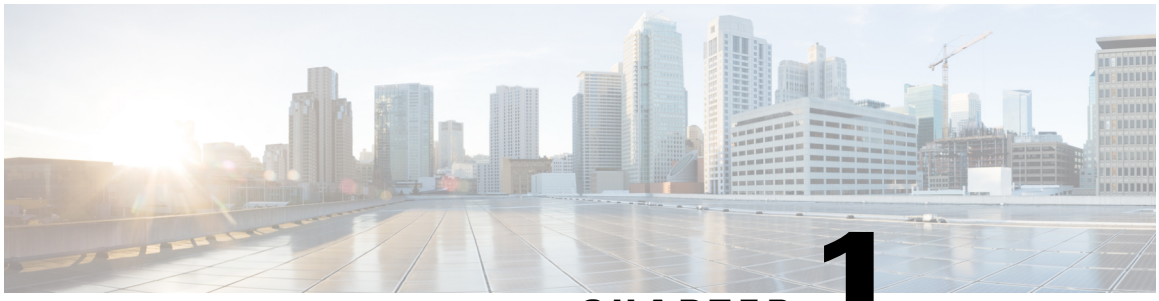
NetFlow Configuration Guide, Cisco IOS Release 15M&T

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS



CHAPTER 1

Cisco IOS NetFlow Overview

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology. This module provides an overview of the NetFlow application and advanced 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 Cisco IOS NetFlow

The NetFlow Application

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow identifies packet flows for both ingress and egress IP packets. It does not involve any connection-setup protocol, either between routers or to any other networking device or end station. NetFlow does not require any change externally--either to the packets themselves or to any networking device. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow capture and export are performed independently on each internetworking device; NetFlow need not be operational on each router in the network.

NetFlow is supported on IP and IP encapsulated traffic over most interface types and encapsulations. However, NetFlow does not support ATM LAN emulation (LANE) and does not support an Inter-Switch Link (ISL)/virtual LAN (VLAN), ATM, or Frame Relay interfaces when more than one input access control list (ACL) is used on the interface. Cisco 12000 IP Service Engine ATM line cards do not have this restriction when more than one input ACL is used on the interface.

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution data, IP flow switching cache information, and flow information. See the NetFlow Flows, on page 3.

NetFlow Benefits Monitoring Analysis and Planning Security and Accounting and Billing

NetFlow captures a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service (ToS) information that can be used for a wide variety of purposes such as network application and user monitoring, network analysis and planning, security analysis, accounting and billing, traffic engineering, and NetFlow data warehousing and data mining.

Network Application and User Monitoring

NetFlow data enables you to view detailed, time- and application-based usage of a network. This information allows you to plan and allocate network and application resources, and provides for extensive near real-time network monitoring capabilities. It can be used to display traffic patterns and application-based views. NetFlow provides proactive problem detection and efficient troubleshooting, and it facilitates rapid problem resolution. You can use NetFlow information to efficiently allocate network resources and to detect and resolve potential security and policy violations.

Network Planning

NetFlow can capture data over a long period of time, which enables you to track and anticipate network growth and plan upgrades. NetFlow service data can be used to optimize network planning, which includes peering, backbone upgrade planning, and routing policy planning. It also enables you 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) usage, and enables the analysis of new network applications. NetFlow offers valuable information that you can use to reduce the cost of operating the network.

Denial of Service and Security Analysis

You can use NetFlow data to identify and classify denial of service (DoS) attacks, viruses, and worms in real-time. Changes in network behavior indicate anomalies that are clearly reflected in NetFlow data. The data is also a valuable forensic tool that you can use to understand and replay the history of security incidents.

>Accounting and Billing

NetFlow data provides fine-grained metering for highly flexible and detailed resource utilization accounting. For example, flow data includes details such as IP addresses, packet and byte counts, timestamps,

type-of-service, and application ports. Service providers might utilize the information for billing based on time-of-day, bandwidth usage, application usage, or quality of service. Enterprise customers might utilize the information for departmental chargeback or cost allocation for resource utilization.

Traffic Engineering

NetFlow provides autonomous system (AS) traffic engineering details. You can use NetFlow-captured traffic data to understand source-to-destination traffic trends. This data can be used for load-balancing traffic across alternate paths or for forwarding traffic to a preferred route. NetFlow can measure the amount of traffic crossing peering or transit points to help you determine if a peering arrangement with other service providers is fair and equitable.

>NetFlow Data Storage and Data Mining

NetFlow data (or derived information) can be stored for later retrieval and analysis in support of marketing and customer service programs. For example, the data can be used to find out which applications and services are being used by internal and external users and to target those users for improved service and advertising. In addition, NetFlow data gives market researchers access to the who, what, where, and how long information relevant to enterprises and service providers.

NetFlow Cisco IOS Packaging Information

Cisco 7200/7500/7400/MGX/AS5800

Although NetFlow functionality is included in all software images for these platforms, you must purchase a separate NetFlow feature license. NetFlow licenses are sold on a per-node basis.

>Other Routers

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

NetFlow Flows

A NetFlow network flow is defined as a unidirectional stream of packets between a given source and destination. The source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is defined by the combination of the following seven key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might also contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format), depending on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Main Cache Operation

The key components of NetFlow are the NetFlow cache that stores IP flow information, and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. NetFlow maintains a flow record within the cache for each active flow. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine.

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers data for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers data for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers data for all egress MPLS-to-IP packets.

NetFlow Export Formats

NetFlow exports data in UDP datagrams in one of five formats: Version 9, Version 8, Version 7, Version 5, or Version 1. Version 9 export format, the latest version, is the most flexible and extensive format. Version 1 was the initial NetFlow export format; Version 7 is supported only on certain platforms, and Version 8 only supports export from aggregation cache. (Versions 2 through 4 and Version 6 were either not released or are not supported.)

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. The distinguishing feature of the NetFlow Version 9 format is that it is template based. Templates provide a means of extending the record format, a feature that should allow future enhancements to NetFlow services without requiring concurrent changes to the basic flow-record format. Internet Protocol Information Export (IPFIX) was based on the Version 9 export format.

- Version 8--A format added to support data export from aggregation caches. Version 8 allows export datagrams to contain a subset of the usual Version 5 export data, if that data is valid for a particular aggregation cache scheme.
- Version 7--A version supported on Catalyst 6000 series switches with a Multilayer Switch Feature Card (MSFC) on CatOS Release 5.5(7) and later.

On Catalyst 6000 series switches with an MSFC, you can export using either the Version 7 or Version 8 format.

Information about and instructions for configuring NetFlow on Catalyst 6000 series switches is available in the Catalyst 6500 Series Switches documentation.

- Version 5--A version that adds BGP autonomous system (AS) information and flow sequence numbers.
- Version 1, the initially released export format, is rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format for data export from the main cache.

For more information on a specific NetFlow data export format, see the "Configuring NetFlow and NetFlow Data Export" module.

NetFlow Operation Processing Order of NetFlow Features

The NetFlow application supports features that you can set up to further analyze network traffic data. NetFlow divides these features and services into the following three categories for processing:

- Preprocessing features that allow you to collect subsets of your network traffic data for analysis.
- Advanced features and services based on the flexible NetFlow Version 9 export format that allow you to collect data on types of traffic in addition to IP traffic.
- Postprocessing features that allow you to define fields that control how traffic data is exported.

You need to decide if you want to further analyze your network traffic. If you do want to do further analysis, you need to make choices in two areas:

- Do you want to customize or fine-tune the way that you collect NetFlow data? For example, you might want to configure packet sampling, or packet filtering, or an aggregation scheme.
- Do you want to collect and analyze data about the use of other Cisco IOS applications? For example, you might want to configure NetFlow support for BGP next hop, multicast, MPLS, or IPv6.

Before you configure or enable an additional NetFlow feature or service, you need to understand the prerequisites, restrictions, and key concepts that apply to each feature or service. Refer to the following sections for information about and links to the NetFlow features and services:

NetFlow Preprocessing Features Filtering and Sampling

The table below briefly describes preprocessing features and indicates where you can find concept and task information about each. You set up these features to select the subset of traffic of interest to you before NetFlow processing begins.

Table 1: NetFlow Preprocessing Features

Preprocessing Feature	Brief Description	Source for Concept and Task Information
Packet sampling	Sets up statistical sampling of network traffic for traffic engineering or capacity planning	See the "Using NetFlow Filtering or Sampling to Select the Network Traffic to Track" module.
Filtering	Sets up a specific subset of network traffic for class-based traffic analysis and monitoring on-network or off-network traffic	See the "Using NetFlow Filtering or Sampling to Select the Network Traffic to Track" module.

NetFlow Advanced Features and Services BGP Next Hop Multicast MPLS NetFlow Layer 2

The table below briefly describes advanced features and services supported by NetFlow and indicates where you can find concept and task information about each. Configure these features and services to collect and analyze NetFlow traffic statistics about them (features such as BGP Next Hop, multicast, and MPLS).

Table 2: NetFlow Advanced Features and Services

Feature or Service	Brief Description	Source for Concept and Task Information
BGP next hop support	Sets up the export of BGP next hop information for the purpose of measuring network traffic on a per BGP next hop basis	See the "Configuring NetFlow BGP Next Hop Support for Accounting and Analysis" module.
Multicast support	Sets up the capture of multicast-specific data that allows you to get a complete multicast traffic billing solution	See the "Configuring NetFlow Multicast Accounting" module.
MPLS support	Sets up the capture of MPLS traffic containing both IP and non-IP packets for use in MPLS network management, network planning, and enterprise accounting	See the "Configuring MPLS-aware NetFlow" module.
NetFlow Layer 2 and Security Monitoring Exports	Sets up the capture of Layer 2 and Layer 3 fields for use in security monitoring, network management, network planning, and enterprise accounting	See the "NetFlow Layer 2 and Security Monitoring Exports" module.

