Flexible Netflow Configuration Guide, Cisco IOS Release 15S

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

Cisco IOS 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.

This module provides an overview of Flexible NetFlow and the advanced Flexible NetFlow features and services.

Finding Feature Information

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

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

Information About Flexible NetFlow

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.

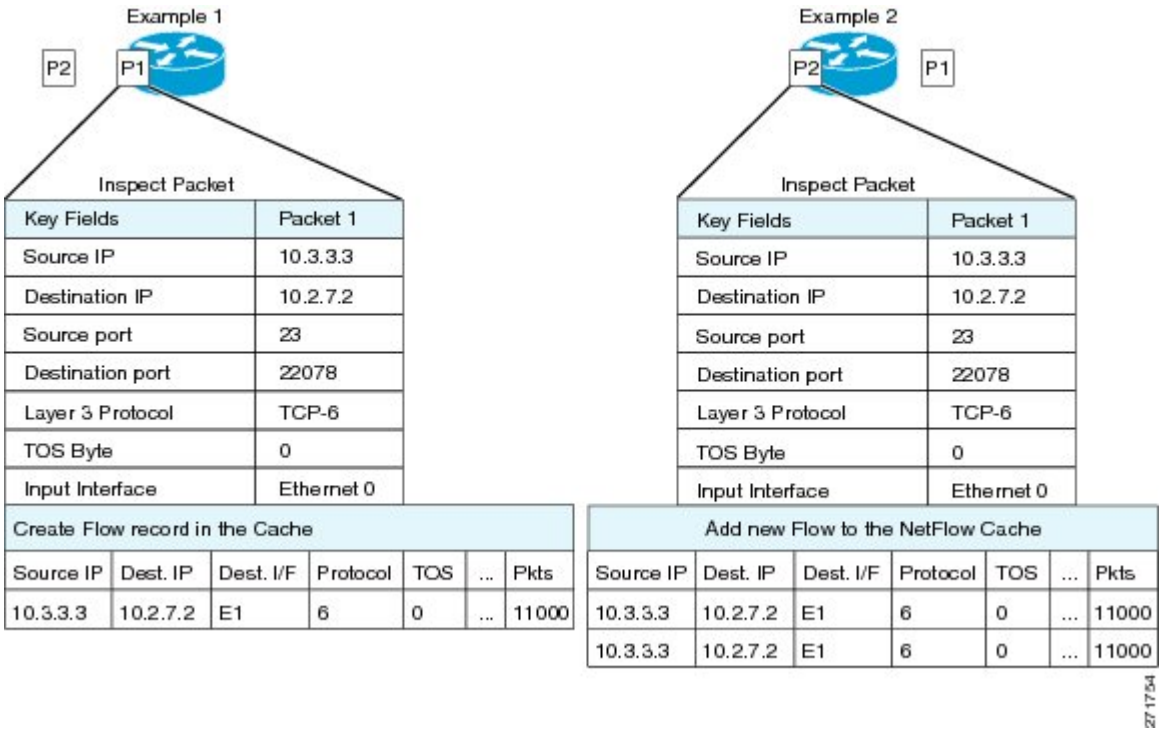
Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. 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 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 export format.
- 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.

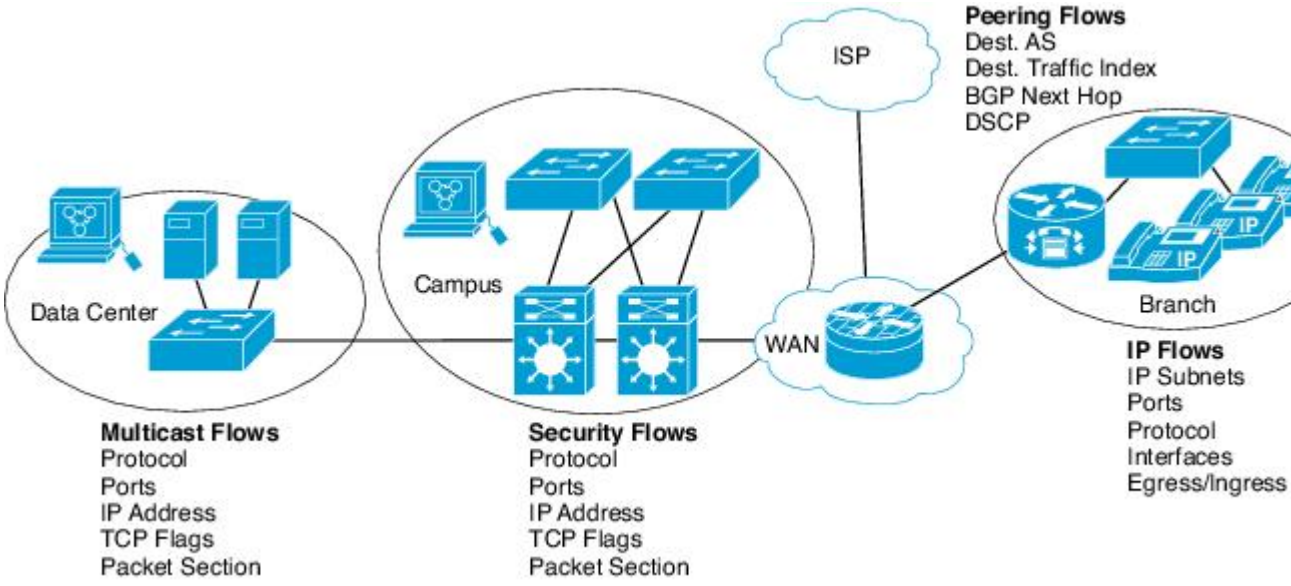
Original NetFlow allows you to understand the activities in the network and thus to optimize network design and reduce operational costs. Flexible NetFlow allows you to understand network behavior with

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:

- Records, page 5
- Flow Monitors, page 5
- Flow Exporters, page 7
- Flow Samplers, page 9

Records

In Flexible NetFlow a combination of key and nonkey fields is called a *record* . Flexible NetFlow records are assigned to Flexible NetFlow flow monitors to define the cache that is used for storing flow data. Flexible NetFlow includes several predefined records that can help you get started using Flexible NetFlow. 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, page 5
- User-Defined Records, page 5

