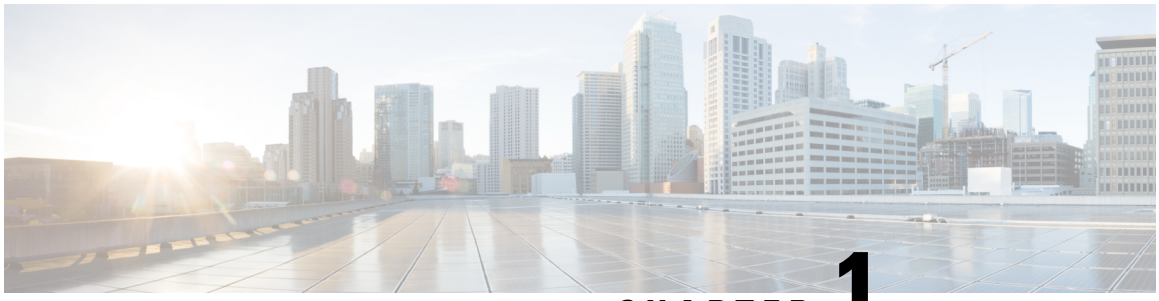
Flexible Netflow Configuration Guide, Cisco IOS Release 15SY

First Published: 2012-11-26

Last Modified: 2012-11-26

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

CONTENTS



CHAPTER 1

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

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

- 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.
- 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.
- Flexible NetFlow does not monitor PPPoE traffic flowing through a Catalyst 6500 Series switch with Supervisor Engine 2T.
- Flow Monitor applied on a VLAN configuration collects layer 2 passing traffic only. To collect inter-VLAN traffic or traffic destined Switch Virtual Interface (SVI), flow monitor needs to be configured on SVI.

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

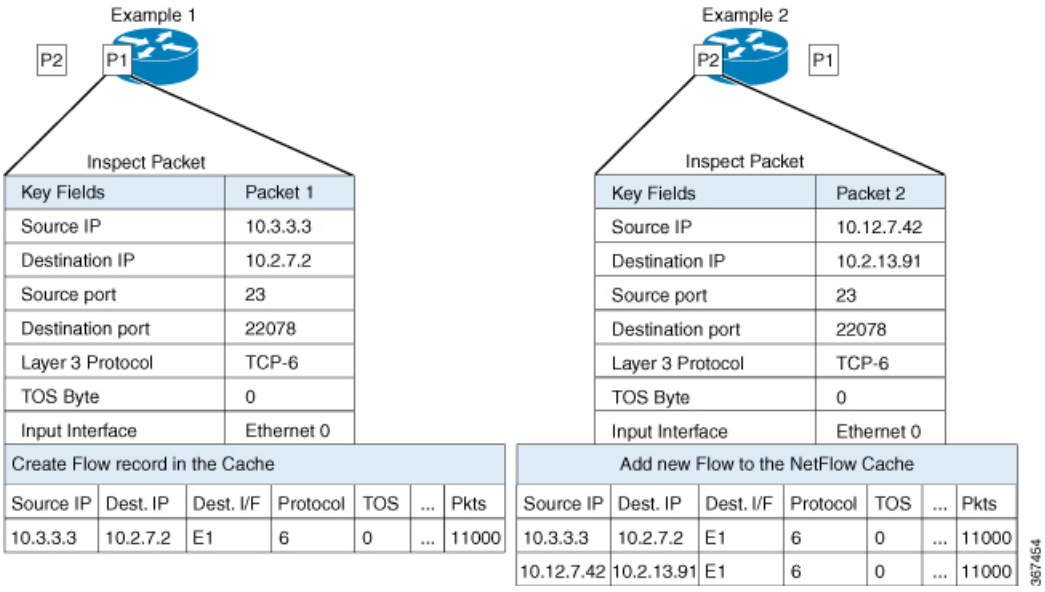
Original NetFlow and Flexible NetFlow both use the concept of flows. A *flow* is defined as a stream of packets between a given source and a given destination.

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

Original NetFlow uses a fixed seven tuples of IP information to identify a flow.

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 and version 10 export formats. With version 10 export format, support for variable length field for the wireless client's SSID is available.
- 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.

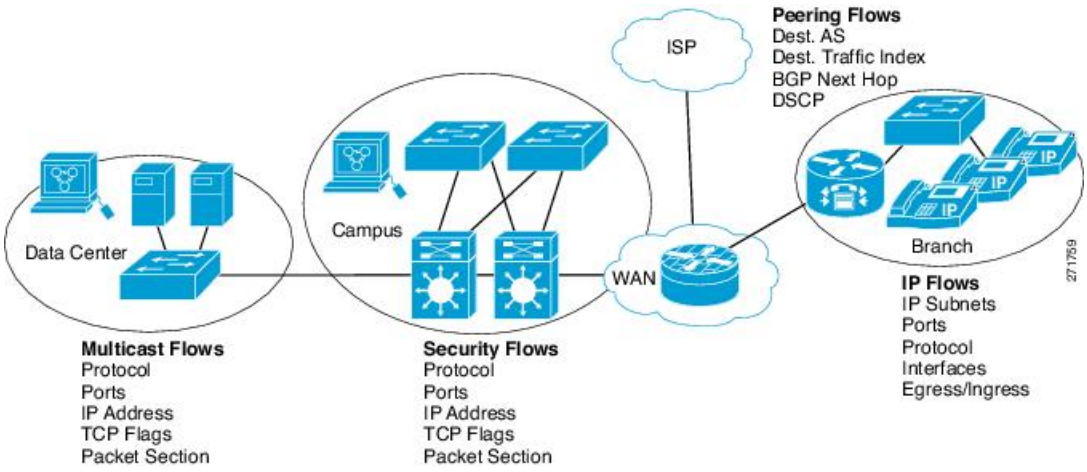
Original NetFlow allows you to understand the activities in the network and thus to optimize network design and reduce operational costs.

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:

Note Starting from Cisco IOS XE Release 3.10S, the number of configurable flow record fields have been increased from 32 to 40.

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.

You can create user-defined records for applications such as QoS and bandwidth monitoring, application and end user traffic profiling, and security monitoring for dDoS attacks. Flexible NetFlow also includes several predefined records that emulate original NetFlow. Flexible NetFlow user-defined records provide the capability to monitor a contiguous section of a packet of a user-configurable size, and use it in a flow record as a key or a nonkey field along with other fields and attributes of the packet. The section may include any Layer 3 data

from the packet. The packet section fields allow the user to monitor any packet fields that are not covered by the Flexible NetFlow predefined keys. The ability to analyze packet fields that are not collected with the predefined keys enables more detailed traffic monitoring, facilitates the investigation of dDoS attacks, and enables implementation of other security applications such as URL monitoring.

Flexible NetFlow provides predefined types of packet sections of a user-configurable size. The following Flexible NetFlow commands (used in Flexible NetFlow flow record configuration mode) can be used to configure the predefined types of packet sections:

- **collect ipv4 section header size** *bytes* --Starts capturing the number of bytes specified by the *bytes*argument from the beginning of the IPv4 header of each packet.
- **collect ipv4 section payload size** *bytes* --Starts capturing bytes immediately after the IPv4 header from each packet. The number of bytes captured is specified by the *bytes* argument.
- **collect ipv6 section header size** *bytes* --Starts capturing the number of bytes specified by the *bytes*argument from the beginning of the IPv6 header of each packet.
- **collect ipv6 section payload size** *bytes* --Starts capturing bytes immediately after the IPv6 header from each packet. The number of bytes captured is specified by the *bytes* argument.

The *bytes* values are the sizes in bytes of these fields in the flow record. If the corresponding fragment of the packet is smaller than the requested section size, Flexible NetFlow will fill the rest of the section field in the flow record with zeros. If the packet type does not match the requested section type, Flexible NetFlow will fill the entire section field in the flow record with zeros.

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.

Note In Cisco IOS Release 12.2(50)SY, packet sections and payloads are not supported.

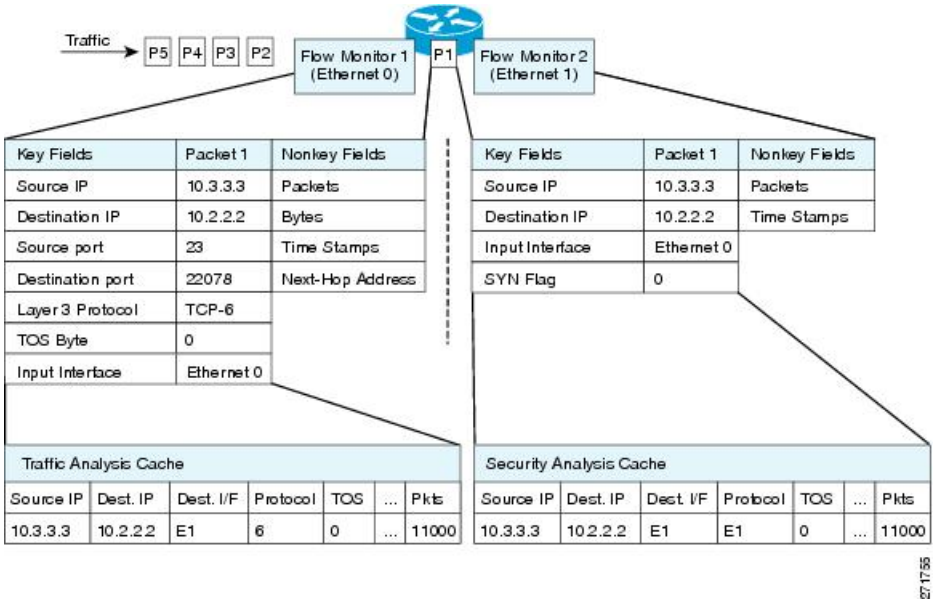
Flow Monitors

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.

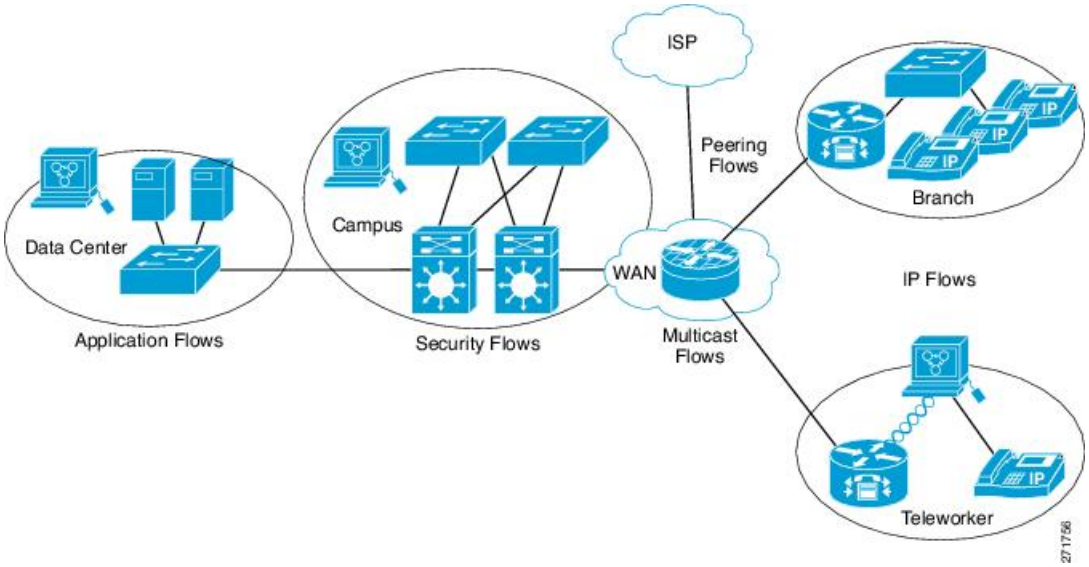
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

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



There are three types of flow monitor caches. You change the type of cache used by the flow monitor after you create the flow monitor. The three types of flow monitor caches are described in the following sections:

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.