NetFlow Postprocessing Features Aggregation Schemes and Export to Multiple Destinations

The table below briefly describes postprocessing features and indicates where you can find concept and task information about each. You configure these features to set up the export of NetFlow data.

Table 3: NetFlow Postprocessing Features

Postprocessing Features	Brief Description	Source for Concept and Task Information
Aggregation schemes	Sets up extra aggregation caches with different combinations of fields that determine which traditional flows are grouped together and collected when a flow expires from the main cache	"Configuring NetFlow Aggregation Caches"
Export to multiple destinations	Sets up identical streams of NetFlow data to be sent to multiple hosts	"Configuring NetFlow and NetFlow Data Export"

NetFlow MIBs

The NetFlow MIB and the NetFlow MIB and Top Talkers features provide real time access to NetFlow cache information. These feature do not require a collector to obtain NetFlow data. This allows smaller enterprises to collect NetFlow data.

With the NetFlow MIB feature, you can access in real time the system information that is stored in the NetFlow cache by utilizing a MIB implementation based on the Simple Network Management Protocol (SNMP). This information is accessed by **get** and **set** commands entered on the network management system (NMS) workstation for which SNMP has been implemented. The NetFlow MIB feature provides MIB objects that allow you to monitor cache flow information, the current NetFlow configuration, and statistics. For details about the NetFlow MIB, see the "Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data" module.

The NetFlow MIB and Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. You can use this feature for security monitoring or accounting purposes for top talkers, and matching and identifying addresses for key users of the network. You configure the criteria by which flows from the NetFlow cache are sorted and placed in a special cache. The flows that are displayed by this feature are known as "top talkers." For details about the NetFlow MIB and Top Talkers, see the "Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands" module.

How to Configure Cisco IOS NetFlow

There are no tasks for the "Cisco IOS NetFlow Overview" module.

See the "Additional References" section for links to configuration information for NetFlow features and services.

Configuration Examples for Cisco IOS NetFlow

There are no configuration examples for the "Cisco IOS NetFlow Overview" module.

See the "Additional References" section for links to configuration information for NetFlow features and services.

Where to Go Next

To configure basic NetFlow, refer to the "Configuring NetFlow and NetFlow Data Export" module. See the "Additional References" section for links to configuration information about additional NetFlow features and services.

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	"Cisco IOS NetFlow Overview"
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	"Getting Started with Configuring NetFlow and NetFlow Data Export"
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	"Configuring NetFlow Aggregation Caches"
Tasks for configuring NetFlow BGP next hop support	"Configuring NetFlow BGP Next Hop Support for Accounting and Analysis"

Related Topic	Document Title
Tasks for configuring NetFlow multicast support	"Configuring NetFlow Multicast Accounting"
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	"NetFlow Layer 2 and Security Monitoring Exports"
Tasks for configuring the SNMP NetFlow MIB	"Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data"
Tasks for configuring the NetFlow MIB and Top Talkers feature	"Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands"
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	"Cisco CNS NetFlow Collection Engine Documentation"

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
• RFC 2460	Internet Protocol, Version 6 (IPv6) Specification

RFCs	Title
• RFC 3954	Cisco Systems NetFlow Services Export Version 9

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided into areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a certain destination.

flow --(NetFlow) A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

IPv6 --IP Version 6. Replacement for the current version of IP (Version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

ISL --Inter-Switch Link. Cisco-proprietary protocol that maintains VLAN information as traffic flows between switches and routers.

MPLS --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along normally routed paths (sometimes called MPLS hop-by-hop forwarding).

multicast --When single packets are copied by the network and sent to a specific subset of network addresses, they are said to be multicast. These addresses are specified in the Destination Address field.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the routing devices in the network. It is emerging as a primary network accounting and security technology.

NetFlow aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router

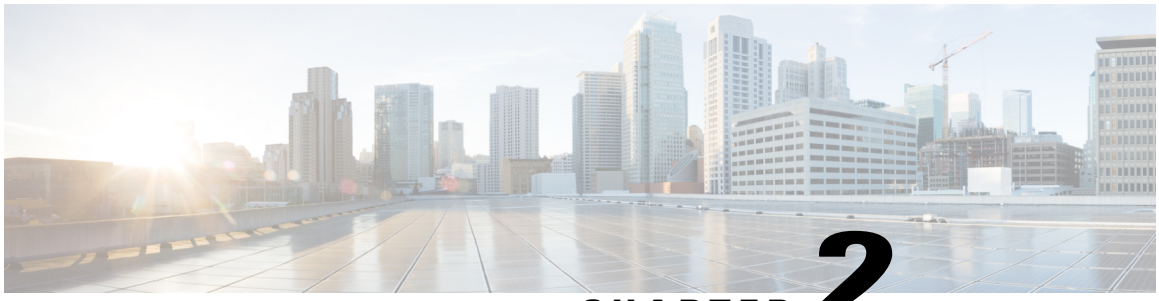
or switch that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow V9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

QoS --quality of service. A measure of performance for a transmission system that reflects the system's transmission quality and service availability.

traffic engineering --Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

VLAN --virtual LAN. Group of devices on one or more LANs that are configured (by management software) so that they can communicate as if they were attached to the same wire, when in fact they are located on a number of different LAN segments. Because VLANs are based on logical instead of physical connections, they are extremely flexible.



CHAPTER 2

Getting Started with Configuring Cisco IOS NetFlow and NetFlow Data Export

This module contains the minimum amount of information about and instructions necessary for configuring NetFlow to capture and export network traffic data. This module is intended to help you get started using NetFlow and NetFlow Data Export as quickly as possible. If you want more detailed information about this feature and instructions for configuring NetFlow and NetFlow Data Export, please refer to Configuring NetFlow and NetFlow Data Export.

NetFlow capture and export are performed independently on each internetworking device on which NetFlow is enabled. NetFlow need not be operational on each router in the network.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. NetFlow is emerging as a primary network accounting and security technology.

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 Configuring NetFlow and NetFlow Data Export

Before you enable NetFlow:

- Configure the router for IP routing.
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching.
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources.

Restrictions for Configuring NetFlow and NetFlow Data Export

NetFlow Data Capture

NetFlow consumes additional memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a smaller number of entries. The default cache size depends on the platform. For example, the default cache size for the Cisco 7500 router is 65536 (64K) entries.

Memory Impact

During times of heavy traffic, the additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T, the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later, the **ip flow ingress** command is used to enable NetFlow on an interface.

Egress NetFlow Accounting in Cisco IOS 12.3T Releases, 12.3(11)T, or Later

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. MPLS statistics are not captured. The MPLS Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrived at the router as MPLS packets and underwent label disposition.

Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

Locally generated traffic (traffic that is generated by the router on which the Egress NetFlow Accounting feature is configured) is not counted as flow traffic for the Egress NetFlow Accounting feature.

Note In Cisco IOS 12.2S releases, egress NetFlow captures either IPv4 packets or MPLS packets as they leave the router.

The Egress NetFlow Accounting feature counts CEF-switched packets only. Process-switched transit packets are not counted.

NetFlow Data Export

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets) versus Version 5. The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

Information About Configuring NetFlow and NetFlow Data Export

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers statistics for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers statistics for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers statistics for all egress MPLS-to-IP packets.

NetFlow Flows Key Fields

A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and by transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format) that depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Data Export Using the Version 9 Export Format

NetFlow Data Export format Version 9 is a flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. The Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.

How to Configure NetFlow and NetFlow Data Export

Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format

Perform this task to configure NetFlow and NetFlow Data Export using the Version 9 export format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*
4. Repeat Step 3 once to configure a second NetFlow export destination.
5. **ip flow-export version 9**
6. **interface** *interface-type interface-number*
7. **ip flow** {**ingress** | **egress**}
8. **exit**
9. Repeat Steps 6 through 8 to enable NetFlow on other interfaces
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	(Optional) IP address or hostname of the workstation to which you want to send the NetFlow information and the number of the UDP port on which the workstation is listening for this input. **Note** The workstation is running an application such as NetFlow Collection Engine (NFC) that is used to analyze the exported data.
Step 4	Repeat Step 3 once to configure a second NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.
Step 5	**ip flow-export version 9** **Example:** `Router(config)# ip flow-export version 9`	(Optional) Enables the export of information in NetFlow cache entries. • The **version 9**keyword specifies that the export packet uses the Version 9 format. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card CEF tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.

	Command or Action	Purpose
Step 6	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 7	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface. • **egress** --Captures traffic that is being transmitted by the interface.
Step 8	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 9	Repeat Steps 6 through 8 to enable NetFlow on other interfaces	(Optional) --
Step 10	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Verifying That NetFlow Is Operational and View NetFlow Statistics

To verify that NetFlow is working properly, perform this optional task.