NetFlow Predefined Records

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

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

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

User-Defined Records

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

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

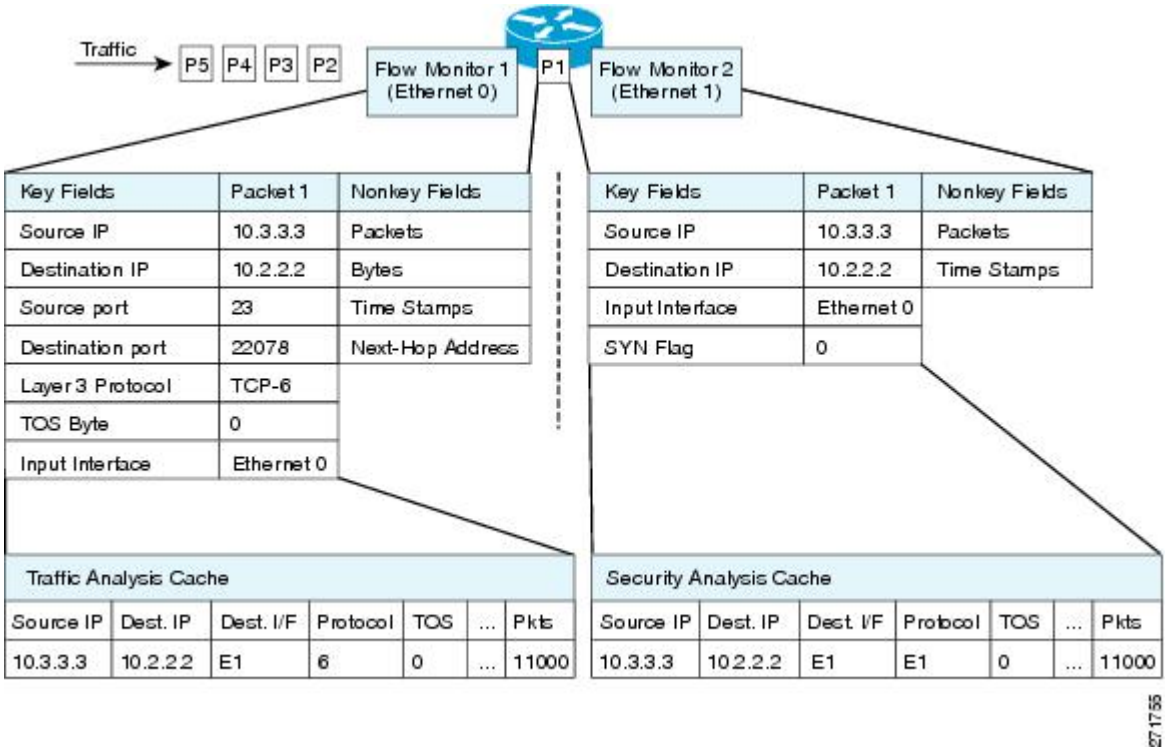
Flow Monitors

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

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

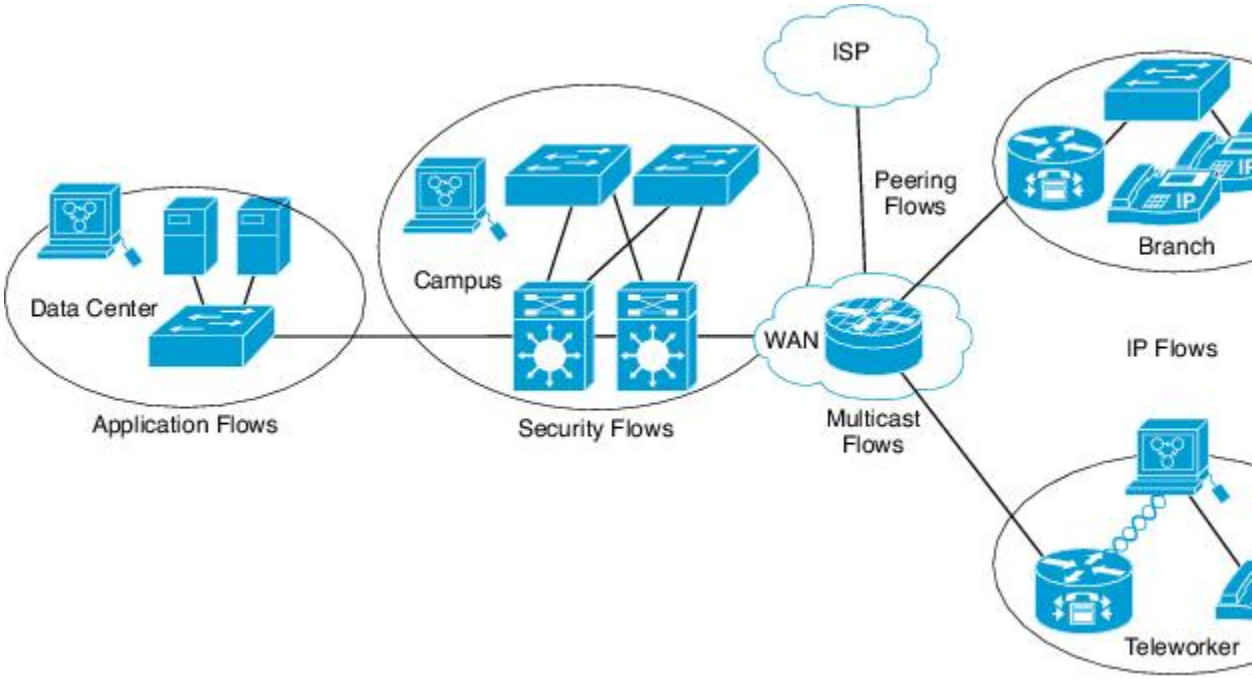
Flexible NetFlow can be used to perform different types of analysis on the same traffic. In the figure below, packet 1 is analyzed using a record designed for standard traffic analysis on the input interface and a record designed for security analysis on the output interface.