Immediate

A cache of type "immediate" ages out every record as soon as it is created. As a result, every flow contains just one packet. The commands that display the cache contents will provide a history of the packets seen.

This mode is desirable when you expect only very small flows and you want a minimum amount of latency between seeing a packet and exporting a report.

Caution This mode may result in a large amount of export data that can overload low-speed links and overwhelm any systems that you are exporting to. We recommended that you configure sampling to reduce the number of packets that are processed.

Note The cache timeout settings have no effect in this mode.

Permanent

A cache of type "permanent" never ages out any flows. A permanent cache is useful when the number of flows you expect to see is low and there is a need to keep long-term statistics on the router. For example, if the only key field in the flow record is the 8-bit IP ToS field, only 256 flows can be monitored. To monitor the long-term usage of the IP ToS field in the network traffic, you can use a permanent cache. Permanent caches are useful for billing applications and for an edge-to-edge traffic matrix for a fixed set of flows that are being tracked. Update messages will be sent periodically to any flow exporters configured according to the "timeout update" setting.

Note When a cache becomes full in permanent mode, new flows will not be monitored. If this occurs, a "Flows not added" message will appear in the cache statistics.

Note A permanent cache uses update counters rather than delta counters. This means that when a flow is exported, the counters represent the totals seen for the full lifetime of the flow and not the additional packets and bytes seen since the last export was sent.

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

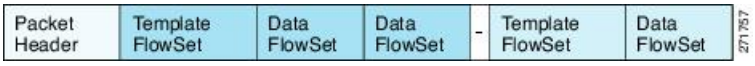
The basic output of NetFlow is a flow record. Several different formats for flow records have evolved as NetFlow has matured. The most recent evolution of the NetFlow export format is known as Version 9. The distinguishing feature of the NetFlow Version 9 export format is that it is template-based. Templates 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.

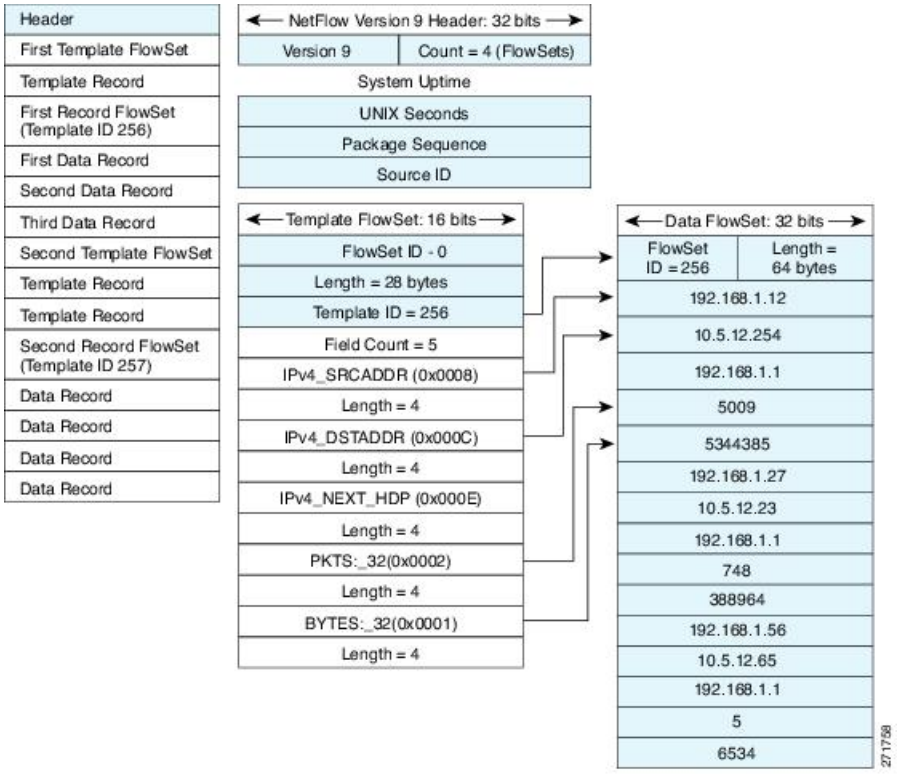
The Version 9 export format consists of a packet header followed by one or more template flow or data flow sets. A template flow set provides a description of the fields that will be present in future data flow sets. These data flow sets may occur later within the same export packet or in subsequent 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, 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 to 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 49 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 Customized 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** *record-name* **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** *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`	Configures a key field for the flow record. **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`	**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** command, and the other **match** commands that are available to configure key fields.

	Command or Action	Purpose
	`Device(config-flow-record)# match flow cts destination group-tag`	**Note** • Ingress: • 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: • 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	**collect interface** {**input** | **output**} **Example:** `Device(config-flow-record)# collect interface input`	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:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 11	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.
Step 12	**show running-config flow record** *record-name* **Example:**	(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.

SUMMARY STEPS

1. **enable**
2. **show flow 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 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.

SUMMARY STEPS

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


!
```

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. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **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** *description* **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.

	Command or Action	Purpose
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**] *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.
Step 8	**show running-config flow monitor** *monitor-name* **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. • Enter your password if prompted.
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 a flow exporter and enters Flexible NetFlow flow exporter configuration mode. • This command also allows you to modify an existing flow exporter.
Step 4	**description** *description* **Example:** `Device(config-flow-exporter)# description Exports to datacenter`	(Optional) Creates a description for the flow exporter.
Step 5	**destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*] **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. • Default: **netflow-v9**.
Step 7	**transport udp** *udp-port* **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.

	Command or Action	Purpose
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** *flow-monitor-name* **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** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	Specifies the name of an exporter that you created previously.
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** *exporter-name* **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** *exporter-name* **Example:** `Device<# show running-config flow exporter FLOW_EXPORTER-1`	(Optional) Displays the configuration of the specified flow exporter.

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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> 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** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.

	Command or Action	Purpose
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. 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	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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

    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

  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

  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
```

```
!
```

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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip**	**ipv6**} **flow monitor** *monitor-name* {**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.	—

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 7	**show flow interface** *type number* **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** *monitor-name* **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.

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:

```
!
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.

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 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
 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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

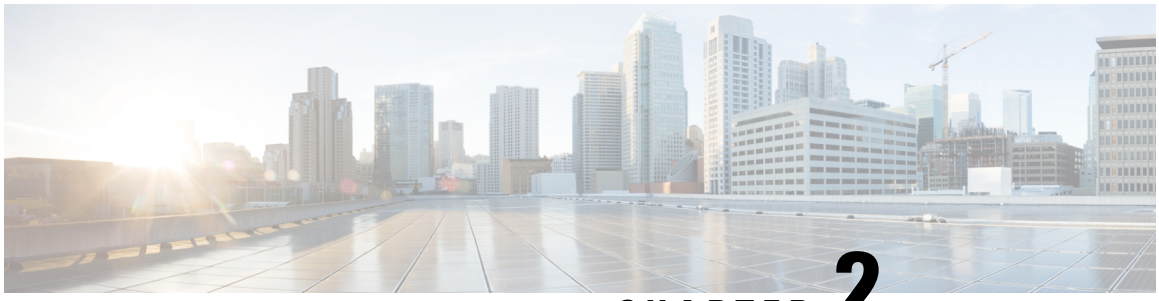
Feature Information for Flexible NetFlow

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	Flexible NetFlow is introduced. 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: **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).



CHAPTER 2

Flexible NetFlow—IPv4 Unicast Flows

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

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 Customized 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** *record-name* **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** *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:**	Configures a key field for the flow record.

	Command or Action	Purpose
	`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** command, and the other **match** commands that are available to configure key fields.
		Note
		• Ingress:
		• 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:
		• 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	**collect interface** {**input** | **output**} **Example:** `Device(config-flow-record)# collect interface input`	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.

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

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. **dscp** *dscp*
7. **source** *interface-type interface-number*
8. **output-features**
9. **template data timeout** *seconds*
10. **transport udp** *udp-port*
11. **ttl** *seconds*
12. **end**
13. **show flow exporter** *exporter-name*
14. **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** *exporter-name* **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.
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	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 7	**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 8	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 9	**template data timeout** *seconds* **Example:**	(Optional) Configures resending of templates based on a timeout.

	Command or Action	Purpose
	`Device(config-flow-exporter)# template data timeout 120`	• The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 10	**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. • The range for the *udp-port* argument is from 1 to 65536.
Step 11	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 12	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 13	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 14	**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.

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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> 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** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.

	Command or Action	Purpose
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. 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	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip**	**ipv6**} **flow monitor** *monitor-name* {**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** *type number* **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** *monitor-name* **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. • 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** *monitor-name* **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** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6** *record* [**peer**] }] **Example:** `Device(config-flow-monitor)# record netflow ipv4 original-input`	Specifies the record for the flow monitor.
Step 5	**exporter** *exporter-name* **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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 8	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**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 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
```

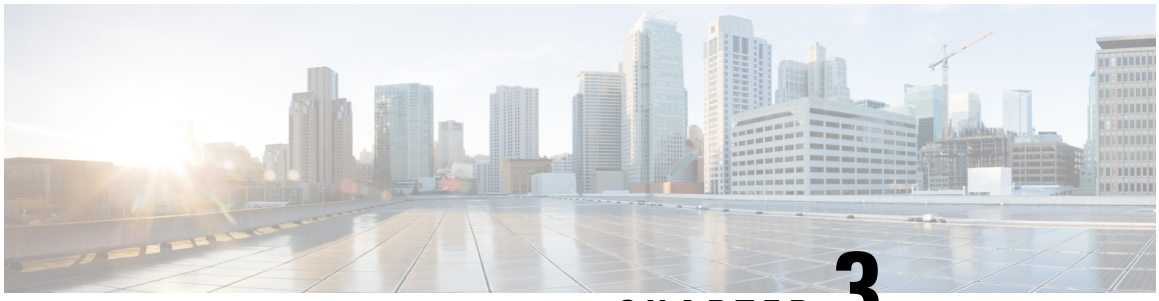
Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

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
!
```



CHAPTER 3

Flexible NetFlow—IPv6 Unicast Flows

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

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 Customized 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** *record-name* **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** *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:**	Configures a key field for the flow record.

	Command or Action	Purpose
	`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** command, and the other **match** commands that are available to configure key fields.
		Note
		• Ingress:
		• 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:
		• 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	**collect interface** {**input** | **output**} **Example:** `Device(config-flow-record)# collect interface input`	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.

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

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. **dscp** *dscp*
7. **source** *interface-type interface-number*
8. **output-features**
9. **template data timeout** *seconds*
10. **transport udp** *udp-port*
11. **ttl** *seconds*
12. **end**
13. **show flow exporter** *exporter-name*
14. **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** *exporter-name* **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.
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	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 7	**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 8	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 9	**template data timeout** *seconds* **Example:**	(Optional) Configures resending of templates based on a timeout.

	Command or Action	Purpose
	`Device(config-flow-exporter)# template data timeout 120`	• The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 10	**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. • The range for the *udp-port* argument is from 1 to 65536.
Step 11	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 12	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 13	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 14	**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.

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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> 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** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.

	Command or Action	Purpose
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. 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	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip**	**ipv6**} **flow monitor** *monitor-name* {**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** *type number* **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** *monitor-name* **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. • 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** *monitor-name* **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** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6** *record* [**peer**] }] **Example:** `Device(config-flow-monitor)# record netflow ipv4 original-input`	Specifies the record for the flow monitor.
Step 5	**exporter** *exporter-name* **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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 8	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**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 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
```