SUMMARY STEPS

1. **show ip flow interface**
2. **show ip cache flow**
3. **show ip cache verbose flow**

DETAILED STEPS

Step 1 **show ip flow interface**

Use this command to display the NetFlow configuration for an interface. The following is sample output from this command:

Example:

```
Router# show ip flow interface
Ethernet0/0
  ip flow ingress
```

Step 2 **show ip cache flow**

Use this command to verify that NetFlow is operational and to display a summary of the NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.8    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.1    1799.6       0.9
ICMP               135      0.0      1133   427      3.1    1799.6       0.8
Total:             945      0.0      1166    91     22.4    1799.6       0.8
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.67.6    Et1/0.1       172.16.10.200   01 0000 0C01    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0043 0043    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0045 0045    51
Et0/0         10.234.53.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 0044 0044    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 00A2 00A2    51
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0014 0014    50
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0015 0015    52
.
.
.
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0087 0087    50
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0050 0050    51
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0089 0089    49
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0050 0050    50
Et0/0         10.251.10.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.162.37.71    Null          172.16.11.3     06 027C 027C    49
```

Step 3 **show ip cache verbose flow**

Use this command to verify that NetFlow is operational and to display a detailed summary of the NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (1130681 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2992518 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.6    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.0    1799.6       0.9
ICMP               135      0.0      1133   427      3.0    1799.6       0.8
Total:             945      0.0      1166    91     21.9    1799.6       0.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0          192.168.67.6    Et1/0.1        172.16.10.200   01 00  10     799
0000 /0  0                     0C01 /0  0     0.0.0.0                28  1258.1
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0043 /0  0                     0043 /0  0     0.0.0.0                28  1258.0
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0045 /0  0                     0045 /0  0     0.0.0.0                28  1258.0
Et0/0          10.234.53.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0                28  1258.1
Et0/0          10.10.19.1      Null           172.16.11.6     11 00  10     799
0044 /0  0                     0044 /0  0     0.0.0.0                28  1258.1
.
.
.
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0087 /0  0                     0087 /0  0     0.0.0.0                40  1258.1
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     798
0089 /0  0                     0089 /0  0     0.0.0.0                40  1256.5
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
Et0/0          10.251.10.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0              1500  1258.1
Et0/0          10.162.37.71    Null           172.16.11.3     06 00  00     798
027C /0  0                     027C /0  0     0.0.0.0                40  1256.4
```

Verifying That NetFlow Data Export Is Operational

To verify that NetFlow data export is operational and to view the statistics for NetFlow data export perform the step in this optional task.

SUMMARY STEPS

1. **show ip flow export**

DETAILED STEPS

show ip flow export
Use this command to display the statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

Example:

```
Router# show ip flow export
Flow export v9 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source interface Ethernet0/0
  Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
```

Configuration Examples for Configuring NetFlow and NetFlow Data Export

Example Configuring Egress NetFlow Accounting

The following example shows how to configure Egress NetFlow Accounting:

```
configure terminal
!
interface ethernet 0/0
 ip flow egress
!
```

Example Configuring NetFlow Subinterface Support

NetFlow Subinterface Support For Ingress (Received) Traffic On a Subinterface

```
configure terminal
!
interface ethernet 0/0.1
 ip flow ingress
!
```

NetFlow SubInterface Support For Egress (Transmitted) Traffic On a Subinterface

```
configure terminal
!
interface ethernet 1/0.1
 ip flow egress
!
```

Note NetFlow performs additional checks for the status of each subinterface that requires more CPU processing time and bandwidth. If you have several subinterfaces configured and you want to configure NetFlow data capture on all of them, we recommend that you configure NetFlow on the main interface instead of on the individual subinterfaces.

Example Configuring NetFlow Multiple Export Destinations

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

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export destination 172.16.10.2 9991
!
```

Note You can configure a maximum of two export destinations for the main cache and for each aggregation cache.

Example Configuring NetFlow and NetFlow Data Export Using the Version 9 Export Format

The following example shows how to configure NetFlow and NetFlow data export using the Version 9 export format:

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export version 9
!
```

Example Configuring NetFlow for Analyzing PPPoE Session Traffic

If you want to obtain accurate NetFlow traffic statistics for PPPoE sessions, you must configure NetFlow on the virtual-template interface, not on the physical interface that is configured with VLAN encapsulation. For example, if you configure NetFlow on the physical interface that is configured for VLAN encapsulation as shown in the following configuration, the NetFlow traffic statistics will not be an accurate representation of the traffic on the PPPoE sessions.

```
!
interface GigabitEthernet2/0/0.10
 encapsulation dot1Q 10
 ip flow egress
 pppoe enable
```

The following example shows how to configure egress NetFlow on a virtual template interface so that you can accurately analyze the packet size distribution statistics of the traffic that the router is sending to the end user over the PPoE session:

```
interface Virtual-Template 1
 ip unnumbered ethernet 0
 encapsulation ppp
 ip flow egress
```