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



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

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



Normal

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

Flow Exporters

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

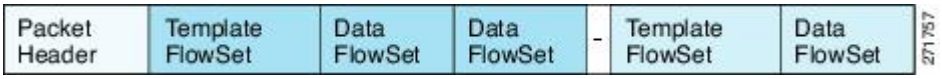
NetFlow Data Export Format Version 9

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

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

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

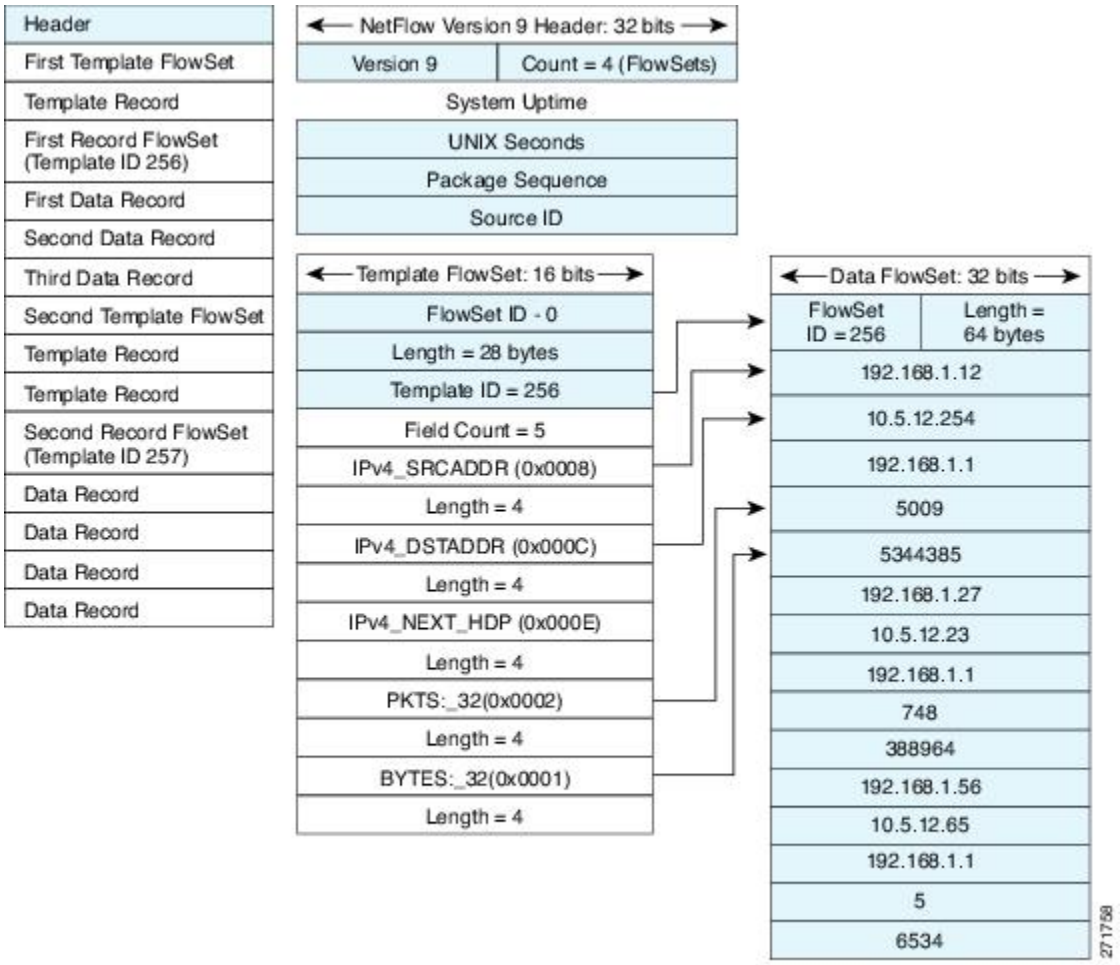
Figure 5 Version 9 Export Packet



NetFlow Version 9 will periodically export the template data so the NetFlow collector will understand what data is to be sent and also export the data flow set for the template. The key advantage to Flexible NetFlow is that the user configures a flow record, which is effectively converted to a Version 9 template and then

forwarded to the collector. The figure below is a detailed example of the NetFlow Version 9 export format, including the header, template flow, and data flow sets.

Figure 6 Detailed Example of the NetFlow Version 9 Export Format



For more information on the Version 9 export format, refer to the white paper titled Cisco IOS NetFlow Version 9 Flow-Record Format, 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 Flexible NetFlow 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.

Feature	Original NetFlow	Flexible NetFlow	Comments
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.
MPLS-Aware NetFlow	Supported	Not supported	--
MPLS Egress NetFlow	Supported	Supported	The Flexible NetFlow--MPLS Egress NetFlow feature implemented MPLS NetFlow egress support for Flexible NetFlow in Cisco IOS Release 12.4(22)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.
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	--

Feature	Original NetFlow	Flexible NetFlow	Comments
NetFlow MIB	Supported	Not supported	--
NetFlow MIB and Top Talkers	Supported	Not supported	--
NetFlow Multicast Support	Supported	Supported	In Cisco IOS Release 12.4(9)T through 12.4(20)T Flexible NetFlow collects statistics for multicast flows. However, specific additional fields such as replication counts for bytes and packets are not supported. The Flexible NetFlow--IPv4 Multicast Statistics Support feature implemented support for capturing multicast replication counts for bytes and packets in Cisco IOS Release 12.4(22)T.
NetFlow Layer 2 and Security Monitoring Exports	Supported	Partially supported	The Flexible NetFlow--Layer 2 Fields feature implemented support for capturing MAC addresses and virtual LAN (VLAN) IDs in Cisco IOS Release 12.4(22)T.
Egress NetFlow Accounting	Supported	Supported	Flexible NetFlow monitors can be used to monitor egress traffic on interfaces and subinterfaces.
NetFlow Reliable Export with SCTP	Supported	Not supported	--
NetFlow Dynamic Top Talkers CLI	Supported	Supported	The Flexible NetFlow--Top N Talkers Support feature implemented in Cisco IOS Release 12.4(22)T provides the same functionailty.

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

Where to Go Next

To implement a basic Flexible NetFlow configuration that emulates original NetFlow traffic analysis and data export, refer to the "Getting Started with Configuring Cisco IOS Flexible NetFlow" module. To implement other Flexible NetFlow configurations, refer to the Where to Go Next, page 13.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
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"
Customizing Flexible NetFlow for your network	"Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors"
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*

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

Getting Started with Configuring Cisco IOS Flexible NetFlow

This document contains information about and instructions for configuring Flexible NetFlow to emulate the data capture, data analysis, and data export features of original NetFlow. The Flexible NetFlow equivalents of some of the other features that have been added to original NetFlow, such as NetFlow Subinterface Support and Multiple Export Destinations, are described in this document. The purpose of this document is to help you start using Flexible NetFlow as quickly as possible, and explains how to configure certain Flexible NetFlow features but does not explain them in detail. The documents listed in the Getting Started with Configuring Cisco IOS Flexible NetFlow, page 15 contain more detailed information on Flexible NetFlow features.

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 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 at the end of this module.

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

Prerequisites for Getting Started with Configuring Flexible NetFlow

- You are familiar with the information in the " Cisco IOS Flexible NetFlow Overview " module.
- The networking device must be running a Cisco IOS release that supports Cisco IOS 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.