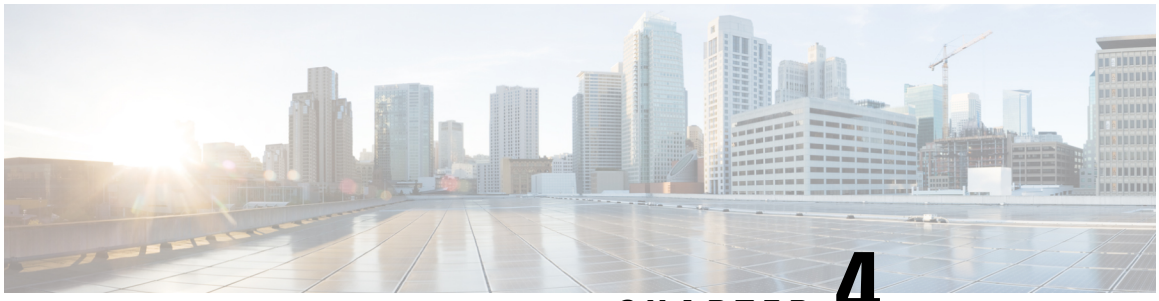
Example: Configuring Flexible NetFlow Egress Accounting for IPv4 and IPv6 Traffic

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
!
```



CHAPTER 4

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

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.

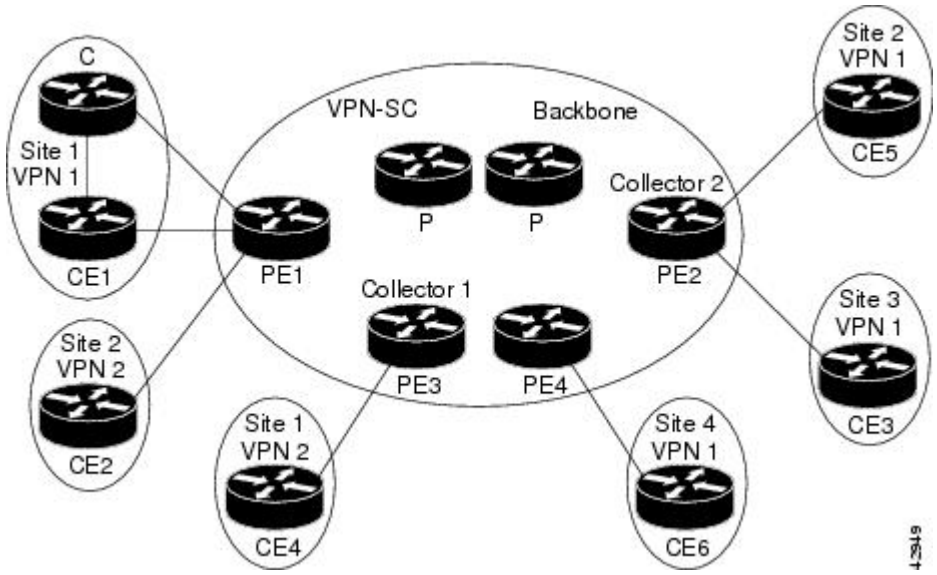
The figure below shows a sample MPLS VPN network topology that includes four VPN 1 sites and two VPN 2 sites. If the Flexible NetFlow - MPLS Egress NetFlow is enabled on an outgoing PE interface by applying

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. • 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** *exporter-name* **Example:** `Device(config)# flow exporter EXPORTER-1`	Creates a flow exporter and enters Flexible NetFlow flow exporter configuration mode. • This command also allows you to modify an existing flow exporter.
Step 4	**description** *description* **Example:** `Device(config-flow-exporter)# description Exports to datacenter`	(Optional) Creates a description for the flow exporter.
Step 5	**destination** {*hostname* | *ip-address*} [**vrf** *vrf-name*] **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. • Default: **netflow-v9**.
Step 7	**transport udp** *udp-port* **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** *flow-monitor-name* **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** *exporter-name* **Example:**	Specifies the name of an exporter that you created previously.

	Command or Action	Purpose
	`Device(config-flow-monitor)# exporter EXPORTER-1`	
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** *exporter-name* **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** *exporter-name* **Example:** `Device<# show running-config flow exporter FLOW_EXPORTER-1`	(Optional) Displays the configuration of the specified flow exporter.

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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> 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** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. 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.	—

	Command or Action	Purpose
Step 8	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**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** *type number* **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** *monitor-name* **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 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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

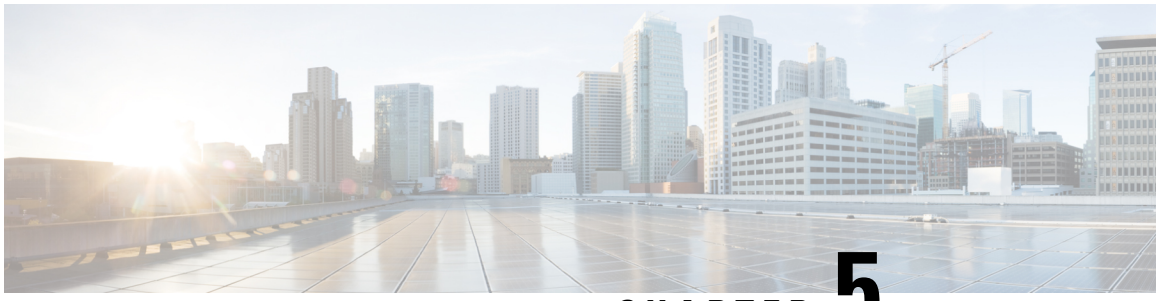
Feature Information for Flexible NetFlow - MPLS Egress NetFlow

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 20: 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 5

Flexible NetFlow v9 Export Format

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

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.

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. **dscp** *dscp*
7. **source** *interface-type interface-number*
8. **output-features**
9. **template data timeout** *seconds*
10. **transport udp** *udp-port*
11. **ttl** *seconds*
12. **end**
13. **show flow exporter** *exporter-name*
14. **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** *exporter-name* **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.
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	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 7	**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 8	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 9	**template data timeout** *seconds* **Example:**	(Optional) Configures resending of templates based on a timeout.

	Command or Action	Purpose
	`Device(config-flow-exporter)# template data timeout 120`	• The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 10	**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. • The range for the *udp-port* argument is from 1 to 65536.
Step 11	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 12	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 13	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 14	**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 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*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

Standards

Standard	Title
None	—

MIBs

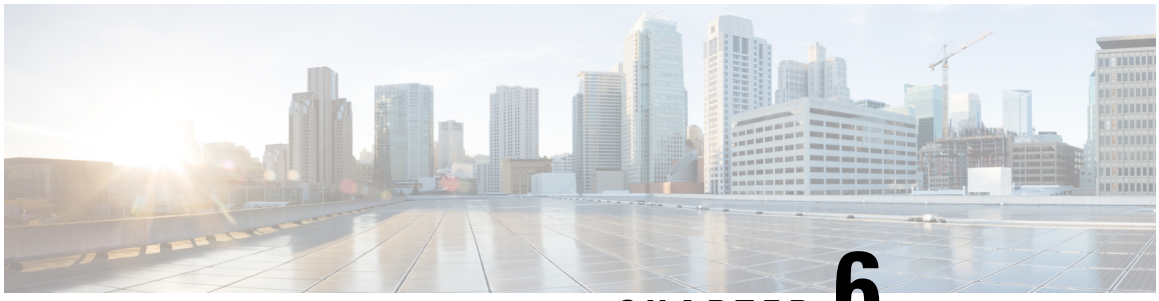
MIB	MIBs Link
None	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html



CHAPTER 6

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

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.

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. **dscp** *dscp*
7. **source** *interface-type interface-number*
8. **output-features**
9. **template data timeout** *seconds*
10. **transport udp** *udp-port*
11. **ttl** *seconds*
12. **end**
13. **show flow exporter** *exporter-name*
14. **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.

	Command or Action	Purpose
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. • 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	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 7	**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 8	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 9	**template data timeout** *seconds* **Example:** `Device(config-flow-exporter)# template data timeout 120`	(Optional) Configures resending of templates based on a timeout. • The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 10	**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. • The range for the *udp-port* argument is from 1 to 65536.

	Command or Action	Purpose
Step 11	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 12	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 13	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 14	**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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

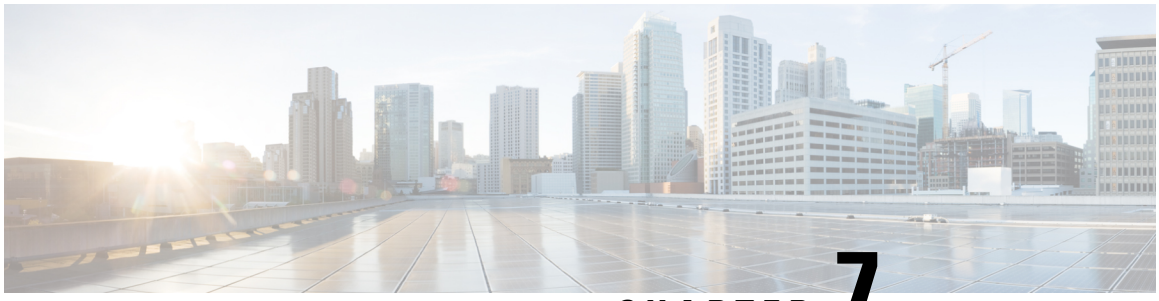
Feature Information for Flexible NetFlow NetFlow V5 Export Protocol

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 21: 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 7

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

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** *monitor-name* **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** *description* **Example:** `Device(config-flow-monitor)# description Used for basic traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **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.

Configuring and Enabling Flow Sampling

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

Note When you specify the "NetFlow original," or the "NetFlow IPv4 original input," or the "NetFlow IPv6 original input" predefined record for the flow monitor to emulate original NetFlow, the flow monitor can be used only for analyzing input (ingress) traffic.

When you specify the "NetFlow IPv4 original output" or the "NetFlow IPv6 original output" predefined record for the flow monitor to emulate the Egress NetFlow Accounting feature, the flow monitor can be used only for analyzing output (egress) traffic.

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** *sampler-name* **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** *description* **Example:** `Device(config-sampler)# description Sample at 50%`	(Optional) Creates a description for the flow sampler.
Step 5	**mode** {**random**} **1 out-of** *window-size* **Example:**	Specifies the sampler mode and the flow sampler window size.

	Command or Action	Purpose
	`Device(config-sampler)# mode random 1 out-of 2`	• The range for the *window-size* argument is from 2 to 32768.
Step 6	**exit** **Example:** `Device(config-sampler)# exit`	Exits sampler configuration mode and returns to global configuration mode.
Step 7	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 8	{**ip** | **ipv6**} **flow monitor** *monitor-name* [[**sampler**] *sampler-name*] {**input** | **output**} **Example:** `Device(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input`	Assigns the flow monitor and the flow sampler that you created to the interface to enable sampling.
Step 9	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 10	**show sampler sampler-name** **Example:** `Device# show sampler SAMPLER-1`	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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

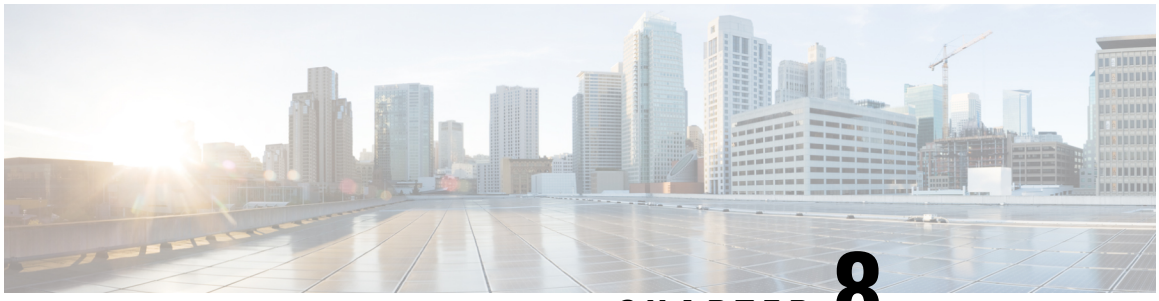
Feature Information for Flexible NetFlow Flow Sampling

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 22: 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 8

Configuring IPv4 Multicast Statistics Support for Flexible NetFlow

This document contains information about and instructions for configuring the Cisco IOS Flexible NetFlow - IPv4 Multicast Statistics Support feature. Prior to the introduction of the Flexible NetFlow - IPv4 Multicast Statistics Support feature, Flexible NetFlow could analyze IPv4 multicast traffic, but could not report the number of replicated bytes or the number of replicated packets in multicast flows. The Flexible NetFlow - IPv4 Multicast Statistics Support feature adds the capability of reporting the number of replicated bytes and the number of replicated packets in multicast flows to Flexible NetFlow.

NetFlow is a Cisco IOS technology that provides statistics on packets flowing through a networking device. NetFlow is the standard for acquiring IP operational data from IP networks. NetFlow provides 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

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 Configuring IPv4 Multicast Statistics Support

- The networking device is running a Cisco IOS release that supports the Flexible NetFlow--IPv4 Multicast Statistics Support feature.
- The networking device is configured for IPv4 unicast routing and IPv4 multicast routing.
- One of the following is enabled on your networking device and on any interfaces on which you want to enable Flexible NetFlow: Cisco Express Forwarding, distributed Cisco Express Forwarding.

Restrictions for Configuring IPv4 Multicast Statistics Support

IPv4 Traffic

- When the replication-factor field is used in a flow record, it will only have a nonzero value in the cache for ingress multicast traffic that is forwarded by the router. If the flow record is used with a flow monitor in output (egress) mode and to monitor unicast traffic, the cache data for the replication factor field is set to 0.

IPv6 Traffic

- Traffic monitoring for multicast statistics is not supported.

Note The**match routing multicast replication-factor** command is not supported on ASR and ISR platforms.

Information About IPv4 Multicast Statistics Support

Replicated Bytes and Packets Reporting

The Flexible NetFlow--IPv4 Multicast Statistics Support feature adds the capability of reporting the number of replicated bytes and the number of replicated packets in multicast flows to Flexible NetFlow. You can capture the packet-replication factor for a specific flow and for each outgoing stream.

You can use the The Flexible NetFlow--IPv4 Multicast Statistics Support feature to identify and count multicast packets on the ingress side or the egress side (or both sides) of a networking device. Multicast ingress accounting provides information about the source and how many times the traffic was replicated. Multicast egress accounting monitors the destination of the traffic flow.

How to Configure IPv4 Multicast Statistics Support

Configuring IPv4 Multicast Statistics Support

This task explains the steps that are used to configure multicast statistics support for IPv4 traffic.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *flow-record-name*
4. **description** *description*
5. **match routing is-multicast**
6. Add key fields for the record as required using other **match** commands.
7. **collect counter** {**bytes replicated** [**long**] | **packets replicated** [**long**]}
8. **collect routing multicast replication-factor**
9. Add nonkey fields for the record as required using other **collect** commands.
10. **exit**
11. **flow monitor** *monitor-name*
12. **description** *description*
13. **record** *record-name*
14. **exit**
15. **interface** *type number*
16. **ip flow monitor** *monitor-name* [**multicast** | **unicast**] {**input** | **output**}
17. Repeat Steps 15 and 16 to activate a flow monitor on any other interfaces in the networking device over which you want to monitor traffic.
18. **end**
19. **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 record** *flow-record-name* **Example:**	Creates a flow record and enters Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
	`Device(config)# flow record FLOW-RECORD-2`	• This command also allows you to modify an existing flow record.
Step 4	**description** *description* **Example:** `Device(config-flow-record)# description Used for IPv4 multicast traffic analysis`	(Optional) Creates a description for the flow record.
Step 5	**match routing is-multicast** **Example:** `Device(config-flow-record)# match routing is-multicast`	Configures IPv4 multicast destination addresses (indicating that the IPv4 traffic is multicast traffic) as a key field for the flow record.
Step 6	Add key fields for the record as required using other **match** commands.	For information about the other **match** commands that are available to configure key fields, refer to the *Cisco IOS Flexible NetFlow Command Reference*.
Step 7	**collect counter** {**bytes replicated** [**long**] | **packets replicated** [**long**]} **Example:** `Device(config-flow-record)# collect counter packets replicated`	Configures the number of bytes or packets multiplied by the multicast replication factor (number of interfaces the multicast traffic is forwarded over) as a nonkey field. • Default: Uses a 32-bit counter. The **long** keyword configures a 64-bit counter.
Step 8	**collect routing multicast replication-factor** **Example:** `Device(config-flow-record)# collect routing multicast replication-factor`	Configures the multicast replication factor (number of interfaces over which multicast traffic is forwarded) as a nonkey field.
Step 9	Add nonkey fields for the record as required using other **collect** commands.	For information about the other **collect** commands that are available to configure nonkey fields, refer to the *Cisco IOS Flexible NetFlow Command Reference*.
Step 10	**exit** **Example:** `Device(config-flow-record)# exit`	Exits Flexible NetFlow flow record configuration mode and returns to global configuration mode.
Step 11	**flow monitor** *monitor-name* **Example:** `Device(config)# flow monitor FLOW-MONITOR-2`	Creates a flow monitor and enters Flexible NetFlow flow monitor configuration mode. • This command also allows you to modify an existing flow monitor.
Step 12	**description** *description* **Example:**	(Optional) Creates a description for the flow monitor.

	Command or Action	Purpose
	`Device(config-flow-monitor)# description Used for IPv4 multicast traffic analysis`	
Step 13	**record** *record-name* **Example:** `Device(config-flow-monitor)# record FLOW-RECORD-2`	Specifies the record for the flow monitor.
Step 14	**exit** **Example:** `Device(config-flow-record)# exit`	Exits Flexible NetFlow flow monitor configuration mode and returns to global configuration mode.
Step 15	**interface** *type number* **Example:** `Device(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 16	**ip flow monitor** *monitor-name* [**multicast** | **unicast**] {**input** | **output**} **Example:** `Device(config-if)# ip flow monitor FLOW-MONITOR-2 input`	Activates the flow monitor that was created previously by assigning it to the interface to analyze traffic. • To monitor only multicast traffic, use the **multicast** keyword. • Default: Unicast traffic and multicast traffic are monitored.
Step 17	Repeat Steps 15 and 16 to activate a flow monitor on any other interfaces in the networking device over which you want to monitor traffic.	--
Step 18	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 19	**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.

Examples

The following output from the **show flow monitor** command shows four multicast flows and three unicast flows:

```
Device# show flow monitor FLOW-MONITOR-2 cache

Cache type:                               Normal
  Cache size:                               4096
  Current entries:                             8
  High Watermark:                              8
  Flows added:                              4074
  Flows aged:                               4066
    - Active timeout   (  1800 secs)          46
    - Inactive timeout (    15 secs)        4020
    - Event aged                                0
    - Watermark aged                            0
    - Emergency aged                            0
IP IS MULTICAST  IPV4 DST ADDR      pkts rep
===============  ===============  ==========
Yes              224.192.16.1          16642
Yes              224.192.65.1          16621
No               10.1.4.2                  0
No               10.1.2.2                  0
No               10.1.3.2                  0
Yes              224.0.0.13                0
No               255.255.255.255           0
Yes              224.0.0.1                 0
```

Configuration Examples for IPv4 Multicast Statistics Support

Example: Configuring IPv4 Multicast Statistics Support

This example shows how to configure the following:

- IPv4 multicast destination addresses (indicating that the IPv4 traffic is multicast traffic) as a key field.
- The destination IPv4 address as a key field.
- The replicated packet count as a nonkey field.
- The replication factor as a nonkey field.
- The flow monitor in order to monitor only multicast traffic.

This sample starts in global configuration mode:

```
!
flow record FLOW-RECORD-2
 match routing is-multicast
 match ipv4 destination address
 collect counter packets replicated
 collect routing multicast replication-factor
 exit
!
flow monitor FLOW-MONITOR-2
 record FLOW-RECORD-2
 exit
!
interface GigabitEthernet 0/0/0
 no shut
 ip address 10.1.1.2 255.255.255.0
```

```
 ip flow monitor FLOW-MONITOR-2 multicast 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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

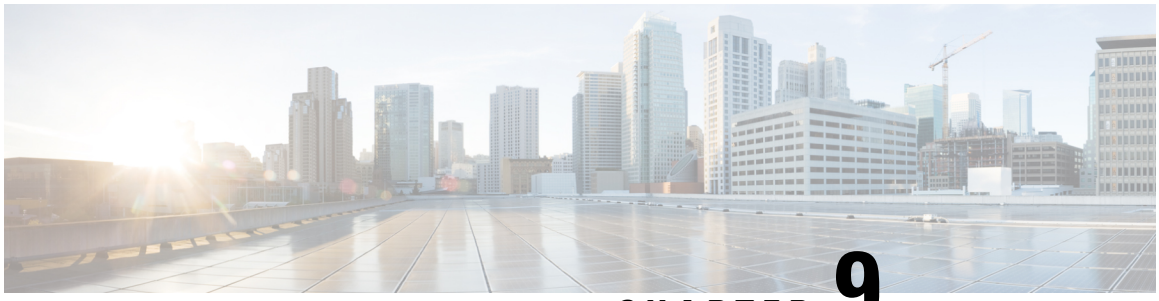
Feature Information for IPv4 Multicast Statistics Support

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 23: Feature Information for Flexible NetFlow --IPv4 Multicast Statistics Support

Feature Name	Releases	Feature Information
Flexible NetFlow--IPv4 Multicast Statistics Support	12.2(33)SRE 12.2(50)SY 12.4(22)T	The Flexible NetFlow--IPv4 Multicast Statistics Support feature adds the capability of reporting the number of replicated bytes and the number of replicated packets in multicast flows to Flexible NetFlow. 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 counter**, **collect routing is-multicast**, **collect routing multicast replication-factor**, **match routing is-multicast**, **match routing multicast replication-factor**, **ip flow monitor**, **ipv6 flow monitor**.



