187](#)

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.

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

Information About Flexible Netflow Egress VRF Support

Flexible Netflow—Egress VRF Support Overview

The Flexible Netflow—Egress VRF Support feature enables collecting the virtual routing and forwarding (VRF) ID from outgoing packets on a router by applying an output flow monitor having a flow record that collects the VRF ID as a key or a nonkey field.

How to Configure Flexible Netflow Egress VRF Support

Creating a Flow Record

Perform this task to configure a customized flow record.

Customized flow records are used to analyze traffic data for a specific purpose. A customized flow record must have at least one **match** criterion for use as the key field and typically has at least one **collect** criterion for use as a nonkey field.

There are hundreds of possible permutations of customized flow records. This task shows the steps that are used to create one of the possible permutations. Modify the steps in this task as appropriate to create a customized flow record for your requirements.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {ip | ipv6} {destination | source} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **match flow cts** {source | destination} **group-tag**
8. **collect interface** {input | output}
9. Repeat the above step as required to configure additional nonkey fields for the record.
10. **end**
11. **show flow record** *record-name*
12. **show running-config flow record** *record-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow record <i>record-name</i> Example: Device(config)# flow record FLOW-RECORD-1 | Creates a flow record and enters Flexible NetFlow flow record configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow record. |

| | Command or Action | Purpose |
|---------------|---|--|
| Step 4 | <p>description <i>description</i></p> <p>Example:</p> <pre>Device(config-flow-record)# description Used for basic traffic analysis</pre> | (Optional) Creates a description for the flow record. |
| Step 5 | <p>match {ip ipv6} {destination source} address</p> <p>Example:</p> <pre>Device(config-flow-record)# match ipv4 destination address</pre> | <p>Note This example configures the IPv4 destination address as a key field for the record. For information about the other key fields available for the match ipv4 command, and the other match commands that are available to configure key fields.</p> |
| Step 6 | Repeat Step 5 as required to configure additional key fields for the record. | — |
| Step 7 | <p>match flow cts {source destination} group-tag</p> <p>Example:</p> <pre>Device(config-flow-record)# match flow cts source group-tag</pre> <pre>Device(config-flow-record)# match flow cts destination group-tag</pre> | <p>Note This example configures the CTS source group tag and destination group tag as a key field for the record. For information about the other key fields available for the match ipv4/ipv6 command, and the other match commands that are available to configure key fields.</p> <p>Note</p> <ul style="list-style-type: none"> • Ingress: <ul style="list-style-type: none"> • In an incoming packet, if a header is present, SGT will reflect the same value as the header. If no value is present, it will show zero. • The DGT value will not depend on the ingress port SGACL configuration. • Egress: <ul style="list-style-type: none"> • If either propagate SGT or CTS is disabled on the egress interface, then SGT will be zero. • In an outgoing packet, if SGACL configuration that corresponds to the (SGT, DGT) exists, DGT will be non-zero. • If SGACL is disabled on the egress port/VLAN or if global SGACL enforcement is disabled, then DGT will be zero |

| | Command or Action | Purpose |
|----------------|--|---|
| Step 8 | collect interface {input output} Example: <pre>Device(config-flow-record)# collect interface input</pre> | Configures the input interface as a nonkey field for the record. Note This example configures the input interface as a nonkey field for the record. |
| Step 9 | Repeat the above step as required to configure additional nonkey fields for the record. | — |
| Step 10 | end Example: <pre>Device(config-flow-record)# end</pre> | Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode. |
| Step 11 | show flow record <i>record-name</i> Example: <pre>Device# show flow record FLOW_RECORD-1</pre> | (Optional) Displays the current status of the specified flow record. |
| Step 12 | show running-config flow record <i>record-name</i> Example: <pre>Device# show running-config flow record FLOW_RECORD-1</pre> | (Optional) Displays the configuration of the specified flow record. |

Creating a Customized Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries.

Before you begin

If you want to use a customized record instead of using one of the Flexible NetFlow predefined records, you must create the customized record before you can perform this task.