Restrictions for Getting Started with Configuring Flexible NetFlow

- Locally generated traffic (traffic that is generated by the router on which the Flexible NetFlow Output Accounting feature is configured) is not counted as flow traffic for the Output Flexible NetFlow Accounting feature.
- The Flexible NetFlow Output Accounting feature counts CEF-switched packets only. Process-switched transit packets are not counted.

Information About Getting Started with Configuring Flexible NetFlow

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.

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.

Field	Key or Nonkey Field	Definition
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.

The configuration in the How to Get Started with Configuring Flexible NetFlow, page 23 uses the predefined Flexible NetFlow "NetFlow original" record.

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.

Field	Key or Nonkey Field	Definition
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, page 31 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.

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.

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.

Field	Key or Nonkey Field	Definition
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.
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.

Flexible NetFlow MPLS Egress NetFlow

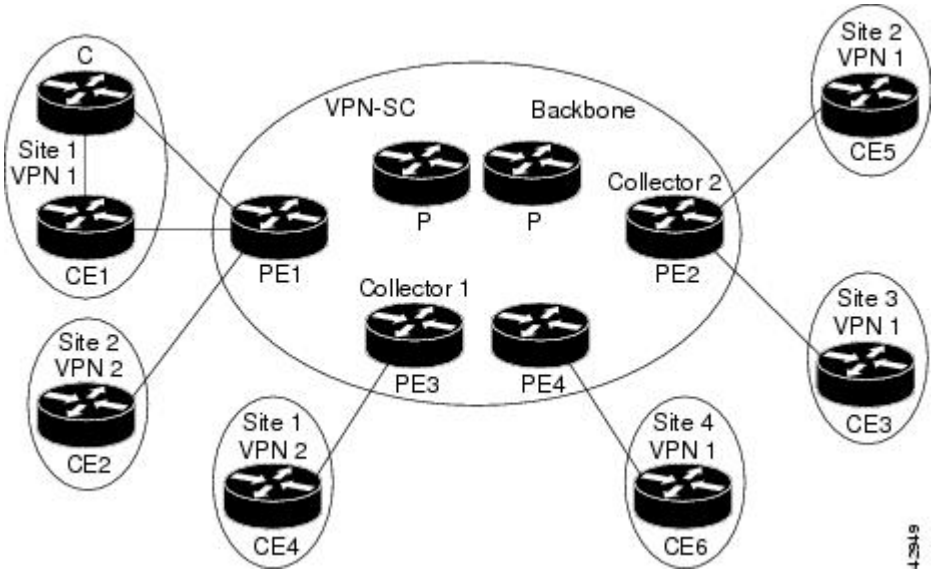
The Flexible NetFlow--MPLS Egress NetFlow feature allows you to capture IP flow information for packets that arrive on a router as Multiprotocol Label Switching (MPLS) packets and are transmitted as IP packets. This feature allows you to capture the MPLS VPN IP flows that are traveling through the service 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.

How to Get Started with Configuring Flexible NetFlow

The tasks in this section explain how to configure and verify the emulation of original (ingress) NetFlow data capture with Flexible NetFlow for traffic that is received by the router and how to configure and verify the emulation of original NetFlow data export with Flexible NetFlow.

Note Flexible NetFlow emulation of original NetFlow requires the configuration of a flow monitor and the application of the flow monitor to at least one interface that is receiving the traffic that you want to analyze.

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

- Configuring a Flow Monitor for IPv4 or IPv6 Traffic Using the Predefined Record, page 24
- Applying an IPv4 Flow Monitor to an Interface, page 25
- Applying an IPv6 Flow Monitor to an Interface, page 27
- Configuring a Flow Exporter for the Flow Monitor, page 29

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.

	Command or Action	Purpose
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.
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.

Applying an IPv4 Flow Monitor to an Interface

Before it can be activated an IPv4 flow monitor must be applied to at least one interface. To activate an IPv4 flow monitor, perform the following required task.

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* **input**
5. **end**
6. **show flow interface** *type number*
7. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip flow monitor** *monitor-name* **input** **Example:** `Router(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.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show flow interface** *type number* **Example:** `Router# show flow interface ethernet 0/0`	Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface.
Step 7	**show flow monitor name** *monitor-name* **cache format record** **Example:** `Router# 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.

Applying an IPv6 Flow Monitor to an Interface

Before it can be activated an IPv6 flow monitor must be applied to at least one interface. To activate an IPv6 flow monitor, perform the following required task.

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ipv6 flow monitor** *monitor-name* **input**
5. **end**
6. **show flow interface** *type number*
7. **show flow monitor name** *monitor-name* **cache format record**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ipv6 flow monitor** *monitor-name* **input** **Example:** `Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 input`	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show flow interface** *type number* **Example:** `Router# show flow interface ethernet 0/0`	Displays the status of Flexible NetFlow (enabled or disabled) on the specified interface.
Step 7	**show flow monitor name** *monitor-name* **cache format record** **Example:** `Router# 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 a Flow Exporter for the Flow Monitor

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, perform the following optional task.

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.

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.

	Command or Action	Purpose
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.

	Command or Action	Purpose
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.

Configuration Examples for Emulating Original NetFlow Features with Flexible 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 sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-output
```