CHAPTER 9

Flexible NetFlow - Top N Talkers Support

This document contains information about and instructions for using the Flexible NetFlow - Top N Talkers Support feature. The Flexible NetFlow - Top N Talkers Support feature helps you analyze the large amount of data that Flexible NetFlow captures from the traffic in your network by providing the ability to filter, aggregate, and sort the data in the Flexible NetFlow cache as you display it. When you are sorting and displaying the data in the cache, you can limit the display output to a specific number of entries with the highest values (Top N Talkers) for traffic volume, packet counters, and so on. The Flexible NetFlow - Top N Talkers Support feature facilitates real-time traffic analysis by requiring only the use of **show** commands, which can be entered in many different variations using the available keywords and arguments to meet your traffic data analysis requirements.

NetFlow is a Cisco 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 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

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 - Top N Talkers Support

- The networking device is running a Cisco release that supports the Flexible NetFlow - Top N Talkers Support feature.

No configuration tasks are associated with the Flexible NetFlow - Top N Talkers Support feature. Therefore, in order for you to use the Flexible NetFlow - Top N Talkers Support feature, traffic analysis with Flexible NetFlow must already be configured on the networking device.

Information About Flexible NetFlow - Top N Talkers Support

Flexible NetFlow Data Flow Filtering

The flow filtering function of the Flexible NetFlow - Top N Talkers Support feature filters the flow data in a flow monitor cache based on the criteria that you specify, and displays the data.

The flow filtering function of the Flexible NetFlow - Top N Talkers Support feature is provided by the **show flow monitor cache filter** command. For more information on the **show flow monitor cache filter** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Flow Sorting and Top N Talkers

The flow sorting function of the Flexible NetFlow - Top N Talkers Support feature sorts flow data from the Flexible NetFlow cache based on the criteria that you specify and displays the data. You can also use the flow sorting function of the Flexible NetFlow - Top N Talkers Support feature to limit the display output to a specific number of entries (top *n* talkers, where *n* is the number or talkers to display) by using the **top** keyword of the **show flow monitor cache sort** command.

The flow sorting and Top N Talkers function of the Flexible NetFlow - Top N Talkers Support feature is provided by the **show flow monitor cache sort** command. For more information on the **show flow monitor cache sort** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Combined Use of Flow Filtering and Flow Sorting with Top N Talkers

where *options* is any permissible combination of arguments and keywords. See the "Configuration Examples for Flexible NetFlow - Top N Talkers Support " section for more information.

Memory and Performance Impact of Top N Talkers

The Flexible NetFlow - Top N Talkers Support feature can use a large number of CPU cycles and possibly also system memory for a short time. However, because the Flexible NetFlow - Top N Talkers Support feature uses only **show** commands, the CPU usage should be run at a low priority because no real-time data processing is involved. The memory usage can be mitigated by using a larger granularity of aggregation or no aggregation at all.

How to Analyze Network Traffic Using Flexible NetFlow Top N Talkers

Filtering Flow Data from the Flexible NetFlow Cache

This task shows you how to use the **show flow monitor cache filter** command with a regular expression to filter the flow monitor cache data and display the results. For more information on regular expressions and the **show flow monitor cache filter** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Perform this task to filter the flow monitor cache data using a regular expression and display the results.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [**name**] *monitor-name* **cache filter**]] [**format** {**csv** | **record** | **table**}]

DETAILED STEPS

Step 1 **enable**

Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show flow monitor** [**name**] *monitor-name* **cache filter**]] [**format** {**csv** | **record** | **table**}]

Filters the flow monitor cache data on the IPv4 type of service (ToS) value.

Example:

Sorting Flow Data from the Flexible NetFlow Cache

This task shows you how to use the **show flow monitor cache sort** command to sort the flow monitor cache data, and display the results. For more information on the **show flow monitor cache sort** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Perform this task to sort the flow monitor cache data and display the results.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [**name**] *monitor-name* **cache sort** *options* [**top** [*number*]] [**format** {**csv** | **record** | **table**}]

DETAILED STEPS

Step 1 **enable**

Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show flow monitor** [**name**] *monitor-name* **cache sort** *options* [**top** [*number*]] [**format** {**csv** | **record** | **table**}]

Displays the cache data sorted on the number of packets from highest to lowest.

Note When the **top** keyword is not used, the default number of sorted flows shown is 20.

Example:

```
Device# show flow monitor FLOW-MONITOR-1 cache sort highest counter packets

Processed 26 flows
Aggregated to 26 flows
Showing the top 20 flows
IPV4 SOURCE ADDRESS:       10.1.1.3
IPV4 DESTINATION ADDRESS:  172.16.10.11
TRNS SOURCE PORT:          443
TRNS DESTINATION PORT:     443
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             22760
counter packets:           1569
timestamp first:           19:42:32.924
timestamp last:            19:57:28.656
IPV4 SOURCE ADDRESS:       10.10.11.2
IPV4 DESTINATION ADDRESS:  172.16.10.6
TRNS SOURCE PORT:          65
TRNS DESTINATION PORT:     65
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             22720
counter packets:           568
timestamp first:           19:42:34.264
timestamp last:            19:57:28.428
```

```
.
.
.
IPV4 SOURCE ADDRESS:       192.168.67.6
IPV4 DESTINATION ADDRESS:  172.16.10.200
TRNS SOURCE PORT:          0
TRNS DESTINATION PORT:     3073
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               1
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             15848
counter packets:           344
timestamp first:           19:42:36.852
timestamp last:            19:57:27.836
IPV4 SOURCE ADDRESS:       10.234.53.1
IPV4 DESTINATION ADDRESS:  172.16.10.2
TRNS SOURCE PORT:          0
TRNS DESTINATION PORT:     2048
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               1
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             15848
counter packets:           213
timestamp first:           19:42:36.904
timestamp last:            19:57:27.888
```

Displaying the Top N Talkers with Sorted Flow Data

This task shows you how to use the **show flow monitor cache sort** command to sort the flow monitor cache data, and to limit the display results to a specific number of high volume flows. For more information on the **show flow monitor cache sort** command, refer to the *Cisco IOS Flexible NetFlow Command Reference*.

Perform this task to sort the flow monitor cache data and limit the display output using to a specific number of high volume flows.

SUMMARY STEPS

1. **enable**
2. **show flow monitor** [**name**] *monitor-name* **cache sort** *options* [**top** [*number*]] [**format** {**csv** | **record** | **table**}]

DETAILED STEPS

Step 1 **enable**

Enters privileged EXEC mode.

Example:

```
Device> enable
```

Step 2 **show flow monitor** [**name**] *monitor-name* **cache sort** *options* [**top** [*number*]] [**format** {**csv** | **record** | **table**}]

Displays the cache data sorted on the number of packets from highest to lowest and limits the output to the three highest volume flows.

Example:

```
Device# show flow monitor FLOW-MONITOR-1 cache sort highest counter packets top 3

Processed 25 flows
Aggregated to 25 flows
Showing the top 3 flows
IPV4 SOURCE ADDRESS:       10.1.1.3
IPV4 DESTINATION ADDRESS:  172.16.10.11
TRNS SOURCE PORT:          443
TRNS DESTINATION PORT:     443
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             32360
counter packets:           1897
timestamp first:           19:42:32.924
timestamp last:            20:03:47.100
IPV4 SOURCE ADDRESS:       10.10.11.2
IPV4 DESTINATION ADDRESS:  172.16.10.6
TRNS SOURCE PORT:          65
TRNS DESTINATION PORT:     65
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             32360
counter packets:           809
timestamp first:           19:42:34.264
timestamp last:            20:03:48.460
IPV4 SOURCE ADDRESS:       172.16.1.84
```

```
IPV4 DESTINATION ADDRESS:  172.16.10.19
TRNS SOURCE PORT:          80
TRNS DESTINATION PORT:     80
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /24
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             32320
counter packets:           345
timestamp first:           19:42:34.512
timestamp last:            20:03:47.140
```

Configuration Examples for Flexible NetFlow Top N Talkers

Example: Displaying the Top Talkers with Filtered and Sorted Flow Data

Example: Filtering Using Multiple Filtering Criteria

The following example filters the cache data on the IPv4 destination address and the destination port:

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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

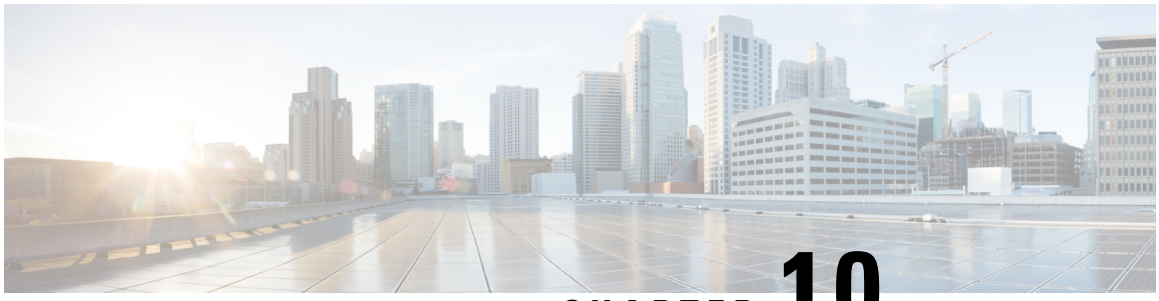
Feature Information for Flexible NetFlow - Top N Talkers

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 - Top N Talkers

Feature Name	Releases	Feature Information
Flexible NetFlow - Top N Talkers Support		This feature helps you analyze the large amount of data Flexible NetFlow captures from the traffic in your network by providing the ability to filter, aggregate, and sort the data in the Flexible NetFlow cache as you display it. 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: **show flow monitor cache aggregate**, **show flow monitor cache filter**, **show flow monitor cache**.



CHAPTER 10

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

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 Customized 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** *record-name* **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.

	Command or Action	Purpose
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`	Configures a key field for the flow record. **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** command, and the other **match** commands that are available to configure key fields.
		Note
		• Ingress:
		• 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:
		• 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:** `Device(config-flow-record)# collect interface input`	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:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 11	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.
Step 12	**show running-config flow record** *record-name* **Example:** `Device# show running-config flow record FLOW_RECORD-1`	(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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> 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** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type.

	Command or Action	Purpose
		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	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip**	**ipv6**} **flow monitor** *monitor-name* {**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** *type number* **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** *monitor-name* **cache format record** **Example:**	Displays the status, statistics, and flow data in the cache for the specified flow monitor.

	Command or Action	Purpose
	`Device# show flow monitor name FLOW_MONITOR-1 cache format record`	

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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

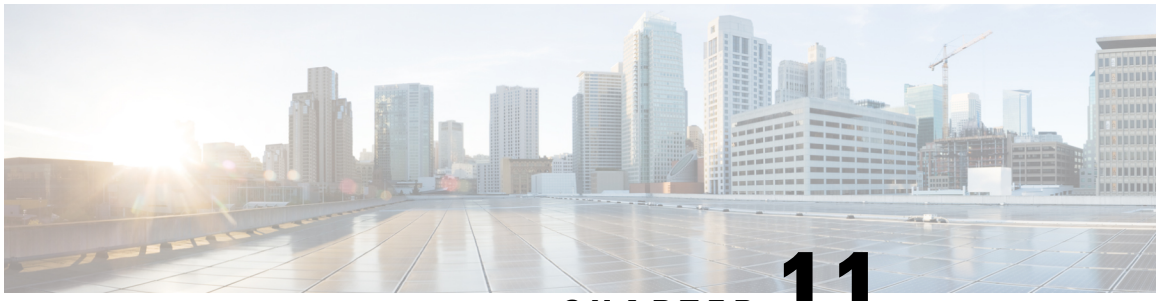
Feature Information for Flexible NetFlow—Ingress VRF Support

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 25: 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 11

TrustSec NetFlow IPv4 SGACL Deny and Drop Export

The TrustSec NetFlow IPv4 SGACL Deny and Drop Export feature enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv4 traffic.