If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor. For information about the **ip flow monitor** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}
6. **cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | **type** {**immediate** | **normal** | **permanent**}}
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.
8. **statistics packet** **protocol**
9. **statistics packet** **size**
10. **exporter** *exporter-name*
11. **end**
12. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]]
13. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: Device(config-flow-monitor)# description Used for basic ipv4 traffic analysis | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> netflow-original netflow { ipv4 ipv6 } <i>record</i> [peer]} Example: Device(config-flow-monitor)# record FLOW-RECORD-1 | Specifies the record for the flow monitor. |
| Step 6 | cache { entries <i>number</i> timeout { active inactive update } <i>seconds</i> type { immediate normal permanent }} | (Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. |

| | Command or Action | Purpose |
|----------------|--|---|
| | <p>Example:</p> <pre>Device(config-flow-monitor)# cache type normal</pre> | <ul style="list-style-type: none"> The values for the keywords associated with the timeout keyword have no effect when the cache type is set to immediate. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | <p>statistics packet protocol</p> <p>Example:</p> <pre>Device(config-flow-monitor)# statistics packet protocol</pre> | (Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors. |
| Step 9 | <p>statistics packet size</p> <p>Example:</p> <pre>Device(config-flow-monitor)# statistics packet size</pre> | (Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors. |
| Step 10 | <p>exporter exporter-name</p> <p>Example:</p> <pre>Device(config-flow-monitor)# exporter EXPORTER-1</pre> | (Optional) Specifies the name of an exporter that was created previously. |
| Step 11 | <p>end</p> <p>Example:</p> <pre>Device(config-flow-monitor)# end</pre> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 12 | <p>show flow monitor [[name] <i>monitor-name</i> [cache [format {csv record table}]] [statistics]]</p> <p>Example:</p> <pre>Device# show flow monitor FLOW-MONITOR-2 cache</pre> | (Optional) Displays the status and statistics for a Flexible NetFlow flow monitor. |
| Step 13 | <p>show running-config flow monitor <i>monitor-name</i></p> <p>Example:</p> <pre>Device# show running-config flow monitor FLOW_MONITOR-1</pre> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* **{input | output}**
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|---|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. • Enter your password if prompted. |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: Device(config)# interface GigabitEthernet 0/0/0 | Specifies an interface and enters interface configuration mode. |
| Step 4 | {ip ipv6} flow monitor <i>monitor-name</i> {input output} Example: Device(config-if)# ip flow monitor FLOW-MONITOR-1 input | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | end Example: Device(config-if)# end | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | show flow interface <i>type number</i> Example: Device# show flow interface GigabitEthernet 0/0/0 | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |

| | Command or Action | Purpose |
|---------------|--|---|
| Step 8 | show flow monitor name <i>monitor-name</i> cache format record Example: Device# show flow monitor name FLOW_MONITOR-1 cache format record | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuration Examples for Flexible Netflow Egress VRF Support

Example Configuring Flexible NetFlow for Egress VRF Support

The following example configures the collection of the virtual routing and forwarding (VRF) ID from outgoing packets on a router by applying an output flow monitor having a flow record that collects the VRF ID as a key field.