```
 exit
!
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-output
 exit
!
ip cef
ipv6 cef
!
interface Ethernet0/0
 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 sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 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 monitor FLOW-MONITOR-2
 record netflow ipv6 original-input
 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 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 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
!
```

Where to Go Next

For information on advanced Flexible NetFlow configurations for specific purposes such as quality of service (QoS) and bandwidth monitoring, application and user flow monitoring and profiling, and security analysis, refer to the "Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors" module.

If you want to configure additional options for data export for Flexible NetFlow, refer to the "Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters" module.

If you want to configure flow sampling to reduce the CPU overhead of analyzing traffic, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module.

If you want to configure any of the predefined records for Flexible NetFlow refer, to the "Configuring Cisco IOS Flexible NetFlow with Predefined Records" module.

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"
Configuring flow exporters to export Flexible NetFlow data	"Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters"
Customizing Flexible NetFlow	"Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors"
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"

Related Topic	Document Title
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 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 6 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	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**,

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

Feature Name	Releases	Feature Information
Flexible NetFlow: Export to an IPv6 Address	15.2(2)T	This feature enables Flexible NetFlow to export data to a destination using an IPv6 address. The following commands were introduced or modified: **destination**
Flexible NetFlow: IPFIX Export Format	15.2(4)M	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**.

Configuring Cisco IOS Flexible NetFlow with Predefined Records

This module contains information about and instructions for configuring Flexible NetFlow using predefined records. Many of the Flexible NetFlow predefined records use the same key and nonkey fields as the aggregation caches available in original NetFlow. However, the predefined Flexible NetFlow records do not perform aggregation.

NetFlow is a Cisco IOS 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 at the end of this module.

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

Prerequisites for Flexible NetFlow with Predefined Records

- You are familiar with the information in the " Cisco IOS Flexible NetFlow Overview " module.

- The networking device must be running a Cisco IOS 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.

Restrictions for Flexible NetFlow with Predefined Records

Cisco IOS Release 12.2(50)SY

- Predefined records specifying mask and prefix are not supported.

Information About Configuring Flexible NetFlow with Predefined Records

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 7 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.

Field	Key or Nonkey Field	Definition
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.

The configuration in the How to Get Started with Configuring Flexible NetFlow, page 23 uses the predefined Flexible NetFlow "NetFlow original" record.

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 8 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.

Field	Key or Nonkey Field	Definition
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, page 31 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 9 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.

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.

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 10 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.

Field	Key or NonKey Field	Definition
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.
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 11 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).

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.

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 12 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).

Field	Key or Nonkey Field	Definition
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 13 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.

Field	Key or Nonkey Field	Definition
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 14 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).
IP Destination autonomous system	Key	Autonomous system of the destination IP address (peer or origin).

Field	Key or Nonkey Field	Definition
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 15 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.

Field	Key or Nonkey Field	Definition
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.
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 16 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).

Field	Key or Nonkey Field	Definition
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.
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 17 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).

Field	Key or Nonkey Field	Definition
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.
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 18 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.
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 19 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.
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.

Field	Key or Nonkey Field	Definition
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 20 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 21 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.

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.

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 22 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.

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.

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 23 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.

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.

How to Configure a Predefined Record for the Flow Monitor

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

- Configuring a Flow Monitor for IPv4 Traffic Using a Predefined Record, page 60
- Configuring a Flow Monitor for IPv6 Traffic Using a Predefined Record, page 62
- Applying an IPv4 Flow Monitor to an Interface, page 64
- Applying an IPv6 Flow Monitor to an Interface, page 65

Configuring a Flow Monitor for IPv4 Traffic Using a Predefined Record

To configure a flow monitor for IPv4 traffic using a 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 on 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-original** | **netflow ipv4** *record* [**peer**]}
6. **end**
7. **show flow record** *record-name*
8. **show running-config flow record** *record-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Router(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:** `Router(config-flow-monitor)# description Used for monitoring IPv4 traffic`	(Optional) Creates a description for the flow monitor.
Step 5	**record** {**netflow-original**	**netflow ipv4** *record* [**peer**]} **Example:** `Router(config-flow-monitor)# record netflow ipv4 original-input`	Specifies the record for the flow monitor.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config-flow-monitor)# end`	Exits Flexible NetFlowflow monitor configuration mode and returns to privileged EXEC mode.
Step 7	**show flow record** *record-name* **Example:** `Router# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.
Step 8	**show running-config flow record** *record-name* **Example:** `Router# show running-config flow record FLOW_RECORD-1`	(Optional) Displays the configuration of the specified flow record.

Configuring a Flow Monitor for IPv6 Traffic Using a Predefined Record

To configure a flow monitor for IPv6 traffic using a 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 on 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 ipv6** *record* [**peer**]
6. **end**
7. **show flow record** *record-name*
8. **show running-config flow record** *record-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**flow monitor** *monitor-name* **Example:** `Router(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 4	**description** *description* **Example:** `Router(config-flow-monitor)# description Used for monitoring IPv6 traffic`	(Optional) Creates a description for the flow monitor.
Step 5	**record netflow ipv6** *record* [**peer**] **Example:** `Router(config-flow-monitor)# record netflow ipv6 original-input`	Specifies the record for the flow monitor.
Step 6	**end** **Example:** `Router(config-flow-monitor)# end`	Exits Flexible NetFlow flow monitor configuration mode and returns to privileged EXEC mode.
Step 7	**show flow record** *record-name* **Example:** `Router# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.

	Command or Action	Purpose
Step 8	**show running-config flow record** *record-name* **Example:** `Router# show running-config flow record FLOW_RECORD-1`	(Optional) Displays the configuration of the specified flow record.

Applying an IPv4 Flow Monitor to an Interface

Before it can be activated, an IPv4 flow monitor must be applied to at least one interface. To activate an IPv4 flow monitor by applying the flow monitor to an interface, perform the following required task.

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

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

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow monitor** *monitor-name* {**input** | **output**}
5. **end**
6. **show flow monitor** *monitor-name*
7. **show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]]

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ip flow monitor** *monitor-name* {**input** | **output**} **Example:** `Router(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. • You can configure input and output traffic analysis concurrently by configuring the **ip flow monitor** *monitor-name* **input** and **ip flow monitor** *monitor-name* **output** commands on the same interface. You can use different flow monitors for input and output traffic analysis.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show flow monitor** *monitor-name* **Example:** `Router# show flow monitor FLOW_MONITOR-1`	(Optional) Displays the current status of the specified flow monitor.
Step 7	**show flow monitor** [[**name**] *monitor-name* [**cache** [**format** {**csv** | **record** | **table**}]][**statistics**]] **Example:** `Router# show flow monitor FLOW-MONITOR-1`	(Optional) Displays the status and statistics for a Flexible NetFlow flow monitor.

Applying an IPv6 Flow Monitor to an Interface

Before it can be activated, an IPv6 flow monitor must be applied to at least one interface. To activate an IPv4 flow monitor by applying the flow monitor to an interface, perform the following required task.

Note When you specify 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 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. **interface** *type number*
4. **ipv6 flow monitor** *monitor-name* {**input** | **output**}
5. **end**
6. **show flow monitor** *monitor-name*
7. **show running-config flow monitor** *monitor-name*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies an interface and enters interface configuration mode.
Step 4	**ipv6 flow monitor** *monitor-name* {**input** | **output**} **Example:** `Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 input`	Activates the flow monitor that you created previously by assigning it to the interface to analyze traffic. • You can configure input and output traffic analysis concurrently by configuring the **ipv6 flow monitor** *monitor-name* **input** and **ipv6 flow monitor** *monitor-name* **output** commands on the same interface. You can use different flow monitors for input and output traffic analysis.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.
Step 6	**show flow monitor** *monitor-name* **Example:** `Router# show flow monitor FLOW_MONITOR-1`	(Optional) Displays the current status of the specified flow monitor.
Step 7	**show running-config flow monitor** *monitor-name* **Example:** `Router# show flow monitor FLOW_MONITOR-1`	(Optional) Displays the configuration of the specified flow monitor.

Configuration Examples for Flexible NetFlow with Predefined Records

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 Ethernet 0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 input
!
```

Where to Go Next

For information on advanced Flexible NetFlow configurations for specific purposes such as quality of service (QoS) and bandwidth monitoring, application and user flow monitoring and profiling, and security analysis, refer to the "Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors" module.