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 TrustSec NetFlow IPv4 SGACL Deny and Drop Export

TrustSec NetFlow IPv4 SGACL Deny and Drop Export Overview

A Security Group Access Control List (SGACL) is used to filter untrusted packets. The TrustSec NetFlow IPv4 SGACL Deny and Drop Export feature enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv4 traffic.

How to Configure TrustSec NetFlow IPv4 SGACL Deny and Drop Export

Creating a Customized 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** *record-name* **Example:**	Creates a flow record and enters Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
	`Device(config)# flow record FLOW-RECORD-1`	• 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`	Configures a key field for the flow record. **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** command, and the other **match** commands that are available to configure key fields.

	Command or Action	Purpose
		Note • Ingress: • 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: • 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	**collect interface** {**input** | **output**} **Example:** `Device(config-flow-record)# collect interface input`	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:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 11	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.
Step 12	**show running-config flow record** *record-name* **Example:**	(Optional) Displays the configuration of the specified flow record.

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

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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. 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	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.

	Command or Action	Purpose
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**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** *type number* **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** *monitor-name* **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 TrustSec NetFlow IPv4 SGACL Deny and Drop Export

Example: Configuring Flexible NetFlow for CTS Fields

This following example configures the collection of the Cisco TrustSec (CTS) fields, source Security Group Tag (SGT) and destination Security Group Tag (DGT), in IPv4 traffic.

This sample starts in global configuration mode:

```
!
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
```

```
exit
flow record rm_1
match ipv4 protocol
match ipv4 source address
match ipv4 destination address
match transport source-port
match transport destination-port
match flow direction
match flow cts source group-tag
match flow cts destination group-tag
collect routing source as
collect routing destination as
collect routing source as peer
collect routing destination as peer
collect routing next-hop address ipv4
collect routing next-hop address ipv4 bgp
collect ipv4 source prefix
collect ipv4 source mask
collect ipv4 destination prefix
collect ipv4 destination mask
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor mm_1
record rm_1
exporter EXPORTER-1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

Additional References for TrustSec NetFlow IPv4 SGACL Deny and Drop Export

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Flexible NetFlow conceptual and configuration information	*Flexible NetFlow Configuration Guide*
Configuration commands for Flexible NetFlow	*Cisco IOS Flexible NetFlow Command Reference*

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	Cisco Systems NetFlow Services Export Version 9

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

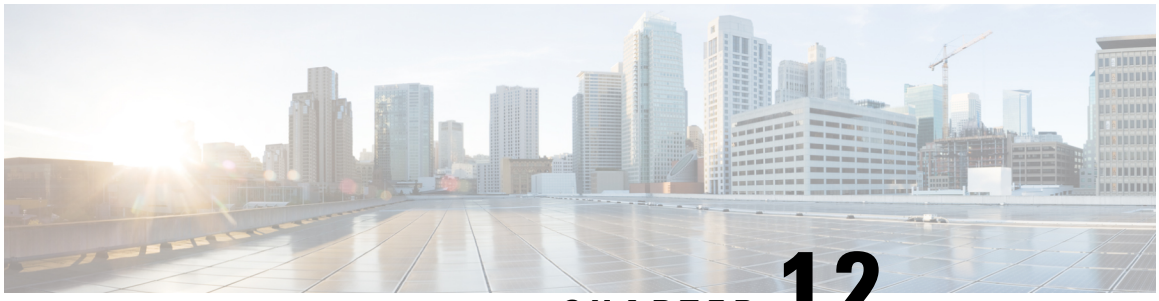
Feature Information for TrustSec NetFlow IPv4 SGACL Deny and Drop Export

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 26: Feature Information for Flexible NetFlow IPv4 SGACL Deny and Drop Export

Feature Name	Releases	Feature Information
TrustSec NetFlow IPv4 SGACL Deny and Drop Export	12.2(50)SY 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv4 traffic. The following commands were introduced or modified: **collect flow, match flow, show flow monitor.**



CHAPTER 12

TrustSec NetFlow IPv6 SGACL Deny and Drop Export

The TrustSec NetFlow IPv6 SGACL Deny and Drop Export feature enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv6 traffic.

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 TrustSec NetFlow IPv6 SGACL Deny and Drop Export

TrustSec NetFlow IPv6 SGACL Deny and Drop Export Overview

A Security Group Access Control List (SGACL) is used to filter untrusted packets. The TrustSec NetFlow IPv6 SGACL Deny and Drop Export feature enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv6 traffic.

How to Configure TrustSec NetFlow IPv6 SGACL Deny and Drop Export

Creating a Customized 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** *record-name* **Example:**	Creates a flow record and enters Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
	`Device(config)# flow record FLOW-RECORD-1`	• 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`	Configures a key field for the flow record. **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** command, and the other **match** commands that are available to configure key fields.

	Command or Action	Purpose
		Note • Ingress: • 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: • 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	**collect interface** {**input** | **output**} **Example:** `Device(config-flow-record)# collect interface input`	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:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 11	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.
Step 12	**show running-config flow record** *record-name* **Example:**	(Optional) Displays the configuration of the specified flow record.

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

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. These record formats can be one of the predefined formats or 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 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.

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* | {**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:** `> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **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** *description* **Example:** `(config-flow-monitor)# description Used for basic ipv4 traffic analysis`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]} **Example:** `(config-flow-monitor)# record FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** | **inactive** | **update**} *seconds* | {**immediate** | **normal** | **permanent**}} **Example:**	(Optional) Modifies the flow monitor cache parameters such as timeout values, number of cache entries, and the cache type. 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	**statistics packet protocol** **Example:** `(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was created previously.

	Command or Action	Purpose
Step 11	**end** **Example:** `(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 12	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]] [**statistics**]] **Example:** `# show flow monitor FLOW-MONITOR-2 cache`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.
Step 13	**show running-config flow monitor** *monitor-name* **Example:** `# show running-config flow monitor FLOW_MONITOR-1`	(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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Device(config)# interface GigabitEthernet 0/0/0`	Specifies an interface and enters interface configuration mode.
Step 4	{**ip** | **ipv6**} **flow monitor** *monitor-name* {**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** *type number* **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** *monitor-name* **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 TrustSec NetFlow IPv6 SGACL Deny and Drop Export

Example: Configuring Flexible NetFlow for CTS Fields in IPv6 traffic

This following example configures the collection of the Cisco TrustSec (CTS) fields, source Security Group Tag (SGT) and destination Security Group Tag (DGT), in IPv6 traffic.

This sample starts in global configuration mode:

```
!
flow exporter EXPORTER-1
destination 172.16.10.2
transport udp 90
```

```
exit
flow record rm_1
match ipv6 protocol
match ipv6 source address
match ipv6 destination address
match transport source-port
match transport destination-port
match flow direction
match flow cts source group-tag
match flow cts destination group-tag
collect routing source as
collect routing destination as
collect routing source as peer
collect routing destination as peer
collect routing next-hop address ipv6
collect routing next-hop address ipv6 bgp
collect ipv6 source prefix
collect ipv6 source mask
collect ipv6 destination prefix
collect ipv6 destination mask
collect interface input
collect interface output
collect counter bytes
collect counter packets
collect timestamp sys-uptime first
collect timestamp sys-uptime last
!
flow monitor mm_1
record rm_1
exporter EXPORTER-1
!
interface FastEthernet0/0
ip address 172.16.2.2 255.255.255.0
ip flow monitor mm_1 input
!
end
```

Additional References for TrustSec NetFlow IPv6 SGACL Deny and Drop Export

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Flexible NetFlow conceptual and configuration information	*Flexible NetFlow Configuration Guide*
Configuration commands for Flexible NetFlow	*Cisco IOS Flexible NetFlow Command Reference*

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	Cisco Systems NetFlow Services Export Version 9

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

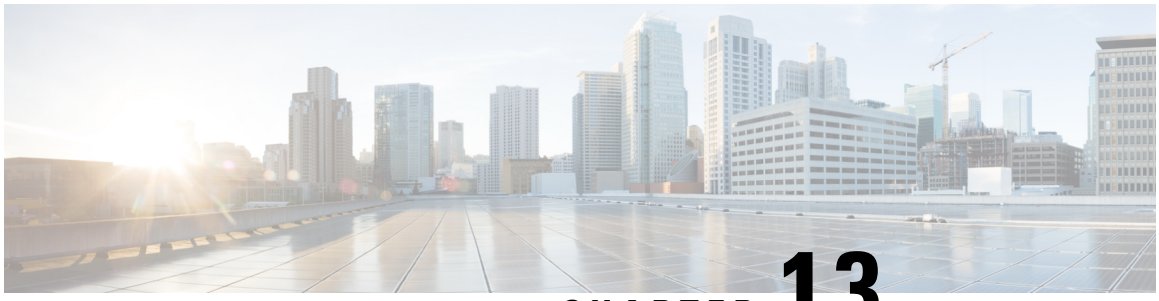
Feature Information for TrustSec NetFlow IPv6 SGACL Deny and Drop Export

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 27: Feature Information for TrustSec NetFlow IPv6 SGACL Deny and Drop Export

Feature Name	Releases	Feature Information
TrustSec NetFlow IPv6 SGACL Deny and Drop ExportS	12.2(50)SY 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to collect Cisco Trusted Security (CTS) information in IPv6 traffic. The following commands were introduced or modified: **collect flow, match flow, show flow monitor.**



CHAPTER 13

Configuring CPU Friendly NetFlow Export

The CPU Friendly NetFlow Export feature for Cisco IOS Flexible NetFlow provides the capability for the software NetFlow modules to adjust their Central Processing Unit (CPU) utilization based on user-configured CPU utlization thresholds for the supervisor and line cards. NetFlow will lower its CPU consumption when utilization exceeds the configured threshold, and vice versa.

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 CPU Friendly NetFlow 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 IPv6.

Information About CPU Friendly NetFlow Export

Overview of CPU Friendly NetFlow Export

The number and complexity of flow records to be exported is the prime cause of CPU use in NetFlow. The CPU Friendly NetFlow Export feature (also known as Yielding NetFlow Data Export, or Yielding NDE) monitors CPU use for both the supervisor and line cards according to user-configured thresholds and dynamically adjusts the rate of export as needed.

How to Configure CPU Friendly NetFlow Export

Configuring the CPU Utilization Threshold

To configure the CPU utilization threshold, the threshold above which NetFlow decreases its CPU consumption, perform the following required task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow hardware** [**egress | export threshold** *total-cpu-threshold-percentage [* **linecard** *linecard-threshold-percentage]* **| usage notify**{**input | output**} [*table-threshold-percentage seconds*]]
4. **end**
5. **show platform flow** [**aging** | {**export | usage | table-contention** {**aggregate | detailed | summary**} }[*instance* | *module]* | {**ip | ipv6} [** *count* | *destination* | *instance* | *module* | *multicast* | *protocol* | *source*] | {**layer2 | mpls } [** *count* | *instance* | *module* **]]**

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:**	Enters global configuration mode.

	Command or Action	Purpose
	`Device# configure terminal`	
Step 3	**flow hardware** [**egress** | **export threshold** *total-cpu-threshold-percentage [* **linecard** *linecard-threshold-percentage]* | **usage notify**{**input** | **output**} [*table-threshold-percentage seconds*]] **Example:** `Device(config)# flow hardware export threshold 25 linecard 25`	Configures the CPU utilization threshold up to which NetFlow export is permitted.
Step 4	**end** **Example:** `Device(config)# end`	Ends the current configuration session and returns to privileged EXEC mode.
Step 5	**show platform flow** [**aging** | {**export** | **usage** | **table-contention** {**aggregate** | **detailed** | **summary**} }[*instance* | *module]* | {**ip** | **ipv6**} **[** *count* | *destination* | *instance* | *module* | *multicast* | *protocol* | *source*] | {**layer2** | **mpls** } **[** *count* | *instance* | *module* **]]** **Example:** `Device# show platform flow export`	Verifies the configuration of the CPU utilization threshold.

Configuration Examples for CPU Friendly NetFlow Export

Example: Configuring CPU Utilization Thresholds for NetFlow Export

The following example shows how to configure CPU utilization thresholds for NetFlow export.

This sample starts in global configuration mode.