This example starts in global configuration mode.

```

!
flow record rm_1
match routing vrf output
match ipv4 source address
match ipv4 destination address
collect interface input
collect interface output
collect counter packets
!
flow monitor mm_1
record rm_1
!
interface GigabitEthernet 0/0/0
ip vrf forwarding green
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 output
!
end

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow—Egress VRF Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 33: Feature Information for Flexible NetFlow—Egress VRF Support

| Feature Name | Releases | Feature Information |
|-------------------------------------|---------------------------|--|
| Flexible NetFlow—Egress VRF Support | Cisco IOS XE Release 3.8S | Enables collecting the virtual routing and forwarding (VRF) ID from outgoing packets on a router by applying an output flow monitor having a flow record that collects the VRF ID as a key or a nonkey field. The following commands were introduced or modified: collect routing , match routing , option (Flexible NetFlow) , show flow monitor . |



CHAPTER 17

Flexible NetFlow - MPLS Support

The Flexible NetFlow - MPLS Support feature supports the monitoring of the following MPLS-related fields:

- MPLS Labels 1-6 (3 bytes -- 20 bits of label, 3 bits of EXP, 1 bit of EOS).
- Top Label EXP i.e. the EXP field for label 1.
- Top Label TTL i.e. the TTL field for label 1.
- [Finding Feature Information, on page 189](#)
- [Information About Flexible NetFlow MPLS Support, on page 189](#)
- [How to Configure Flexible NetFlow MPLS Support, on page 190](#)
- [Configuration Examples for Flexible NetFlow MPLS Support, on page 195](#)
- [Additional References, on page 196](#)
- [Feature Information for Flexible NetFlow: MPLS Support , on page 197](#)

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.

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

Information About Flexible NetFlow MPLS Support

Flexible NetFlow—MPLS Support Overview

This feature enables collecting MPLS label IDs by applying a flow monitor having a flow record that collects the MPLS label IDs as key or nonkey fields.

How to Configure Flexible NetFlow MPLS Support

Configuring a Flow Exporter for the Flow Monitor

Perform this optional task to configure a flow exporter for the flow monitor in order to export the data that is collected by Flexible NetFlow to a remote system for further analysis and storage.

Flow exporters are used to send the data that you collect with Flexible NetFlow to a remote system such as a NetFlow Collection Engine. Exporters use UDP as the transport protocol and use the Version 9 export format.



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 either an IPv4 or IPv6 address.



Note When you configure an exporter, configure the exporter in such a way that the source interface is defined as a WAN interface. This configuration helps you prevent any unpredictable behavior because the NAT is not applied on the packets.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow exporter** *exporter-name*
4. **description** *description*
5. **destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*]
6. **export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**}
7. **transport udp** *udp-port*
8. **exit**
9. **flow monitor** *flow-monitor-name*
10. **exporter** *exporter-name*
11. **end**
12. **show flow exporter** *exporter-name*
13. **show running-config flow exporter** *exporter-name*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Device> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|---------|--|---|
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow exporter <i>exporter-name</i> Example: Device(config)# flow exporter EXPORTER-1 | Creates a flow exporter and enters Flexible NetFlow flow exporter configuration mode. <ul style="list-style-type: none"> This command also allows you to modify an existing flow exporter. |
| Step 4 | description <i>description</i> Example: Device(config-flow-exporter)# description Exports to datacenter | (Optional) Creates a description for the flow exporter. |
| Step 5 | destination {<i>hostname</i> <i>ip-address</i>} [<i>vrf vrf-name</i>] Example: Device(config-flow-exporter)# destination 172.16.10.2 | Specifies the hostname or IP address of the system to which the exporter sends data. Note You can export to a destination using either an IPv4 or IPv6 address. |
| Step 6 | export-protocol {<i>netflow-v5</i> <i>netflow-v9</i> <i>ipfix</i>} Example: Device(config-flow-exporter)# export-protocol netflow-v9 | Specifies the version of the NetFlow export protocol used by the exporter. <ul style="list-style-type: none"> Default: netflow-v9. |
| Step 7 | transport udp <i>udp-port</i> Example: Device(config-flow-exporter)# transport udp 65 | Configures UDP as the transport protocol and specifies the UDP port on which the destination system is listening for exported Flexible NetFlow traffic. |
| Step 8 | exit Example: Device(config-flow-exporter)# exit | Exits Flexible NetFlow flow exporter configuration mode and returns to global configuration mode. |
| Step 9 | flow monitor <i>flow-monitor-name</i> Example: Device(config)# flow monitor FLOW-MONITOR-1 | Enters Flexible NetFlow flow monitor configuration mode for the flow monitor that you created previously. |
| Step 10 | exporter <i>exporter-name</i> Example: | Specifies the name of an exporter that you created previously. |

| | Command or Action | Purpose |
|----------------|--|---|
| | <code>Device(config-flow-monitor)# exporter EXPORTER-1</code> | |
| Step 11 | end Example: <code>Device(config-flow-monitor)# end</code> | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |
| Step 12 | show flow exporter <i>exporter-name</i> Example: <code>Device# show flow exporter FLOW_EXPORTER-1</code> | (Optional) Displays the current status of the specified flow exporter. |