The following display output from the **show ip cache flow** command shows that this PPPoE session traffic is comprised primarily of 1536-byte packets.

```
Router# show ip cache flow
IP packet size distribution (11014160 total packets):
  1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
  .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
   512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
  .000 .000 .000 .000 .999 .000 .000 .000 .000 .000 .000
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track

Related Topic	Document Title
Tasks for configuring random sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation
Configuration commands for NetFlow	*Cisco IOS NetFlow Command Reference*

Standards

Standards	Title
No new or modified standards are supported , and support for existing standards has not been modified.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported, and support for existing MIBs has not been modified.	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

RFCs	Title
No new or modified RFCs are supported, and support for existing RFCs has not been modified .	--

Technical Assistance

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

Feature Information for Configuring NetFlow and NetFlow Data Export

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

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

Table 4: Feature Information for Configuring NetFlow and NetFlow Data Export

Feature Name	Releases	Feature Configuration Information
Egress NetFlow Accounting	12.3(11)T 15.0(1)S	The Egress NetFlow Accounting feature allows NetFlow statistics to be gathered on egress traffic that is exiting the router. Previous versions of NetFlow allow statistics to be gathered only on ingress traffic that is entering the router. The following commands were introduced by this feature: **ip flow egress** and **ip flow-egress input-interface**. The following commands were modified by this feature: **flow-sampler**, **match**, **show ip cache flow**, **show ip cache verbose flow**, and **show ip flow interface**.
NetFlow Multiple Export Destinations	12.0(19)S 12.2(2)T 12.2(14)S 15.0(1)S	The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. The following commands were modified by this feature: **ip flow-aggregation cache**, **ip flow-export destination**, and **show ip flow export**.
NetFlow Subinterface Support	12.0(22)S 12.2(14)S 12.2(15)T	The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. The following command was introduced by this feature: **ip flow ingress**. The following command was modified by this feature: **show ip interface**.

Feature Name	Releases	Feature Configuration Information
NetFlow v9 Export Format	12.0(24)S 12.2(18)S 12.2(27)SBC 12.2(18)SXF 12.3(1) 15.0(1)S	The NetFlow v9 Export Format is flexible and extensible, which provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, NAT, and BGP next hop. The following commands were modified by this feature: **debug ip flow export**, **export**, **ip flow-export**, and **show ip flow export**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

CEF --Cisco Express Forwarding. Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used by a router to reach a certain destination.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --Type of packet built by a device (for example, a router) with NetFlow services enabled that is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information on IP flows).

fast switching --Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

MPLS --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along a normally routed path (sometimes called MPLS hop-by-hop forwarding).

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

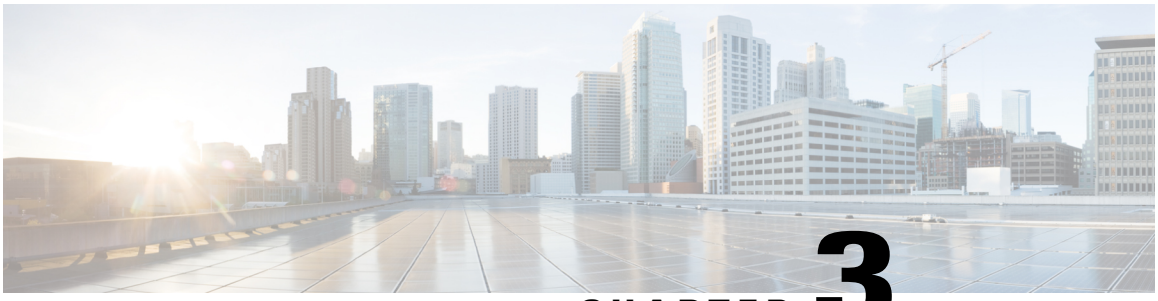
NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This

feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

RP --Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. Sometimes called a Supervisory Processor.



CHAPTER 3

Configuring NetFlow and NetFlow Data Export

This module contains information about and instructions for configuring NetFlow to capture and export network traffic data. NetFlow capture and export are performed independently on each internetworking device on which NetFlow is enabled. NetFlow need not be operational on each router in the network.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. NetFlow is a primary network accounting and security technology.

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 Configuring NetFlow and NetFlow Data Export

Before you enable NetFlow, you must do the following:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding, distributed Cisco Express Forwarding, or fast switching
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources

Restrictions for Configuring NetFlow and NetFlow Data Export

Preset Size of NetFlow Cache

NetFlow consumes additional memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a smaller number of entries. The default cache size depends on the platform.

Egress NetFlow Accounting in Cisco IOS XE Release 2.1 or Later Releases

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. Multiprotocol Label Switching (MPLS) statistics are not captured. The Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrived at the router as MPLS packets and underwent label disposition.

Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

Locally generated traffic (traffic that is generated by the router on which the Egress NetFlow Accounting feature is configured) is not counted as flow traffic for the Egress NetFlow Accounting feature.

Note Egress NetFlow captures IPv4 packets as they leave the router.

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8.
- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets). The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.
- Management Interface--NetFlow data export is not supported through the Management Interface port.

Policy-Based Routing and NetFlow Data Export

If a local policy is configured, an Aggregation Services Router (ASR) checks the injected packet and applies policy-based routing (PBR) to the packet. When NetFlow Data Export (NDE) packets are injected in the data

path during Cisco Express Forwarding lookup, the PBR local policy is not applied to the NDE packets. Therefore, NDE features on ASR cannot work with PBR.

NetFlow Data Capture

NetFlow consumes a significant amount of memory. If you have memory constraints, you might want to preset the size of the NetFlow cache so that it contains a lower number of entries. The default cache size depends on the platform. For example, the default cache size for the Cisco 7500 router is 65,536 (64K) entries.

Memory Impact

During times of heavy traffic, additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T, the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or a later release, use the **ip flow ingress** command to enable NetFlow on an interface.

Cisco IOS Releases 12.4(20)T or Earlier Releases

The **ip flow ingress** command behavior depends on the Cisco IOS release:

If your router is running a version earlier than Cisco IOS Release 12.4(20)T, and your router does not have a VPN Service Adapter (VSA)-enabled interface, enabling the **ip flow ingress**command will result in the ingress traffic being accounted for twice by the router.

If your router is running a version earlier than Cisco IOS Release 12.4(20)T, and your router has a VSA-enabled interface, enabling the **ip flow ingress** command will result in the encrypted ingress traffic being accounted for only once.

If your router is running a version of Cisco IOS Release12.4(20)T or later, enabling the **ip flow ingress** command will result in the encrypted ingress traffic being accounted for only once.

Egress NetFlow Accounting in Cisco IOS 12.3T Releases, 12.3(11)T, or Later Releases

The Egress NetFlow Accounting feature captures NetFlow statistics for IP traffic only. Multiprotocol Label Switching (MPLS) statistics are not captured. The MPLS Egress NetFlow Accounting feature can be used on a provider edge (PE) router to capture IP traffic flow information for egress IP packets that arrive at the router as MPLS packets and undergo label disposition.

Egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

Locally generated traffic (traffic that is generated by the router on which the Egress NetFlow Accounting feature is configured) is not counted as flow traffic for the Egress NetFlow Accounting feature.

Note In Cisco IOS 12.2S releases, egress NetFlow captures either IPv4 or MPLS packets as they leave the router.

NetFlow Data Export

NetFlow export is not supported over IPSec VPN if the source of the NetFlow data is the same device at which the VPN tunnel is terminated. In such a situation, the NetFlow packets will egress the crypto-map interface in clear text. This may cause issues with ISP connections (cellular interfaces) due to RFC 1918 anti-spoofing. As an alternative, you can use Flexible NetFlow with the **output-features** command.

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.
- Export bandwidth--The export bandwidth use increases for Version 9 (because of template flowsets) when compared to Version 5. The increase in bandwidth usage varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets; this has a bandwidth cost of about 4 percent. If required, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases the overall performance because generating and maintaining valid template flowsets requires additional processing.

Restrictions for NetFlow Version 8 Export Format

Version 8 export format is available only for aggregation caches; it cannot be expanded to support new features.

Restrictions for NetFlow Version 5 Export Format

Version 5 export format is suitable only for the main cache; it cannot be expanded to support new features.

Restrictions for NetFlow Version 1 Export Format

The Version 1 format was the initially released version. Do not use the Version 1 format unless you are using a legacy collection system that requires it. Use Version 9 or Version 5 export format.