```
!
flow hardware export threshold 25
flow hardware export threshold 25 linecard 25
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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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

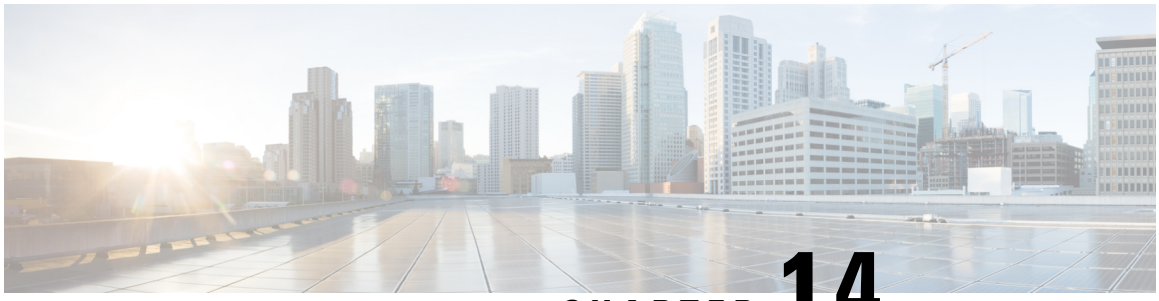
Feature Information for CPU Friendly NetFlow Export

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn . An account on Cisco.com is not required.

Note The table below 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.

Table 28: Feature Information for CPU Friendly NetFlow Export

Feature Name	Releases	Feature Information
CPU Friendly NetFlow Export	12.2(50)SY 15.0(1)SY 15.0(1)SY1	The CPU Friendly NetFlow Export feature provides the capability for the software NetFlow modules to adjust their Central Processing Unit (CPU) utilization based on user configured CPU thresholds for the supervisor and line cards, so that when the total CPU utilization is above the configured threshold, NetFlow decreases its CPU consumption, and vice versa. Information about the CPU Friendly NetFlow Export feature is included in the following sections: The following commands were introduced or modified: **flow hardware, show platform flow.**



CHAPTER 14

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

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 171.

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. • 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>
Borokers:
[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     DHCPC
 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 preforming 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	*Cisco IOS High Availability Command Reference*
Cisco IOS debug commands	*Cisco IOS Debug Command Reference*
SSO - BFD	" Bidirectional Forwarding Detection " chapter in the *IP Routing Protocols Configuration Guide*
SSO HSRP	"Configuring HSRP" chapter in the *IP Application Services Configuration Guide*
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	*Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*

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

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
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. 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. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/techsupport

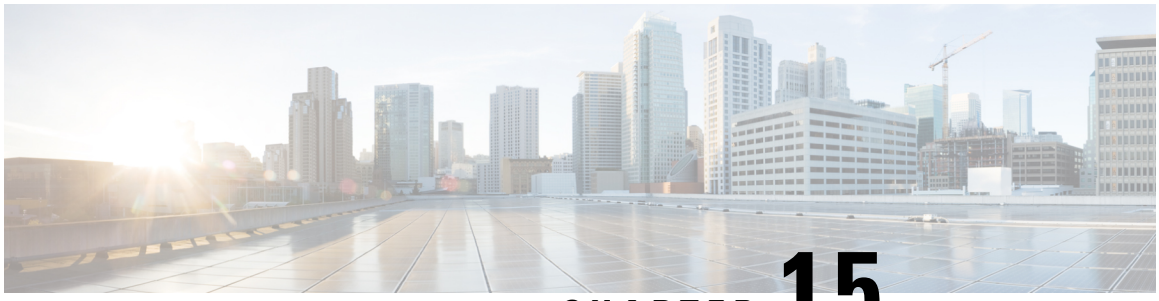
Glossary

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 switching occurs, forwarding and sessions are maintained. SSO makes an RP failure undetectable to the network.



CHAPTER 15

Configuring Accounting for IPv6 Layer 2 Bridged Traffic

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release.

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

Prerequisites for Monitoring IPv6 Bridged Flows

- The networking device must be running a Cisco release release that supports Flexible NetFlow.
- 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 IPv6.
- You have configured a flow record, flow monitor, flow exporter, and flow sampler.

Information About Monitoring IPv6 Layer 2 Bridged Traffic

This feature expands the **ipv6 flow monitor** command to include a **layer2-bridged** keyword that enables you to configure Flexible Netflow to monitor IPv6 Layer 2 bridged traffic on both Switched Virtual Interfaces (SVIs) and VLANs, with or without flow samplers.

How to Configure the Monitoring of IPv6 Layer 2 Bridged Traffic

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 Record, Flow Monitor, and Exporter to Monitor IPv6 Layer 2 Bridged Traffic

To configure a flow record, flow monitor, and exporter to monitor IPv6 Layer 2 bridged traffic, perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *name*
4. **match datalink source-vlan-id**
5. **match flow cts destination group**
6. **match flow cts source group**
7. **match flow direction**
8. **match interface input**
9. **match interface input physical**
10. **match interface output**
11. **match ipv4 destination address**
12. **match ipv4 dscp**
13. **match ipv4 precedence**
14. **match ipv4 protocol**
15. **match ipv4 source address**
16. **match ipv4 tos**
17. **match transport destination-port**
18. **match transport source-port**
19. **collect counter bytes**

20. **collect counter packets**
21. **collect interface output**
22. **collect interface input**
23. **collect ipv4 destination mask**
24. **collect ipv4 destination prefix**
25. **collect ipv4 source mask**
26. **collect ipv4 source prefix**
27. **collect timestamp sys-uptime first**
28. **collect timestamp sys-uptime last**
29. **collect transport tcp flags**
30. **exit**
31. **flow exporter** *exporter-name*
32. **export-protocol netflow-v9**
33. **destination** *ip-address*
34. **exit**
35. **flow monitor** *name*
36. **record** *record-name*
37. **exporter** *exporter-name*
38. **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 record** *name* **Example:** `Device(config)# flow record ipv6-bridged-traffic`	Configures a flow record to monitor IPv6 bridged Layer 2 traffic and enters Flexible NetFlow flow record configuration mode.
Step 4	**match datalink source-vlan-id** **Example:** `Device(config-flow-record)# match datalink source-vlan-id`	Configures the source VLAN ID as a key field.
Step 5	**match flow cts destination group** **Example:** `Device(config-flow-record)# match flow cts destination group`	Configures the flow CTS destination group as a key field.

	Command or Action	Purpose
Step 6	**match flow cts source group** **Example:** `Device(config-flow-record)# match flow cts source group`	Configures the flow CTS source group as a key field.
Step 7	**match flow direction** **Example:** `Device(config-flow-record)# match flow direction`	Configures the flow direction as a key field.
Step 8	**match interface input** **Example:** `Device(config-flow-record)# match interface input`	Configures the input interface as a key field.
Step 9	**match interface input physical** **Example:** `Device(config-flow-record)# match interface input physical`	Configures the physical input interface as a key field.
Step 10	**match interface output** **Example:** `Device(config-flow-record)# match interface input`	Configures the output interface as a key field.
Step 11	**match ipv4 destination address** **Example:** `Device(config-flow-record)# match ipv4 destination address`	Configures the IPv4 destination address as a key field.
Step 12	**match ipv4 dscp** **Example:** `Device(config-flow-record)# match ipv4 dscp`	Configures the IPv4 DSCP as a key field.
Step 13	**match ipv4 precedence** **Example:** `Device(config-flow-record)# match ipv4 precedence`	Configures the IPv4 precedence as a key field.
Step 14	**match ipv4 protocol** **Example:** `Device(config-flow-record)# match ipv4 protocol`	Configures the IPv4 protocol as a key field.

	Command or Action	Purpose
Step 15	**match ipv4 source address** **Example:** `Device(config-flow-record)# match ipv4 source address`	Configures the IPv4 source address as a key field.
Step 16	**match ipv4 tos** **Example:** `Device(config-flow-record)# match ipv4 tos`	Configures the IPv4 TOS as a key field.
Step 17	**match transport destination-port** **Example:** `Device(config-flow-record)# match transport destination-port`	Configures the transport destination port as a key field.
Step 18	**match transport source-port** **Example:** `Device(config-flow-record)# match transport source-port`	Configures the transport source port as a key field.
Step 19	**collect counter bytes** **Example:** `Device(config-flow-record)# collect counter bytes`	Collects the total number of bytes.
Step 20	**collect counter packets** **Example:** `Device(config-flow-record)# collect counter packets`	Collects the total number of packets.
Step 21	**collect interface output** **Example:** `Device(config-flow-record)# collect interface output`	Collects the output interface.
Step 22	**collect interface input** **Example:** `Device(config-flow-record)# collect interface input`	Collects the input interface.
Step 23	**collect ipv4 destination mask** **Example:**	Collects the Ipv4 destination mask.

	Command or Action	Purpose
	`Device(config-flow-record)# collect ipv4 destination mask`	
Step 24	**collect ipv4 destination prefix** **Example:** `Device(config-flow-record)# collect ipv4 destination prefix`	Collects the Ipv4 destination prefix.
Step 25	**collect ipv4 source mask** **Example:** `Device(config-flow-record)# collect ipv4 source mask`	Collects the Ipv4 source mask.
Step 26	**collect ipv4 source prefix** **Example:** `Device(config-flow-record)# collect ipv4 source prefix`	Collects the Ipv4 source prefix.
Step 27	**collect timestamp sys-uptime first** **Example:** `Device(config-flow-record)# collect timestamp sys-uptime first`	Collects the first timestamp of the system uptime.
Step 28	**collect timestamp sys-uptime last** **Example:** `Device(config-flow-record)# collect timestamp sys-uptime last`	Collects the last timestamp of the system uptime.
Step 29	**collect transport tcp flags** **Example:** `Device(config-flow-record)# collect transport tcp flags`	Collects the TCP transport flags.
Step 30	**exit** **Example:** `Device(config-flow-record)# exit`	Exits Flexible NetFlow flow record configuration mode.