| Step 13 | show running-config flow exporter <i>exporter-name</i> Example: <code>Device<# show running-config flow exporter FLOW_EXPORTER-1</code> | (Optional) Displays the configuration of the specified flow exporter. |

Creating a Flow Monitor

Perform this required task to create a customized flow monitor.

Each flow monitor has a separate cache assigned to it. Each flow monitor requires a record to define the contents and layout of its cache entries. These record formats can be a user-defined format. An advanced user can create a customized format using the **flow record** command.

Before you begin

If you want to use a customized record, you must create the customized record before you can perform this task. If you want to add a flow exporter to the flow monitor for data export, you must create the exporter before you can complete this task.



Note

You must use the **no ip flow monitor** command to remove a flow monitor from all of the interfaces to which you have applied it before you can modify the parameters for the **record** command on the flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor** *monitor-name*
4. **description** *description*
5. **record** {*record-name*}
6. **cache** {*timeout* {**active**} *seconds* | **type** { **normal** }
7. Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor.

8. **exporter** *exporter-name*
9. **end**
10. **show flow monitor** [[*name*] *monitor-name* [**cache** [**format** {*csv* | *record* | *table*}]]]
11. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|--|--|
| Step 1 | enable Example: <pre>> enable</pre> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <pre># configure terminal</pre> | Enters global configuration mode. |
| Step 3 | flow monitor <i>monitor-name</i> Example: <pre>(config)# flow monitor FLOW-MONITOR-1</pre> | Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. <ul style="list-style-type: none"> • This command also allows you to modify an existing flow monitor. |
| Step 4 | description <i>description</i> Example: <pre>(config-flow-monitor)# description Used for basic ipv4 traffic analysis</pre> | (Optional) Creates a description for the flow monitor. |
| Step 5 | record { <i>record-name</i> } Example: <pre>(config-flow-monitor)# record FLOW-RECORD-1</pre> | Specifies the record for the flow monitor. |
| Step 6 | cache { timeout { <i>active</i> } <i>seconds</i> type { normal } Example: | <ul style="list-style-type: none"> • type normal—Configure normal flow removal from the flow cache. |
| Step 7 | Repeat Step 6 as required to finish modifying the cache parameters for this flow monitor. | — |
| Step 8 | exporter <i>exporter-name</i> Example: <pre>(config-flow-monitor)# exporter EXPORTER-1</pre> | (Optional) Specifies the name of an exporter that was created previously. |
| Step 9 | end Example: | Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode. |

| | Command or Action | Purpose |
|----------------|--|--|
| | <code>(config-flow-monitor)# end</code> | |
| Step 10 | show flow monitor [[name] <i>monitor-name</i> [cache [format {csv record table}]]] Example: <code># show flow monitor FLOW-MONITOR-2 cache</code> | (Optional) Displays the status for a Flexible NetFlow flow monitor. |
| Step 11 | show running-config flow monitor <i>monitor-name</i> Example: <code># show running-config flow monitor FLOW_MONITOR-1</code> | (Optional) Displays the configuration of the specified flow monitor. |

Applying a Flow Monitor to an Interface

Before it can be activated, a flow monitor must be applied to at least one interface. Perform this required task to activate a flow monitor.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **{ip | ipv6} flow monitor** *monitor-name* {input | output}
5. Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic.
6. **end**
7. **show flow interface** *type number*
8. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

| | Command or Action | Purpose |
|---------------|---|--|
| Step 1 | enable Example: <code>Device> enable</code> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: <code>Device# configure terminal</code> | Enters global configuration mode. |
| Step 3 | interface <i>type number</i> Example: | Specifies an interface and enters interface configuration mode. |

| | Command or Action | Purpose |
|---------------|--|---|
| | Device(config)# interface GigabitEthernet 0/0/0 | |
| Step 4 | <p>{ip ipv6} flow monitor <i>monitor-name</i> {input output}</p> <p>Example:</p> <pre>Device(config-if)# ip flow monitor FLOW-MONITOR-1 input</pre> | Activates a flow monitor that was created previously by assigning it to the interface to analyze traffic. |
| Step 5 | Repeat Steps 3 and 4 to activate a flow monitor on any other interfaces in the device over which you want to monitor traffic. | — |
| Step 6 | <p>end</p> <p>Example:</p> <pre>Device(config-if)# end</pre> | Exits interface configuration mode and returns to privileged EXEC mode. |
| Step 7 | <p>show flow interface <i>type number</i></p> <p>Example:</p> <pre>Device# show flow interface GigabitEthernet 0/0/0</pre> | Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface. |
| Step 8 | <p>show flow monitor name <i>monitor-name</i> cache format record</p> <p>Example:</p> <pre>Device# show flow monitor name FLOW_MONITOR-1 cache format record</pre> | Displays the status, statistics, and flow data in the cache for the specified flow monitor. |

Configuration Examples for Flexible NetFlow MPLS Support

Example: Configuring Flexible NetFlow for MPLS Support

The following example shows how to configure a flow monitor using the Flexible NetFlow "BGP ToS next-hop" predefined record to monitor IPv4 traffic.

This sample starts in global configuration mode:

```
Router(config)#flow record mpls_1
Router(config-flow-record)#match mpls label 1 details
Router(config-flow-record)#match mpls label 1 exp
Router(config-flow-record)#match mpls label 1 ttl
Router(config-flow-record)#match mpls label 2 details
Router(config-flow-record)#match mpls label 3 details
Router(config-flow-record)#collect mpls label 4 details
Router(config-flow-record)#collect mpls label 5 details
!
flow monitor mpls_1
```

```

record mpls_1
!
interface Ethernet 0/0
 mpls flow monitor mpls_1 input
 mpls flow monitor mpls_1 output
!

```

Additional References

Related Documents

| Related Topic | Document Title |
|---|---|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow conceptual information and configuration tasks | <i>Flexible NetFlow Configuration Guide</i> |
| Flexible NetFlow commands | <i>Cisco IOS Flexible NetFlow Command Reference</i> |

Standards/RFCs

| Standard | Title |
|--|-------|
| No new or modified standards/RFCs are supported by this feature. | — |

MIBs

| MIB | MIBs Link |
|------|---|
| None | To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs |

Technical Assistance

| Description | Link |
|---|---|
| The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password. | http://www.cisco.com/cisco/web/support/index.html |

Feature Information for Flexible NetFlow: MPLS Support

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 34: Feature Information for Flexible NetFlow: MPLS Support

| Feature Name | Releases | Feature Information |
|--------------------------------|---------------------------|---|
| Flexible NetFlow: MPLS Support | Cisco IOS XE Release 3.9S | Enables collecting MPLS label IDs by applying a flow monitor having a flow record that collects the MPLS label IDs as key or nonkey fields. The following commands were introduced or modified: collect mplslabel, match mplslabel, mpls flow monitor. |



CHAPTER 18

Flexible NetFlow—Prevent Export Storms

The Flexible NetFlow—Prevent Export Storms feature uses export spreading to prevent export storms that occur due to the creation of a synchronized cache. The export of the previous interval is spread during the current interval to prevent export storms.

- [Finding Feature Information, on page 199](#)
- [Information About Flexible NetFlow—Prevent Export Storms, on page 199](#)
- [How to Configure Flexible NetFlow—Prevent Export Storms, on page 200](#)
- [Configuration Examples for Flexible NetFlow—Prevent Export Storms, on page 201](#)
- [Additional References for Flexible NetFlow—Prevent Export Storms, on page 202](#)
- [Feature Information for Flexible NetFlow—Prevent Export Storms, on page 202](#)

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.

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

Information About Flexible NetFlow—Prevent Export Storms

Flexible NetFlow—Prevent Export Storms Overview

The Flexible NetFlow—Prevent Export Storms feature prevents export storms at a NetFlow Collecting (NFC) device, especially when multiple Flexible NetFlow (FNF) entities are configured to export FNF records to the same NFC at the same synchronized wallclock time. Export storms occur due to the creation of the synchronized cache type. Export spreading reduces the severity of export storms and mitigates their impact.

Synchronized cache with spreading requires adding the interval timestamp field for the synchronized cache. When no spreading is configured, it is recommended to add the interval as a key, but the configuration is not rejected to maintain backward compatibility. If no export spread is specified, the default behavior is immediate export. The spread time must be smaller than half of the interval. Therefore, it will be set to half the interval time or to the configured spread interval, whichever is lower (but not lower than 1 second).

You must not enable spreading when the interval sync timeout is lower than 10 seconds (5-second spreading). This requirement comes from the need for asynchronous monitors to aggregate the data within a few seconds. Spreading might start a couple of seconds after the interval ends in order to complete the aggregation. If a synchronized interval value is lower than 10 seconds, no spreading option is visible in the command-line interface (CLI). The default spread interval, if unspecified, is 30 seconds. The maximum synchronized interval timeout value is 300 seconds. For native FNF monitors, the maximum synchronized interval timeout value could be larger. The rate calculation is provisioned as follows:

- The simple implementation is a constant rate based on the cache-size/spread-interval.