Information About Configuring NetFlow and NetFlow Data Export

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers statistics for the following ingress IP packets:

- IP-to-IP packets
- IP-to-MPLS packets
- Frame Relay-terminated packets
- ATM-terminated packets

NetFlow captures data for all egress (outgoing) packets through the use of the following features:

- Egress NetFlow Accounting--NetFlow gathers statistics for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers statistics for all egress MPLS-to-IP packets.

NetFlow Flows Key Fields

A network flow is identified as a unidirectional stream of packets between a given source and destination--both are defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is identified as the combination of the following key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service (ToS)
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field that is different from another packet, it is considered to belong to another flow. A flow might contain other accounting fields (such as the autonomous system number in the NetFlow export Version 5 flow format) that depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Cache Management and Data Export

The key components of NetFlow are the NetFlow cache or data source that stores IP flow information and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. A flow record is maintained within the NetFlow cache for each active flow. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device such as the NetFlow Collection Engine.

NetFlow is efficient, with the amount of export data being about 1.5 percent of the switched traffic in the router. NetFlow accounts for every packet (nonsampled mode) and provides a highly condensed and detailed view of all network traffic that enters the router or switch.

The key to NetFlow-enabled switching scalability and performance is highly intelligent flow cache management, especially for densely populated and busy edge routers handling large numbers of concurrent, short duration flows. The NetFlow cache management software contains a highly sophisticated set of algorithms for efficiently determining whether a packet is part of an existing flow or whether the packet requires a new flow cache entry. The algorithms are also capable of dynamically updating the per-flow accounting measurements that reside in the NetFlow cache, and determining cache aging or flow expiration.

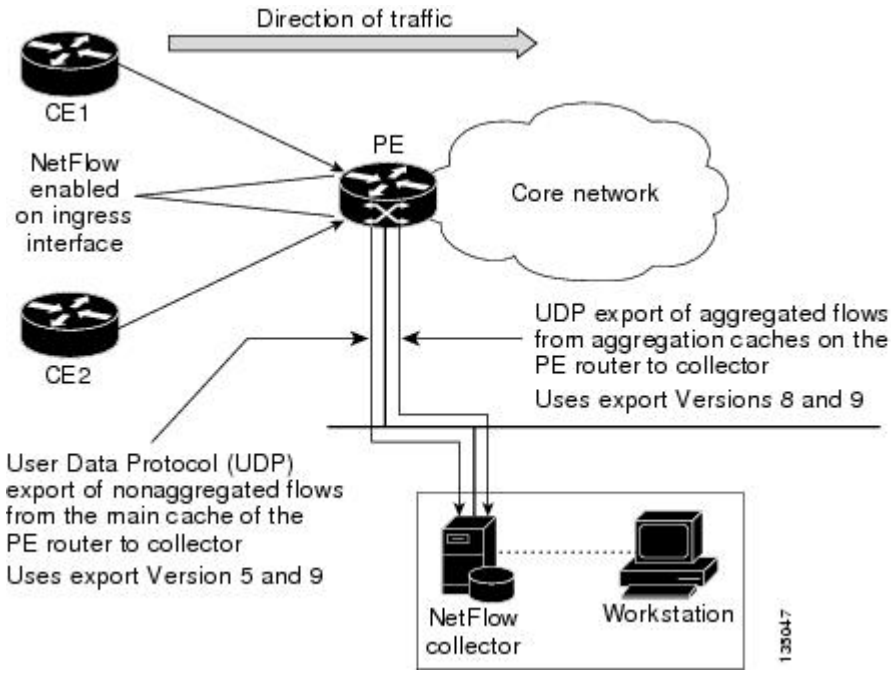
The rules for expiring NetFlow cache entries include the following:

- Flows that have been idle for a specified time are expired and removed from the cache.
- Long lived flows are expired and removed from the cache. (Flows are not allowed to live for more than 30 minutes by default; the underlying packet conversation remains undisturbed.)

- As the cache becomes full, a number of heuristics are applied to aggressively age groups of flows simultaneously.
- TCP connections that have reached the end of the byte stream (FIN) or have been reset (RST) are expired.

Expired flows are grouped into "NetFlow export" datagrams for export from the NetFlow- enabled device. NetFlow export datagrams can consist of up to 30 flow records for Version 5 or Version 9 flow export. The NetFlow functionality is configured on a per-interface basis. To configure NetFlow export capabilities, you need to specify the IP address and application port number of the Cisco NetFlow or third-party flow collector. The flow collector is a device that provides NetFlow export data filtering and aggregation capabilities. The figure below shows an example of NetFlow data export from the main and aggregation caches to a collector.

Figure 1: NetFlow Data Export from the Main and Aggregation Caches



NetFlow Export Format Versions 9 8 5 and 1

Overview

NetFlow exports data in UDP datagrams in one of the following formats: Version 9, Version 8, Version 7, Version 5, or Version 1:

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and Border Gateway Protocol (BGP) next hop. The Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extensible, so you can use the same export format with future features.

- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme.
- Version 5--A later enhanced version that adds BGP-AS information and flow sequence numbers. (Versions 2 through 4 were not released.) This is the most commonly used format.
- Version 1--The initially released export format that is rarely used today. Do not use the Version 1 export format unless the legacy collection system that you are using requires it. Use either the Version 9 export format or the Version 5 export format.

Details

The following sections provide more detailed information on NetFlow Data Export Formats:

NetFlow Export Version Formats

For all export versions, the NetFlow export datagram consists of a header and a sequence of flow records. The header contains information such as sequence number, record count, and system uptime. The flow record contains flow information such as IP addresses, ports, and routing information.

The NetFlow Version 9 export format is the newest NetFlow export format. The distinguishing feature of the NetFlow Version 9 export format is that it is template based. Templates make the record format extensible. This feature allows future enhancements to NetFlow without requiring concurrent changes to the basic flow-record format.

The use of templates with the NetFlow Version 9 export format provides several other key benefits:

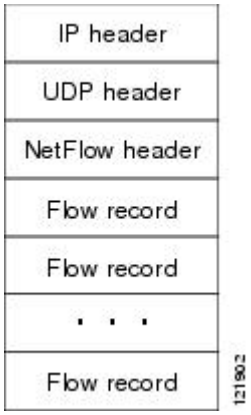
- You can export almost any information from a router or switch, including Layer 2 through 7 information, routing information, and IP Version 6 (IPv6), IP Version 4 (IPv4), Multicast, and MPLS information. This new information allows new applications of export data and provides new views of network behavior.
- Third-party business partners who produce applications that provide collector or display services for NetFlow are not required to recompile their applications each time a new NetFlow export field is added. Instead, they might be able to use an external data file that documents the known template formats.
- New features can be added to NetFlow more quickly, without breaking current implementations.
- Netflow is "future proofed" because the Version 9 export format can be adapted to provide support for new and developing protocols and other non-NetFlow-based approaches to data collection.

The work of the IETF IP, Information Export (IPFIX) Working Group (WG), and the IETF Pack Sampling (PSAMP) WG are based on the NetFlow Version 9 export format.

The Version 1 export format was the original format supported in the initial Cisco IOS software releases containing the NetFlow functionality; it is rarely used today. The Version 5 export format is an enhancement that adds BGP autonomous system information and flow sequence numbers. Versions 2 through 4 and Version 6 export formats were either not released or not supported. The Version 8 export format is the NetFlow export format to use when you enable router-based NetFlow aggregation on Cisco IOS router platforms.

The figure below shows a typical datagram used for NetFlow fixed format export Versions 1, 5, 7, and 8.

Figure 2: Typical Datagram for NetFlow Fixed Format Export Versions 1, 5, 7, 8

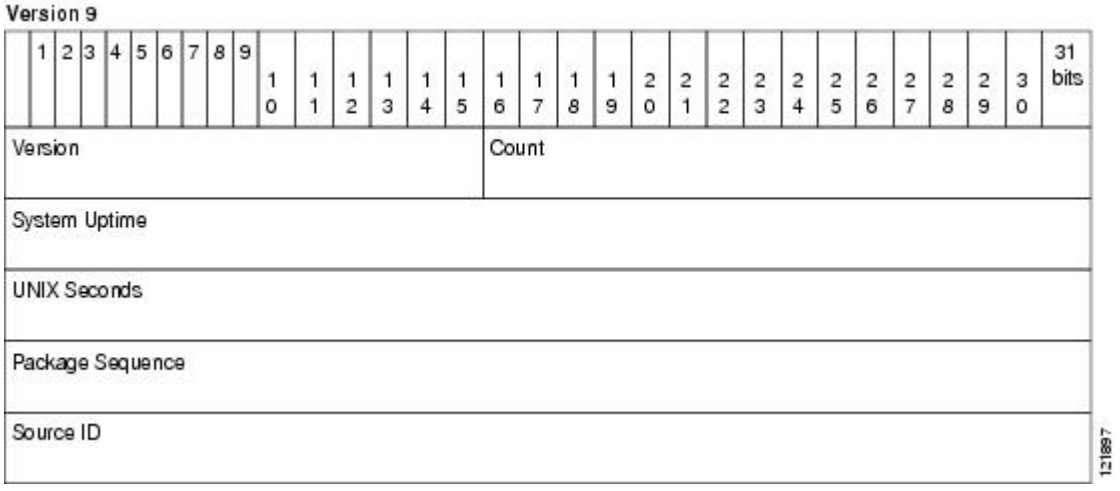


NetFlow Export Packet Header Format

In all the five export versions, the datagram consists of a header and one or more flow records. The first field of the header contains the version number of the export datagram. Typically, a receiving application that accepts any of the format versions allocates a buffer large enough for the largest possible datagram from any of the format versions and then uses the header to determine how to interpret the datagram. The second field in the header contains the number of records in the datagram (indicating the number of expired flows represented by this datagram). Datagram headers for NetFlow Export Versions 5, 8, and 9 also include a "sequence number" field used by NetFlow collectors to check for lost datagrams.

The NetFlow Version 9 export packet header format is shown in the figure below.

Figure 3: NetFlow Version 9 Export Packet Header Format



The table below lists the NetFlow Version 9 export packet header field names and descriptions.

Table 5: NetFlow Version 9 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	The version of NetFlow records exported in this packet; for Version 9, this value is 0x0009.
Count	Number of FlowSet records (both template and data) contained within this packet.
System Uptime	Time in milliseconds since this device was first booted.
UNIX Seconds	Seconds since 0000 Coordinated Universal Time (UTC) 1970.
Package Sequence	Incremental sequence counter of all export packets sent by this export device; this value is cumulative, and it can be used to learn whether any export packets have been missed. This is a change from the NetFlow Version 5 and Version 8 headers, where this number represented "total flows."
Source ID	The Source ID field is a 32-bit value that is used to guarantee uniqueness for each flow exported from a particular device. (The Source ID field is the equivalent of the engine type and engine ID fields found in the NetFlow Version 5 and Version 8 headers.) The format of this field is vendor specific. In Cisco's implementation, the first two bytes are reserved for future expansion and are always zero. Byte 3 provides uniqueness with respect to the routing engine on the exporting device. Byte 4 provides uniqueness with respect to the particular line card or Versatile Interface Processor on the exporting device. Collector devices should use the combination of the source IP address and the Source ID field to associate an incoming NetFlow export packet with a unique instance of NetFlow on a particular device.

NetFlow Flow Record and Export Format Content Information