	Command or Action	Purpose
Step 31	**flow exporter** *exporter-name* **Example:** `Device(config)# flow exporter my-flow-exporter`	Creates an FNF flow exporter and enters Flexible NetFlow flow exporter configuration mode.
Step 32	**export-protocol netflow-v9** **Example:** `Device(config-flow-exporter)# export-protocol netflow-v9`	Configures NetFlow Version 9 export as the export protocol.
Step 33	**destination** *ip-address* **Example:** `Device(config-flow-exporter)# destination 209.165.201.1`	Configures the IP address of the workstation to which you want to send the NetFlow information.
Step 34	**exit** **Example:** `Device(config-flow-exporter)# exit`	Exits Flexible NetFlow flow exporter configuration mode.
Step 35	**flow monitor** *name* **Example:** `Device(config)# flow monitor ipv6-bridged-traffic`	Configures a flow monitor for IPv6 bridged traffic and enters Flexible NetFlow flow monitor configuration mode.
Step 36	**record** *record-name* **Example:** `Device(config-flow-monitor)# record ipv6-bridged-traffic`	Specifies the name of a user-defined flow record that was previously configured.
Step 37	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter my-flow-exporter`	Specifies the name of a flow exporter that was previously configured.
Step 38	**end** **Example:** `Device(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.

Applying a Flow Monitor to a Switched Virtual Interface to Monitor IPv6 Layer 2 Bridged Traffic

To configure Flexible Netlflow to monitor IPv6 Layer 2 Bridged Traffic on a SVI, perform this task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan** *number*
4. **ipv6 flow monitor** *monitor-name* [**sampler** *monitor-name*] **layer2-bridged input**
5. **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	**interface vlan** *number* **Example:** `Device(config)# interface vlan 100`	Configures an interface type and enters interface configuration mode.
Step 4	**ipv6 flow monitor** *monitor-name* [**sampler** *monitor-name*] **layer2-bridged input** **Example:** `Device(config-if)# ipv6 flow monitor ipv6-bridged-traffic sampler S1 layer2-bridged input`	Applies the monitor to the interface.
Step 5	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Applying a Flow Monitor to a VLAN to Monitor IPv6 Layer 2 Bridged Traffic

To configure Flexible Netlflow to monitor IPv6 Layer 2 Bridged Traffic on a VLAN, perform this task:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface vlan** *number*
4. **ipv6 flow monitor** *monitor-name* [**sampler** *monitor-name*] **layer2-bridged input**
5. **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	**interface vlan** *number* **Example:** `Device(config)# vlan configuration 100`	Configures a VLAN and enters VLAN configuration mode.
Step 4	**ipv6 flow monitor** *monitor-name* [**sampler** *monitor-name*] **layer2-bridged input** **Example:** `Device(config-vlan)# ipv6 flow monitor ipv6-bridged-traffic sampler S1 layer2-bridged input`	Applies the monitor to the VLAN.
Step 5	**end** **Example:** `Device(config-vlan)# end`	Exits VLAN configuration mode and returns to privileged EXEC mode.

Configuration Examples for Monitoring IPv6 Layer 2 Bridged Traffic

You can configure Flexible Netflow to monitor IPv6 Layer 2 bridged traffic on both Switched Virtual Interfaces (SVIs) and VALNs, with or without flow samplers.

Example Configuration for SVI-based Monitoring IPv6 Layer 2 Bridged Traffic

The following example is designed to monitor IPv6 Layer 2 bridged traffic on an SVI. 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 sample starts in global configuration mode:

```
!
!
flow record bridged-flow-record
 description bridged flow record
 match ipv6 destination address
 match ipv6 source address
 match interface input
 collect counter bytes long
 collect counter packets long
 exit
!
flow monitor bridged-flow-monitor
 description bridged flow monitor
 record bridged-flow-record
 exit
!
interface vlan 100
 ipv6  flow monitor bridged-flow-monitor layer2-bridged input
 exit
!
```

Example Configuration for VLAN-Based Monitoring of IPv6 Layer3 Bridged Traffic

The following example is designed to monitor IPv6 Layer 2 bridged traffic on a VLAN. 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 sample starts in global configuration mode:

```
!
!
flow record bridged-flow-record
 description bridged flow record
 match ipv6 destination address
 match ipv6 source address
 match interface input
 collect counter bytes long
 collect counter packets long
 exit
!
flow monitor bridged-flow-monitor
 description bridged flow monitor
 record bridged-flow-record
 exit
!
vlan configuration 100
 ipv6  flow monitor bridged-flow-monitor layer2-bridged input
 exit
!
```

Example Configuration for SVI-based Monitoring IPv6 Layer 2 Bridged Traffic Using a Flow Sampler

The following example is designed to monitor IPv6 Layer 2 bridged traffic on an SVI using a sampler. 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 sample starts in global configuration mode:

```
!
!
flow record bridged-flow-record
 description bridged flow record
 match ipv6 destination address
 match ipv6 source address
 match interface input
 collect counter bytes long
 collect counter packets long
 exit
!
flow monitor bridged-flow-monitor
 description bridged flow monitor
 record bridged-flow-record
 exit
!
sampler S1
 mode deterministic 1 out-of 2
 exit
!
interface vlan 100
 ipv6  flow monitor bridged-flow-monitor sampler S1 layer2-bridged input
 exit
!
```

Example Configuration for VLAN-Based Monitoring of IPv6 Layer3 Bridged Traffic Using a Flow Sampler

The following example is designed to monitor IPv6 Layer 2 bridged traffic on a VLAN using a flow sampler. 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 sample starts in global configuration mode:

```
!
!
flow record bridged-flow-record
 description bridged flow record
 match ipv6 destination address
 match ipv6 source address
 match interface input
 collect counter bytes long
 collect counter packets long
 exit
!
flow monitor bridged-flow-monitor
 description bridged flow monitor
 record bridged-flow-record
```

```
 exit
!
sampler S1
 mode deterministic 1 out-of 2
 exit
!
vlan configuration 100
 ipv6  flow monitor bridged-flow-monitor sampler S1 layer2-bridged input
 exit
!
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Flexible NetFlow	"Cisco IOS Flexible NetFlow Overview"
Flexible NetFlow Feature Roadmap	"Cisco IOS Flexible NetFlow Features Roadmap"
Emulating original NetFlow with Flexible NetFlow	"Getting Started with Configuring Cisco IOS Flexible NetFlow"
Configuring flow exporters to export Flexible NetFlow data.	"Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters"
Configuring flow sampling to reduce the overhead of monitoring traffic with Flexible NetFlow	"Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic"
Configuring Flexible NetFlow using predefined records	"Configuring Cisco IOS Flexible NetFlow with Predefined Records"
Using Flexible NetFlow Top N Talkers to analyze network traffic	"Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic"
Configuring IPv4 multicast statistics support for Flexible NetFlow	"Configuring IPv4 Multicast Statistics Support for Cisco IOS Flexible NetFlow"
Configuration commands for Flexible NetFlow	*Cisco IOS Flexible NetFlow Command Reference*

Standards

Standard	Title
None	--

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

RFCs

RFC	Title
RFC 3954	*Cisco Systems NetFlow Services Export Version 9*

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

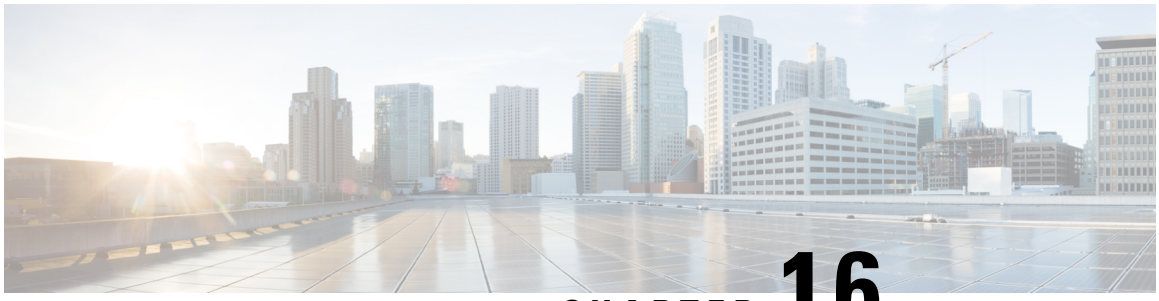
Feature Information for Configuring Accounting for IPv6 Layer 2 Bridged Traffic

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 IPv6 Bridged Flows Feature

Feature Name	Releases	Feature Information
Flexible Netflow - IPv6 bridged flows	15.1(1)SY	Flexible Netflow has been enhanced to enable the accounting of Layer 2 switched or bridged IPv6 traffic, for both SVIs and pure VLANs.



CHAPTER 16

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

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.

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. **dscp** *dscp*
7. **source** *interface-type interface-number*
8. **output-features**
9. **template data timeout** *seconds*
10. **transport udp** *udp-port*
11. **ttl** *seconds*
12. **end**
13. **show flow exporter** *exporter-name*
14. **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** *exporter-name* **Example:**	Creates the flow exporter and enters Flexible NetFlow flow exporter configuration mode.

	Command or Action	Purpose
	`Device(config)# flow exporter EXPORTER-1`	• 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	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 7	**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 8	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 9	**template data timeout** *seconds* **Example:** `Device(config-flow-exporter)# template data timeout 120`	(Optional) Configures resending of templates based on a timeout. • The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 10	**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. • The range for the *udp-port* argument is from 1 to 65536.
Step 11	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.

	Command or Action	Purpose
Step 12	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 13	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 14	**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 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
!
```

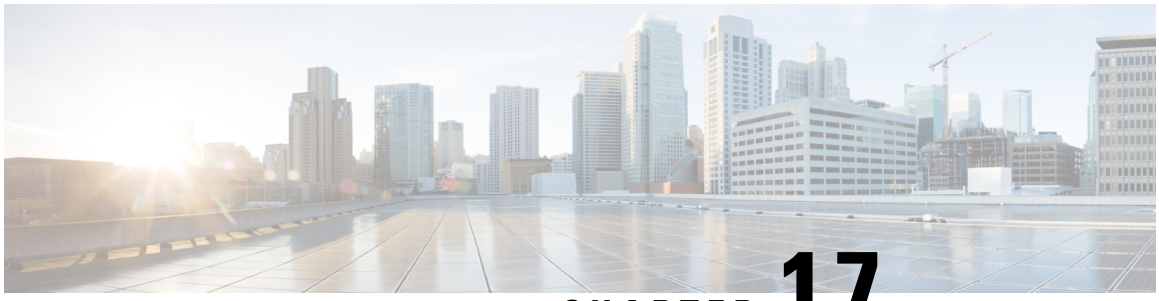
Feature Information for Flexible NetFlow: IPFIX Export Format

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 30: 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 17

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

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.

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. **dscp** *dscp*
7. **source** *interface-type interface-number*
8. **output-features**
9. **template data timeout** *seconds*
10. **transport udp** *udp-port*
11. **ttl** *seconds*
12. **end**
13. **show flow exporter** *exporter-name*
14. **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** *exporter-name* **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.
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.

	Command or Action	Purpose
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	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 7	**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 8	**output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 9	**template data timeout** *seconds* **Example:** `Device(config-flow-exporter)# template data timeout 120`	(Optional) Configures resending of templates based on a timeout. • The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 10	**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. • The range for the *udp-port* argument is from 1 to 65536.
Step 11	**ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 12	**end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 13	**show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.

	Command or Action	Purpose
Step 14	**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 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	*Flexible NetFlow Configuration Guide*
Flexible NetFlow commands	*Cisco IOS Flexible NetFlow Command Reference*

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