- An improved implementation is based on the current-previous-interval-cache-size/spread-interval. This provides better results when the cache is not full.

The NetFlow/IPFIX header timestamp is set to the time when the record leaves the device (and not when the record leaves the NetFlow cache). The timestamp fields in the record itself capture the timestamp of the packets and are accounted for in the NetFlow cache. A new, implementation-driven concept of a “small interval” is now implicitly introduced and understood to be directly in contrast with the concept of a “large interval”. The “large interval” can be thought of as simply the sync interval as configured by the CLI. This is the interval at the beginning of which the entire export process is to be initiated. It corresponds to the “synchronized interval” that is driven and defined by the CLI. At the beginning of a “large interval”, we must take the number of records in the cache and divide that number by the number of seconds available in which to export these records, thus yielding the calculated or derived quantity of “records per second”.

For example, if there are 100,000 records in the cache and 100 seconds in which to export these records, we would calculate and store the value 1000 records/second. Because this quantity is expressed in seconds, it follows that we will need to count the records exported in small intervals that are one second in duration.

This then, implicitly, defines the notion of a “small interval”, which is, to be succinct and equal to one second. Combining this idea of small and large intervals with the need for a state or context, it quickly becomes evident that a timer thread must be able to discern if it is beginning a “small interval” or a “large interval”.

How to Configure Flexible NetFlow—Prevent Export Storms

Configuring Flexible NetFlow—Prevent Export Storms

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow monitor type performance-monitor** *monitor-name*
4. **cache type synchronized**
5. **cache timeout synchronized** *interval* **export-spread** *spread-interval*
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|----------------------------------|---|
| Step 1 | enable Example: | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |

| | Command or Action | Purpose |
|--------|--|--|
| | Device> enable | |
| Step 2 | configure terminal Example: Device# configure terminal | Enters global configuration mode. |
| Step 3 | flow monitor type performance-monitor <i>monitor-name</i> Example: Device(config)# flow monitor type performance-monitor my_mon | Creates a flow monitor and enters flow monitor configuration mode. • This command also allows you to modify an existing flow monitor. |
| Step 4 | cache type synchronized Example: Device(config-flow-monitor)# cache type synchronized | Configures the cache type for a Performance Monitor flow monitor. |
| Step 5 | cache timeout synchronized <i>interval</i> export-spread <i>spread-interval</i> Example: Device(config-flow-monitor)# cache timeout synchronized 12 export-spread 5 | Configures export spreading. |
| Step 6 | end Example: Device(config-flow-monitor)# end | Returns to privileged EXEC mode. |

Configuration Examples for Flexible NetFlow—Prevent Export Storms

Example: Flexible NetFlow—Prevent Export Storms Configuration

The following example shows how to enable and configure export spreading and prevent export storms where the synchronized interval timeout value is 12 seconds and the export spread interval is 5 seconds:

```
Device> enable
Device# configure terminal
Device(config)# flow monitor type performance-monitor my_mon
Device(config-flow-monitor)# cache type synchronized
Device(config-flow-monitor)# cache timeout synchronized 12 export-spread 5
```

Additional References for Flexible NetFlow—Prevent Export Storms

Related Documents

| Related Topic | Document Title |
|---------------------------|--|
| Cisco IOS commands | Cisco IOS Master Command List, All Releases |
| Flexible NetFlow commands | Cisco IOS Flexible NetFlow Command Reference |

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—Prevent Export Storms

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

| Feature Name | Releases | Feature Information |
|--|----------------------------|---|
| Flexible NetFlow - Prevent Export Storms | Cisco IOS XE Release 3.11S | The Flexible NetFlow—Prevent Export Storms feature uses export spreading to prevent export storms that occur due to the creation of a synchronized cache. The export of the previous interval is spread during the current interval to prevent export storms. |