This section gives details about the Cisco export format flow record. The table below indicates which flow record format fields are available for Versions 5 and 9. ('Yes' indicates that the field is available. 'No' indicates that the field is not available.)

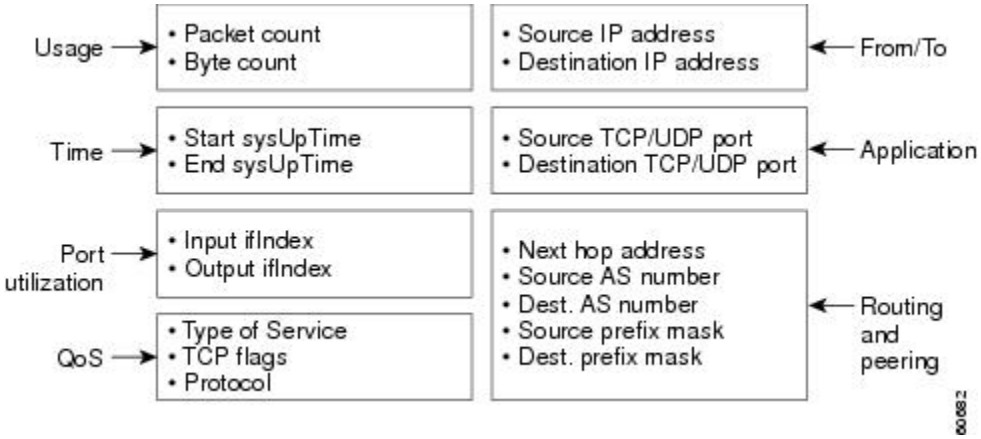
Table 6: NetFlow Flow Record Format Fields for Format Versions 5, and 9

Field	Version 5	Version 9
Source IP address	Yes	Yes
Destination IP address	Yes	Yes
Source TCP/UDP application port	Yes	Yes
Destination TCP/UDP application port	Yes	Yes
Next hop router IP address	Yes	Yes
Input physical interface index	Yes	Yes
Output physical interface index	Yes	Yes
Packet count for this flow	Yes	Yes
Byte count for this flow	Yes	Yes
Start of flow timestamp	Yes	Yes
End of flow timestamp	Yes	Yes
IP Protocol (for example, TCP=6; UDP=17)	Yes	Yes
Type of Service (ToS) byte	Yes	Yes
TCP Flags (cumulative OR of TCP flags)	Yes	Yes
Source AS number	Yes	Yes
Destination AS number	Yes	Yes
Source subnet mask	Yes	Yes
Destination subnet mask	Yes	Yes
Flags (indicates, among other things, which flows are invalid)	Yes	Yes
Other flow fields[1]	No	Yes

1 For a list of other flow fields available in Version 9 export format, see Figure 5 .

The figure below is an example of the NetFlow Version 5 export record format, including the contents and description of byte locations. The terms in **bold** indicate values that were added for the Version 5 format.

Figure 4: NetFlow Version 5 Export Record Format



The table below shows the field names and descriptions for the NetFlow Version 5 export record format.

Table 7: NetFlow Version 5 Export Record Format Field Names and Descriptions

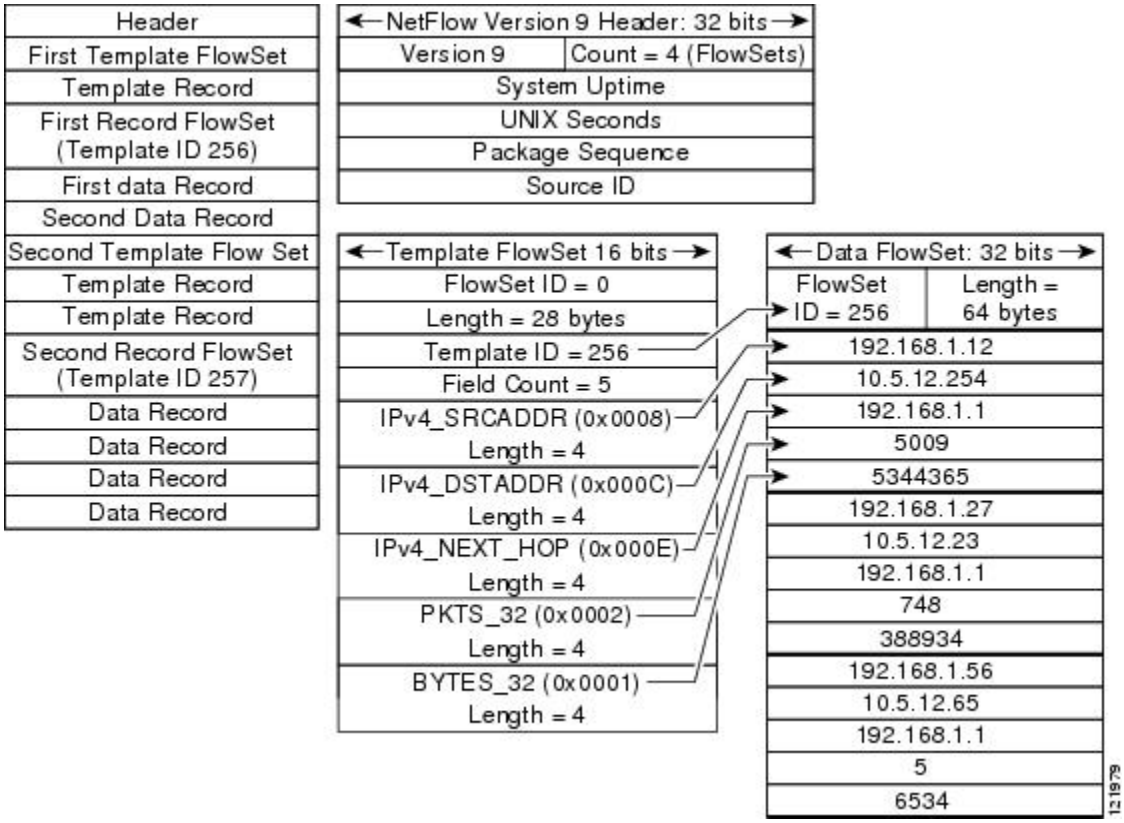
Content	Bytes	Descriptions
srcaddr	0-3	Source IP address
dstaddr	4-7	Destination IP address
nexthop	8-11	Next hop router's IP address
input	12-13	Ingress interface Simple Network Management Protocol (SNMP) ifIndex
output	14-15	Egress interface SNMP ifIndex
dPkts	16-19	Packets in the flow
dOctets	20-23	Octets (bytes) in the flow
first	24-27	SysUptime at start of the flow
last	28-31	SysUptime at the time the last packet of the flow was received
srcport	32-33	Layer 4 source port number or equivalent
dstport	34-35	Layer 4 destination port number or equivalent

Content	Bytes	Descriptions
pad1	36	Unused (zero) byte
tcp_flags	37	Cumulative OR of TCP flags
prot	38	Layer 4 protocol (for example, 6=TCP, 17=UDP)
tos	39	IP type-of-service byte
src_as	40-41	Autonomous system number of the source, either origin or peer
dst_as	42-43	Autonomous system number of the destination, either origin or peer
src_mask	44	Source address prefix mask bits
dst_mask	45	Destination address prefix mask bits
pad2	46-47	PAD2 is unused (zero) bytes

The figure below shows a typical flow record for the Version 9 export format. The NetFlow Version 9 export record format is different from the traditional NetFlow fixed format export record. In NetFlow Version 9, a template describes the NetFlow data and the flow set contains the actual data. This allows for flexible export.

Detailed information about the fields in Version 9 and export format architecture is available in the NetFlow Version 9 Flow-Record Format document.

Figure 5: NetFlow Version 9 Export Packet Example



For all export versions, you can specify a destination where NetFlow data export packets are sent, such as the workstation running NetFlow Collection Engine, when the number of recently expired flows reaches a predetermined maximum, or every second--whichever occurs first. For a Version 1 datagram, up to 24 flows can be sent in a single UDP datagram of approximately 1200 bytes; for a Version 5 datagram, up to 30 flows can be sent in a single UDP datagram of approximately 1500 bytes.

For detailed information on the flow record formats, data types, and export data fields for Versions 1, 7, and 9 and platform-specific information when applicable, see Appendix 2 in the NetFlow Services Solutions Guide .

NetFlow Data Export Format Selection

NetFlow exports data in UDP datagrams in export format Version 9, 8, 5, or 1. The table below describes situations when you might select a particular NetFlow export format.

Table 8: When to Select a Particular NetFlow Export Format

Export Format	Select When...
Version 9	You need to export data from various technologies, such as Multicast, DoS, IPv6, and BGP next hop. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, and BGP next hop. The Version 9 export format supports export from the main cache and from aggregation caches.
Version 8	You need to export data from aggregation caches. The Version 8 export format is available only for export from aggregation caches.
Version 5	You need to export data from the NetFlow main cache, and you are not planning to support new features. Version 5 export format does not support export from aggregation caches.
Version 1	You need to export data to a legacy collection system that requires Version 1 export format. Otherwise, do not use Version 1 export format. Use Version 9 or Version 5 export format.

NetFlow Version 9 Data Export Format

The NetFlow Version 9 Export Format feature was introduced in Cisco IOS Release 12.0(24)S and was integrated into Cisco IOS Release 12.3(1) and Cisco IOS Release 12.2(18)S.

NetFlow Version 9 data export supports Cisco Express Forwarding switching, distributed Cisco Express Forwarding switching, and fast switching.

NetFlow Version 9 is a flexible and extensible means for transferring NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

Using Version 9 export, you can define new formats on the router and send these formats to the NetFlow Collection Engine (formerly called NetFlow FlowCollector) at set intervals. You can enable the features that you want, and the field values corresponding to those features are sent to the NetFlow Collection Engine.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow need not recompile their applications each time a new NetFlow technology is added. Instead, with the NetFlow Version 9 Export Format feature, they can use an external data file that documents the known template formats and field types.

In NetFlow Version 9

- Record formats are defined by templates.

- Template descriptions are communicated from the router to the NetFlow Collection Engine.
- Flow records are sent from the router to the NetFlow Collection Engine with minimal template information so that the NetFlow Collection Engine can relate the records to the appropriate template.
- Version 9 is independent of the underlying transport protocol (UDP, TCP, SCTP, and so on).

NetFlow Version 9 Template-Based Flow Record Format

The main feature of NetFlow Version 9 export format is that it is template based. A template describes a NetFlow record format and attributes of fields (such as type and length) within the record. The router assigns each template an ID, which is communicated to the NetFlow Collection Engine along with the template description. The template ID is used for all further communication from the router to the NetFlow Collection Engine.

NetFlow Version 9 Export Flow Records

The basic output of NetFlow is a flow record. In NetFlow Version 9 export format, a flow record follows the same sequence of fields as found in the template definition. The template to which NetFlow flow records belong is determined by the prefixing of the template ID to the group of NetFlow flow records that belong to a template. For a complete discussion of existing NetFlow flow-record formats, see the NetFlow Services Solutions Guide.

NetFlow Version 9 Export Packet

In NetFlow Version 9, an export packet consists of the packet header and flowsets. The packet header identifies the NetFlow Version 9 Data Export Format, on page 42f"> Figure 3 for Version 9 export packet header details. Flowsets are of two types: template flowsets and data flowsets. The template flowset describes the fields that will be in the data flowsets (or flow records). Each data flowset contains the values or statistics of one or more flows with the same template ID. When the NetFlow Collection Engine receives a template flowset, it stores the flowset and export source address so that subsequent data flowsets that match the flowset ID and source combination are parsed according to the field definitions in the template flowset. Version 9 supports NetFlow Collection Engine Version 4.0. For an example of a Version 9 export packet, see NetFlow Version 9 Data Export Format, on page 42.

NetFlow Export Templates

NetFlow implements a variety of templates, each exporting a different set of fields for a specific purpose. For example, the MPLS templates are different from the Optimized Edge Routing (OER) templates and the various option templates.

The table below lists the export templates and the specific set of fields the export pertains to.

Table 9: NetFlow Export Templates

Number of Export Templates	Exports Fields Pertaining to...
1	IPv4 main cache
8	MPLS labels 0 to 3
21	Aggregation caches with or without BGP subflows
3	BGP, BGP Next Hop (NH), and Multicast

Number of Export Templates	Exports Fields Pertaining to...
4	OER
2	MAC and auxiliary information
11	Random sampler information, interface names, sampling option, and exporter status options

NetFlow Version 8 Data Export Format

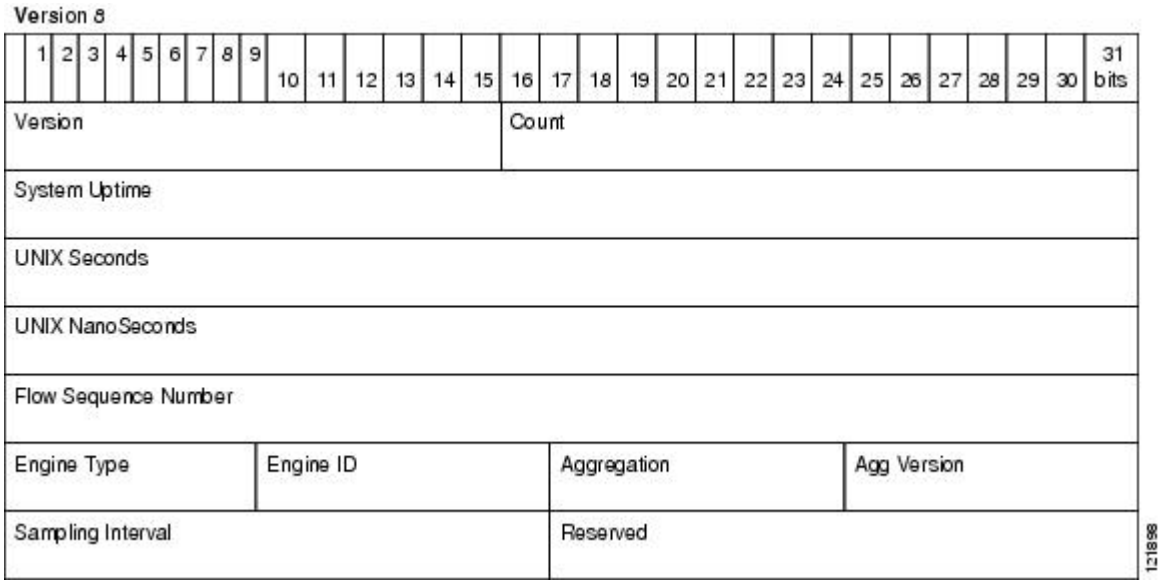
The Version 8 data export format is the NetFlow export format used when the router-based NetFlow Aggregation feature is enabled on Cisco IOS router platforms. The Version 8 format allows for export datagrams to contain a subset of the Version 5 export data that is based on the configured aggregation cache scheme. For example, a certain subset of the Version 5 export data is exported for the destination prefix aggregation scheme, and a different subset is exported for the source-prefix aggregation scheme.

The Version 8 export format was introduced in Cisco IOS Release 12.0(3)T for the Cisco IOS NetFlow Aggregation feature. An additional six aggregation schemes that also use Version 8 format were defined for the NetFlow ToS-Based Router Aggregation feature introduced in Cisco IOS 12.0(15)S and integrated into Cisco IOS Releases 12.2(4)T and 12.2(14)S. Refer to the "Configuring NetFlow Aggregation Caches" module for information on configuring Version 8 data export for aggregation caches.