If you want to configure flow sampling to reduce the CPU overhead of analyzing traffic, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module.

If you want to configure data export for Flexible NetFlow, refer to the "Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters" module.

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"
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"
Customizing Flexible NetFlow	"Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors"
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"
Using Flexible NetFlow Top N Talkers to analyze network traffic	"Using Cisco IOS Flexible NetFlow Top N Talkers to Analyze Network Traffic"

Related Topic	Document Title
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 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 24 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	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

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

Configuring Data Export for Flexible NetFlow with Flow Exporters

This document contains information about and instructions for configuring flow exporters to export Flexible NetFlow data to remote systems such as a UNIX server running NetFlow collector.

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 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 at the end of this module.

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

Prerequisites for Data Export for Flexible NetFlow with Flow Exporters

- You are familiar with the information in the "Cisco IOS Flexible NetFlow Overview" module.

- The networking device must be running a Cisco IOS or Cisco IOS XE 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.

Restrictions for Data Export for Flexible NetFlow with Flow Exporters

- 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 Data Export for Flexible NetFlow with Flow Exporters

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 Data Export for Flexible NetFlow with Flow Exporters

The tasks in this section explain how 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 collector. Flow exporters use UDP as the transport protocol.

Restrictions

Each flow exporter supports only one destination. If you want to export the data to multiple destinations, you must configure multiple flow exporters and assign them to the flow monitor. Flow exporters are added to flow monitors to enable data export from the flow monitor cache.

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

Configuring the Flow Exporter

To configure the flow exporter, perform the following required task.

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**flow exporter** *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.

	Command or Action	Purpose
Step 4	**description** *description* **Example:** `Device(config-flow-exporter)# description Exports to the datacenter`	(Optional) Configures a description to the exporter that will appear in the configuration and the display of the **show flow exporter** command.
Step 5	**destination** {*ip-address* | *hostname*} [**vrf** *vrf-name*] **Example:** `Device(config-flow-exporter)# destination 172.16.10.2`	Specifies the IP address or hostname of the destination system for the exporter. **Note** You can export to a destination using either an IPv4 or IPv6 address.
Step 6	**export-protocol** {**netflow-v5** | **netflow-v9** | **ipfix**} **Example:** `Device(config-flow-exporter)# export-protocol netflow-v9`	Specifies the version of the NetFlow export protocol used by the exporter. The export of extracted fields from NBAR is supported only over IPFIX. • Default: **netflow-v9**.
Step 7	**dscp** *dscp* **Example:** `Device(config-flow-exporter)# dscp 63`	(Optional) Configures differentiated services code point (DSCP) parameters for datagrams sent by the exporter. • The range for the *dscp* argument is from 0 to 63. Default: 0.
Step 8	**source** *interface-type interface-number* **Example:** `Device(config-flow-exporter)# source ethernet 0/0`	(Optional) Specifies the local interface from which the exporter will use the IP address as the source IP address for exported datagrams.
Step 9	**option** {**exporter-stats** | **interface-table** | **sampler-table**| **vrf-table**} [**timeout** *seconds*] **Example:** `Device(config-flow-exporter)# option exporter-stats timeout 120`	(Optional) Configures options data parameters for the exporter. • You can configure all three options concurrently. • The range for the *seconds* argument is 1 to 86,400. Default: 600.

Command or Action	Purpose
Step 10 **output-features** **Example:** `Device(config-flow-exporter)# output-features`	(Optional) Enables sending export packets using quality of service (QoS) and encryption.
Step 11 **template data timeout** *seconds* **Example:** `Device(config-flow-exporter)# template data timeout 120`	(Optional) Configure resending of templates based on a timeout. • The range for the *seconds* argument is 1 to 86400 (86400 seconds = 24 hours).
Step 12 **transport udp** *udp-port* **Example:** `Device(config-flow-exporter)# transport udp 650`	Specifies the UDP port on which the destination system is listening for exported datagrams. • The range for the *udp-port* argument is from 1 to 65536.
Step 13 **ttl** *seconds* **Example:** `Device(config-flow-exporter)# ttl 15`	(Optional) Configures the time-to-live (TTL) value for datagrams sent by the exporter. • The range for the *seconds* argument is from 1 to 255.
Step 14 **end** **Example:** `Device(config-flow-exporter)# end`	Exits flow exporter configuration mode and returns to privileged EXEC mode.
Step 15 **show flow exporter** *exporter-name* **Example:** `Device# show flow exporter FLOW_EXPORTER-1`	(Optional) Displays the current status of the specified flow exporter.
Step 16 **show running-config flow exporter** *exporter-name* **Example:** `Device# show running-config flow exporter FLOW_EXPORTER-1`	(Optional) Displays the configuration of the specified flow exporter.

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.

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. **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.

	Command or Action	Purpose
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	**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 ethernet 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.

	Command or Action	Purpose
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 Data Export with Flow Exporters

Example: Configuring Multiple Export Destinations

The following example shows how to configure multiple export destinations for Flexible NetFlow for IPv4 and 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 monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exporter EXPORTER-2
 exporter EXPORTER-1
!
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-input
 exporter EXPORTER-2
 exporter EXPORTER-1
!
ip cef
!
```

```
interface Ethernet 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:       netflow original-input
  Flow Exporter:     EXPORTER-1
                     EXPORTER-2
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

Example: Configuring Sending Export Packets Using QoS

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

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

This sample starts in global configuration mode:

```
!
flow record FLOW-RECORD-1
 match ipv4 source address
 collect counter packets
!
flow exporter FLOW-EXPORTER-1
 destination 10.0.1.2
 output-features
 dscp 18
!
flow monitor FLOW-MONITOR-1
 record FLOW-RECORD-1
 exporter FLOW-EXPORTER-1
 cache entries 1024
!
ip cef
!
class-map match-any COS3
!
policy-map PH_LABS_FRL_64k_16k_16k_8k_8k
 class COS3
  bandwidth percent 2
  random-detect dscp-based
  random-detect exponential-weighting-constant 1
  random-detect dscp 18 200 300 10
!
interface Ethernet 0/0
 ip address 10.0.0.1 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
interface Ethernet 0/1
 ip address 10.0.1.1 255.255.255.0
 service-policy output PH_LABS_FRL_64k_16k_16k_8k_8k
!
```

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

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

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
!
```

Where to Go Next

For information on advanced Flexible NetFlow configurations for specific purposes such as QoS and bandwidth monitoring, application and user flow monitoring and profiling, and security analysis, refer to the "Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors" module.

If you want to configure flow sampling to reduce the CPU overhead of analyzing traffic, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module.

If you want to configure any of the predefined records for Flexible NetFlow, refer to the "Configuring Cisco IOS Flexible NetFlow with Predefined Records" module.

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"
Emulating original NetFlow with Flexible NetFlow	"Getting Started with Configuring Cisco IOS Flexible NetFlow"
Customizing Flexible NetFlow	"Customizing Cisco IOS Flexible NetFlow Flow Records and Flow Monitors"
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 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 25 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	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**,

Feature Name	Releases	Feature Information
		template data timeout, **transport** (Flexible NetFlow).
Flexible NetFlow--IPv4 Unicast Flows	12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to monitor IPv4 traffic. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **collect routing**, **debug flow record**, **collect ipv4**, **collect ipv4 destination**, **collect ipv4 fragmentation**, **collect ipv4 section**, **collect ipv4 source**, **ip flow monitor**, **match ipv4**, **match ipv4 destination**, **match ipv4 fragmentation**, **match ipv4 section**, **match ipv4 source**, **match routing**, **record**, **show flow monitor**, **show flow record**.
Flexible NetFlow--NetFlow v9 Export Format	12.2(33)SRE 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1	Enables sending export packets using the Version 9 export format. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. No commands were introduced or modified by this feature.

Feature Name	Releases	Feature Information
Flexible NetFlow--IPv6 Unicast Flows	12.2(33)SRE 12.2(50)SY 12.4(20)T 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to monitor IPv6 traffic. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **collect routing**, **debug flow record**, **match routing**, **record**, **show flow monitor**, **show flow record**, **collect ipv6**, **collect ipv6 destination**, **collect ipv6 extension map**, **collect ipv6 fragmentation**, **collect ipv6 hop-limit**, **collect ipv6 length**, **collect ipv6 section**, **collect ipv6 source**, **collect transport icmp ipv6**, **ipv6 flow monitor**, **match ipv6**, **match ipv6 destination**, **match ipv6 extension map**, **match ipv6 fragmentation**, **match ipv6 hop-limit**, **match ipv6 length**, **match ipv6 section**, **match ipv6 source**, **match transport icmp ipv6**.
Flexible NetFlow--Output Features on Data Export	12.4(20)T	Enables sending export packets using QoS and encryption. The following command was introduced: **output-features**.
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	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**.

Feature Name	Releases	Feature Information
Flexible NetFlow: Export to an IPv6 Address	15.2(2)T	This feature enables Flexible NetFlow to export data to a destination using an IPv6 address. The following commands were introduced or modified: **destination**
Flexible NetFlow: IPFIX Export Format	15.2(4)M	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**.

Customizing Flexible NetFlow Flow Records and Flow Monitors

This document contains information about and instructions for customizing Cisco IOS Flexible NetFlow flow records and flow monitors. If the tasks and configuration examples in the "Getting Started with Configuring Cisco IOS Flexible NetFlow" module and the "Configuring Cisco IOS Flexible NetFlow with Predefined Records" module were not suitable for your traffic analysis requirements, you can use the information and instructions in this document to customize Flexible NetFlow to meet your traffic analysis requirements.

NetFlow is a Cisco IOS 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 at the end of this module.

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

Prerequisites for Customizing Flexible NetFlow Flow Records and Flow Monitors

- You are familiar with the information in the " Cisco IOS Flexible NetFlow Overview " module.
- You are familiar with the Flexible NetFlow key fields as they are defined in the following commands in the *Cisco IOS Flexible NetFlow Command Reference* :
  - **match flow**
  - **match interface**
  - **match** {**ipv4** | **ipv6**}
  - **match routing**
  - **match transpor**t
- You are familiar with the Flexible NetFlow nonkey fields as they are defined in the following commands in the *Cisco IOS Flexible NetFlow Command Reference* :
  - **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 IOS release that supports Flexible NetFlow.

IPv4 Traffic

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

IPv6 Traffic

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

Information About Customizing Flexible NetFlow Flow Records and Flow Monitors

- Criteria for Identifying Traffic To Be Used in Analysis in Flexible NetFlow, page 92

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. Rapid generation by the source of TCP SYN packets from random IP addresses can fill the connection queue and cause denial of TCP services (such as e-mail, file transfer, or WWW) 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.

How to Customize Flexible NetFlow Flow Records and Flow Monitors

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 Customized Flow Record, page 94

- Creating a Customized Flow Monitor, page 96
- Applying a Flow Monitor to an Interface, page 98

Configuring 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 explains the steps that are used to create one of the possible permutations. Modify the steps in these tasks as appropriate to create a customized flow record for your requirements.

To configure a customized flow record, perform the following task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow record** *record-name*
4. **description** *description*
5. **match** {**ipv4** | **ipv6**}{**destination** | **source**} **address**
6. Repeat Step 5 as required to configure additional key fields for the record.
7. **collect interface** {**input** | **output**}
8. Repeat Step 7 as required to configure additional nonkey fields for the record.
9. **end**
10. **show flow record** *record-name*
11. **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.

	Command or Action	Purpose
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** {**ipv4** | **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, refer to the *Cisco IOS Flexible NetFlow Command Reference* .
Step 6	Repeat Step 5 as required to configure additional key fields for the record.	--
Step 7	**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. For information on the other **collect** commands that are available to configure nonkey fields, refer to the *Cisco IOS Flexible NetFlow Command Reference* .
Step 8	Repeat Step 7 as required to configure additional nonkey fields for the record.	--
Step 9	**end** **Example:** `Device(config-flow-record)# end`	Exits Flexible NetFlow flow record configuration mode and returns to privileged EXEC mode.
Step 10	**show flow record** *record-name* **Example:** `Device# show flow record FLOW_RECORD-1`	(Optional) Displays the current status of the specified flow record.

	Command or Action	Purpose
Step 11	**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

To create a customized 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.

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

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

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

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • 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 ipv4 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 FLOW-RECORD-1`	Specifies the record for the flow monitor.
Step 6	**cache** {**entries** *number* | **timeout** {**active** |**inactive**|**update**} *seconds* | **type** {**immediate** | **normal** | **permanent**}} **Example:** `Device(config-flow-monitor)# cache type normal`	(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:** `Device(config-flow-monitor)# statistics packet protocol`	(Optional) Enables the collection of protocol distribution statistics for Flexible NetFlow monitors.
Step 9	**statistics packet size** **Example:** `Device(config-flow-monitor)# statistics packet size`	(Optional) Enables the collection of size distribution statistics for Flexible NetFlow monitors.
Step 10	**exporter** *exporter-name* **Example:** `Device(config-flow-monitor)# exporter EXPORTER-1`	(Optional) Specifies the name of an exporter that was 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 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 13	**show running-config flow monitor** *monitor-name* **Example:** `Device# 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. To activate a flow monitor, perform the following required task.

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.

	Command or Action	Purpose
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 Customizing Flow Records and Flow Monitors

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 sample 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 a Customized Flow Record Cache for Monitoring IPv6 Traffic

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

This sample starts in global configuration mode:

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

Example: Configuring Flexible NetFlow for Monitoring MAC and VLAN Statistics

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

This sample starts in global configuration mode:

```
!
 flow record LAYER-2-FIELDS-1
 match ipv4 source address
 match ipv4 destination address
 match datalink dot1q vlan output
 match datalink mac source address input
 match datalink mac source address output
 match datalink mac destination address input
 match flow direction
!
 exit
!
!
flow monitor FLOW-MONITOR-4
 record LAYER-2-FIELDS-1
 exit
!
ip cef
!
interface GigabitEthernet0/0/1
 ip address 172.16.6.2 255.255.255.0
 ip flow monitor FLOW-MONITOR-1 input
!
```

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 sample 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 Serial2/0
ip vrf forwarding green
ip address 172.16.2.2 255.255.255.252
ip flow monitor mm_1 output
!
end
```

Example: Configuring Flexible NetFlow for Network-Based Application Recognition

The following example uses Network-based Application recognition (NBAR) to create different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key field.

This sample starts in global configuration mode:

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

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
```

Where to Go Next

If you want to configure data export for Flexible NetFlow, refer to the "Configuring Data Export for Cisco IOS Flexible NetFlow with Flow Exporters" module.

If you want to configure flow sampling to reduce the CPU overhead of analyzing traffic, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module.

If you want to configure any of the predefined records for Flexible NetFlow, refer to the "Configuring Cisco IOS Flexible NetFlow with Predefined Records" module.

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 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 26 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	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**,

Feature Name	Releases	Feature Information
		template data timeout, **transport** (Flexible NetFlow).
Flexible NetFlow--IPv4 Unicast Flows	12.2(33)SRC 12.2(50)SY 12.4(9)T 15.0(1)SY 15.0(1)SY1	Enables Flexible NetFlow to monitor IPv4 traffic. Support for this feature was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC. The following commands were introduced or modified: **collect routing**, **debug flow record**, **collect ipv4**, **collect ipv4 destination**, **collect ipv4 fragmentation**, **collect ipv4 section**, **collect ipv4 source**, **ip flow monitor**, **match ipv4**, **match ipv4 destination**, **match ipv4 fragmentation**, **match ipv4 section**, **match ipv4 source**, **match routing**, **record**, **show flow monitor**, **show flow record**.
Flexible NetFlow--Layer 2 Fields	12.2(33)SRE 12.4(22)T	Enables collecting statistics for Layer 2 fields such as MAC addresses and virtual LAN (VLAN) IDs from traffic. Support for this feature was added for Cisco 7200 and 7300 Network Processing Engine (NPE) series routers in Cisco IOS Release 12.2(33)SRE. The following commands were introduced or modified: **collect datalink dot1q vlan** , **collect datalink mac**, **match datalink dot1q vlan**, **match datalink mac**.

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

Feature Name	Releases	Feature Information
Flexible NetFlow--NBAR Application Recognition	15.0(1)M	Network-based Application recognition (NBAR) enables creation of different flows for each application seen between any two IP hosts by applying a flow monitor having a flow record that collects the application name as a key or a nonkey field. The following commands were introduced or modified: **collect application name, match application name, option** (Flexible NetFlow), **show flow monitor.**
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.**
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.**

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 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 caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

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

Prerequisites for Using Flow Sampling

- 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 Flexible NetFlow Samplers

- Flow Samplers, page 112

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 Flexible NetFlow 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, page 112
- Configuring and Enabling Flow Sampling, page 114

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. To configure a 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 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.

	Command or Action	Purpose
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

To configure and enable a flow sampler, perform the following required task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **sampler** *sampler-name*
4. **description** *description*
5. **mode** {**deterministic** | **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.

	Command or Action	Purpose
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** {**deterministic** | **random**} **1 out-of** *window-size* **Example:** `Device(config-sampler)# mode random 1 out-of 2`	Specifies the sampler mode and the flow sampler window size. • The range for the *window-size* argument is from 2 to 32,768.
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.

	Command or Action	Purpose
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.

Configuration Examples for Using Flexible NetFlow Flow Sampling

Example: Configuring and Enabling a Deterministic Sampler for IPv4 Traffic

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

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-output
 exit
!
sampler SAMPLER-1
 mode deterministic 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 deterministic sampling for IPv4 input traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-1
 record netflow ipv4 original-input
 exit
!
```

```
sampler SAMPLER-1
 mode deterministic 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: Configuring and Enabling a Deterministic Sampler for IPv6 Traffic

The following example shows how to configure and enable deterministic sampling for IPv6 output traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-output
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 flow monitor FLOW-MONITOR-2 sampler SAMPLER-1 output
!
```

The following example shows how to configure and enable deterministic sampling for IPv6 input traffic.

This sample starts in global configuration mode:

```
!
flow monitor FLOW-MONITOR-2
 record netflow ipv6 original-input
 exit
!
sampler SAMPLER-1
 mode deterministic 1 out-of 2
 exit
!
ip cef
ipv6 cef
!
interface GigabitEthernet 0/0/0
 ipv6 address 2001:DB8:2:ABCD::2/48
 ipv6 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:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(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:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Router(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 flow monitor command again without the sampler keyword and argument:

```
Router(config)# interface GigabitEthernet 0/0/0
Router(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:

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

Additional References

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/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—Random 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 27 Feature Information for Flexible Netflow—Random 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** .