The Version 8 datagram consists of a header with the version number (which is 8) and time-stamp information, followed by one or more records corresponding to individual entries in the NetFlow cache.

The figure below displays the NetFlow Version 8 export packet header format.

Figure 6: NetFlow Version 8 Export Packet Header Format



The table below lists the NetFlow Version 8 export packet header field names and definitions.

Table 10: NetFlow Version 8 Export Packet Header Field Names and Descriptions

Field Name	Description
Version	Flow export format version number. In this case 8.
Count	Number of export records in the datagram.
System Uptime	Number of milliseconds since the router last booted.
UNIX Seconds	Number of seconds since 0000 UTC 1970.
UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
Flow Sequence Number	Sequence counter of total flows sent for this export stream.
Engine Type	The type of switching engine. RP = 0 and LC = 1.
Engine ID	Slot number of the NetFlow engine.
Aggregation	Type of aggregation scheme being used.
Agg Version	Aggregation subformat version number. The current value is 2.
Sampling Interval	Interval value used if Sampled NetFlow is configured.
Reserved	Reserved.

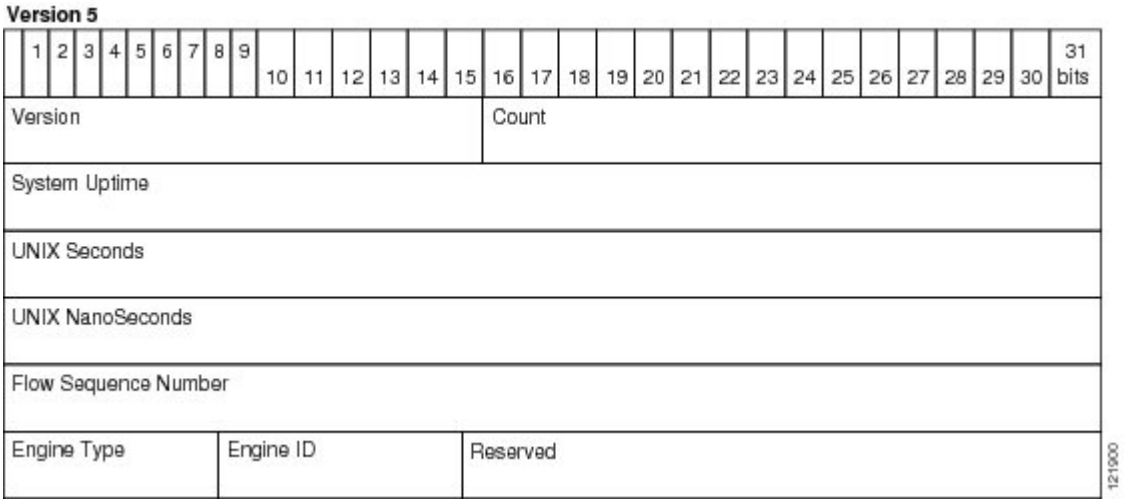
NetFlow Version 5 Data Export Format

The Version 5 data export format adds support for BGP autonomous system information and flow sequence numbers.

Because NetFlow uses UDP to send export datagrams, datagrams can be lost. The Version 5 header format contains a flow sequence number to find out whether flow export information has been lost. The sequence number is equal to the sequence number of the previous datagram plus the number of flows in the previous datagram. After receiving a new datagram, the receiving application can subtract the expected sequence number from the sequence number in the header to get the number of missed flows.

All fields in the Version 5 export format are in network byte order. The figure below shows the NetFlow Version 5 export packet header format.

Figure 7: NetFlow Version 5 Export Packet Header Format



The table below lists the NetFlow Version 5 export packet header field names and descriptions.

Table 11: NetFlow Version 5 Export Packet Header Field Names and Descriptions

Bytes	Field	Description
0 to 1	Version	Flow export format version number. In this case 5.
2 to 3	Count	Number of export records in the datagram.
4 to 7	System Uptime	Number of milliseconds since the router last booted.
8 to 11	UNIX Seconds	Number of seconds since 0000 UTC 1970.
12 to 15	UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.
16 to 19	Flow Sequence Number	Sequence counter of total flows sent for this export stream.
20	Engine Type	The type of switching engine. RP = 0 and LC = 1.
21	Engine ID	Slot number of the NetFlow engine.

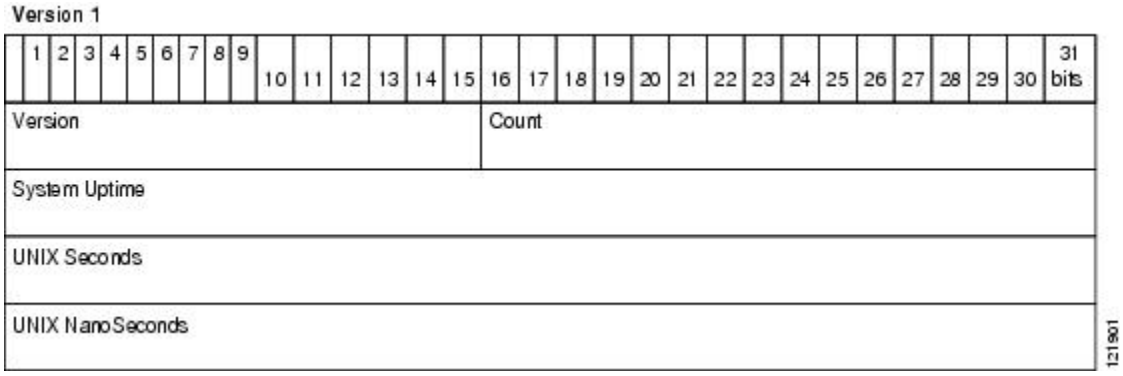
Bytes	Field	Description
22 to 23	Reserved	Reserved.

NetFlow Version 1 Data Export Format

The NetFlow Version 1 data export format was the format supported in the initial Cisco IOS software releases containing the NetFlow functionality. It is rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format.

The figure below shows the NetFlow Version 1 export packet header format.

Figure 8: Version 1 Export Packet Header Format



The table below lists the NetFlow Version 1 export packet header field names and descriptions.

Table 12: NetFlow Version 1 Packet Header Field Names and Descriptions

Field Name	Description
Version	Flow export format version number. In this case 1.
Count	Number of export records in the datagram.
System Uptime	Number of milliseconds since the router last booted.
UNIX Seconds	Number of seconds since 0000 UTC 1970.
UNIX NanoSeconds	Number of residual nanoseconds since 0000 UTC 1970.

Egress NetFlow Accounting Benefits NetFlow Accounting Simplified

The Egress NetFlow Accounting feature can simplify the NetFlow configuration. The following example shows how.

In the two figures below, both incoming and outgoing (ingress and egress) flow statistics are required for the server. The server is attached to Router B. The "cloud" in the figure represents the core of the network and includes MPLS VPNs.

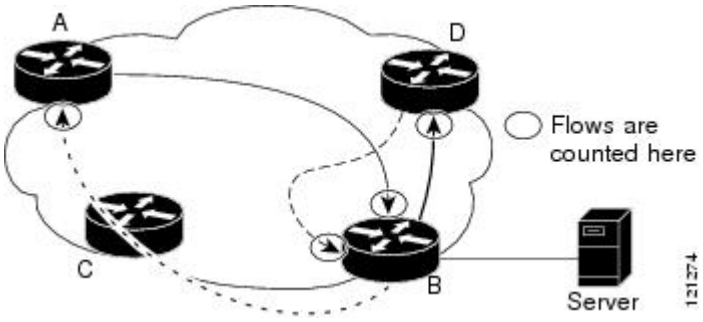
All traffic denoted by the arrows must be accounted for. The solid arrows represent IP traffic and the dotted arrows represent MPLS VPNs.

The first figure below shows how the flow traffic was tracked before the introduction of the Egress NetFlow Accounting feature. The second figure below shows how the flow traffic is tracked after the introduction of the Egress NetFlow Accounting feature. The Egress NetFlow Accounting feature simplifies configuration tasks and facilitates collection and tracking of incoming and outgoing flow statistics for the server in this example.

Because only ingress flows could be tracked before the Egress NetFlow Accounting feature was introduced, the following NetFlow configurations had to be implemented for the tracking of ingress and egress flows from Router B:

- Enable NetFlow on an interface on Router B to track ingress IP traffic from Router A to Router B.
- Enable NetFlow on an interface on Router D to track ingress IP traffic from Router B to Router D.
- Enable NetFlow on an interface on Router A to track ingress traffic from the MPLS VPN from Router B to Router A.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router D to Router B.

Figure 9: Ingress-Only NetFlow Example



A configuration such as the one used in the figure above requires that NetFlow statistics from three separate routers be added to obtain the flow statistics for the server.

In comparison, the example in the figure below shows NetFlow, the Egress NetFlow Accounting feature, and the MPLS Egress NetFlow Accounting feature being used to capture ingress and egress flow statistics for Router B, thus obtaining the required flow statistics for the server.

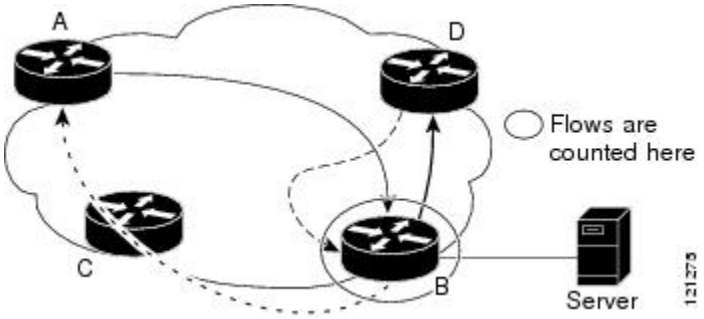
In the figure below, the following NetFlow configurations are applied to Router B:

- Enable NetFlow on an interface on Router B to track ingress IP traffic from Router A to Router B.

- Enable the Egress NetFlow Accounting feature on an interface on Router B to track egress IP traffic from Router B to Router D.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router B to Router D.
- Enable NetFlow on an interface on Router B to track ingress traffic from the MPLS VPN from Router B to Router A.

After NetFlow is configured on Router B, you can display all NetFlow statistics for the server by using the **show ip cache flow** command or the **show ip cache verbose flow** command for Router B.

Figure 10: Egress NetFlow Accounting Example



NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection

You can configure NetFlow on a per-subinterface basis. If your network contains thousands of subinterfaces, you can collect export records from just a few of them. The result is lower bandwidth requirements for NetFlow data export and reduced platform requirements for NetFlow data-collection devices.

The configuration of NetFlow on selected subinterfaces provides the following benefits:

- Reduced bandwidth requirement between routing devices and NetFlow management workstations.
- Reduced NetFlow workstation requirements; the number of flows sent to the workstation for processing is reduced.

NetFlow Multiple Export Destinations Benefits

The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations for the NetFlow data. With this feature enabled, two identical streams of NetFlow data are sent to the destination host. Currently, the maximum number of export destinations allowed is two.

The NetFlow Multiple Export Destinations feature improves the chances of receiving complete NetFlow data because it provides redundant streams of data. Because the same export data is sent to more than one NetFlow collector, fewer packets are lost.

NetFlow on a Distributed VIP Interface

On a Cisco 7500 series router with a Route Switch Processor (RSP) and with VIP controllers, the VIP hardware can be configured to switch packets received by the VIP interfaces with no per-packet intervention on the part of the RSP. This process is called distributed switching. When VIP distributed switching is enabled, the input VIP interface switches IP packets instead of forwarding them to the RSP for switching. Distributed switching decreases the demand on the RSP. VIP interfaces with distributed switching enabled can be configured for NetFlow.

How to Configure NetFlow and NetFlow Data Export

This section contains instructions for configuring NetFlow to capture and export network traffic data. Perform the following tasks to configure NetFlow to capture and export network traffic data:

Configuring NetFlow

Perform the following task to enable NetFlow on an interface.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces.
7. **end**

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.

	Command or Action	Purpose
Step 3	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 4	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress` **Example:**	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and enters global configuration mode. **Note** You need to use this command only if you want to enable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 to enable NetFlow on other interfaces.	This step is optional.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying that NetFlow Is Operational and Displaying NetFlow Statistics

Perform the following task to verify that NetFlow is operational and to display NetFlow statistics.

SUMMARY STEPS

1. **show ip flow interface**
2. **show ip cache flow**
3. **show ip cache verbose flow**

DETAILED STEPS

Step 1 **show ip flow interface**

Use this command to display the NetFlow configuration for an interface. The following is sample output from this command:

Example:

```
Router# show ip flow interface

Ethernet0/0
  ip flow ingress
Router#
```

Step 2 **show ip cache flow**

Use this command to verify that NetFlow is operational and to display a summary of NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache flow
IP packet size distribution (1103746 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2921778 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.8    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.1    1799.6       0.9
ICMP               135      0.0      1133   427      3.1    1799.6       0.8
Total:             945      0.0      1166    91     22.4    1799.6       0.8
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et0/0         192.168.67.6    Et1/0.1       172.16.10.200   01 0000 0C01    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0043 0043    51
Et0/0         10.10.18.1      Null          172.16.11.5     11 0045 0045    51
Et0/0         10.234.53.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 0044 0044    51
Et0/0         10.10.19.1      Null          172.16.11.6     11 00A2 00A2    51
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0014 0014    50
Et0/0         192.168.87.200  Et1/0.1       172.16.10.2     06 0015 0015    52
.
.
.
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0087 0087    50
Et0/0         172.16.1.84     Et1/0.1       172.16.10.19    06 0050 0050    51
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0089 0089    49
Et0/0         172.16.1.85     Et1/0.1       172.16.10.20    06 0050 0050    50
Et0/0         10.251.10.1     Et1/0.1       172.16.10.2     01 0000 0800    51
Et0/0         10.162.37.71    Null          172.16.11.3     06 027C 027C    49
Router#
```

Step 3 **show ip cache verbose flow**

Use this command to verify that NetFlow is operational and to display a detailed summary of NetFlow statistics. The following is sample output from this command:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (1130681 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .249 .694 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .027 .000 .027 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  35 active, 4061 inactive, 980 added
  2992518 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP            108      0.0      1133    40      2.4    1799.6       0.9
TCP-FTPD           108      0.0      1133    40      2.4    1799.6       0.9
TCP-WWW             54      0.0      1133    40      1.2    1799.6       0.8
TCP-SMTP            54      0.0      1133    40      1.2    1799.6       0.8
TCP-BGP             27      0.0      1133    40      0.6    1799.6       0.7
TCP-NNTP            27      0.0      1133    40      0.6    1799.6       0.7
TCP-other          297      0.0      1133    40      6.6    1799.7       0.8
UDP-TFTP            27      0.0      1133    28      0.6    1799.6       1.0
UDP-other          108      0.0      1417    28      3.0    1799.6       0.9
ICMP               135      0.0      1133   427      3.0    1799.6       0.8
Total:             945      0.0      1166    91     21.9    1799.6       0.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0          192.168.67.6    Et1/0.1        172.16.10.200   01 00  10     799
0000 /0  0                     0C01 /0  0     0.0.0.0                28  1258.1
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0043 /0  0                     0043 /0  0     0.0.0.0                28  1258.0
Et0/0          10.10.18.1      Null           172.16.11.5     11 00  10     799
0045 /0  0                     0045 /0  0     0.0.0.0                28  1258.0
Et0/0          10.234.53.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0                28  1258.1
Et0/0          10.10.19.1      Null           172.16.11.6     11 00  10     799
0044 /0  0                     0044 /0  0     0.0.0.0                28  1258.1
.
.
.
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0087 /0  0                     0087 /0  0     0.0.0.0                40  1258.1
Et0/0          172.16.1.84     Et1/0.1        172.16.10.19    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     798
0089 /0  0                     0089 /0  0     0.0.0.0                40  1256.5
Et0/0          172.16.1.85     Et1/0.1        172.16.10.20    06 00  00     799
0050 /0  0                     0050 /0  0     0.0.0.0                40  1258.0
Et0/0          10.251.10.1     Et1/0.1        172.16.10.2     01 00  10     799
0000 /0  0                     0800 /0  0     0.0.0.0              1500  1258.1
Et0/0          10.162.37.71    Null           172.16.11.3     06 00  00     798
027C /0  0                     027C /0  0     0.0.0.0                40  1256.4
Router#
```

Configuring NetFlow Data Export Using the Version 9 Export Format

Perform the steps in this optional task to configure NetFlow Data Export using the Version 9 export format.

Note This task does not include instructions for configuring Reliable NetFlow Data Export using the Stream Control Transmission Protocol (SCTP). Refer to the NetFlow Reliable Export with SCTP module for information about and instructions for configuring Reliable NetFlow Data Export using SCTP.

Before You Begin

This task does not include the steps for configuring NetFlow. You must configure NetFlow by enabling it on at least one interface in the router in order to export traffic data with NetFlow Data Export. Refer to the Configuring NetFlow, on page 50 for information about configuring NetFlow.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*
4. Repeat Step 3 once to configure an additional NetFlow export destination.
5. **ip flow-export source** *interface-type interface-number*
6. **ip flow-export version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**]
7. **ip flow-export interface-names**
8. **ip flow-export template refresh-rate** *packets*
9. **ip flow-export template timeout-rate** *minutes*
10. **i p flow-export template options export-stats**
11. **ip flow-export template options refresh-rate** *packets*
12. **ip flow-export template options timeout-rate** *minutes*
13. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port* **Example:** `Router(config)# ip flow-export destination 172.16.10.2 99`	Specifies the IP address, or hostname of the NetFlow collector, and the UDP port the NetFlow collector is listening on.
Step 4	Repeat Step 3 once to configure an additional NetFlow export destination.	(Optional) You can configure a maximum of two export destinations for NetFlow.
Step 5	**ip flow-export source** *interface-type interface-number* **Example:** `Router(config)# ip flow-export source ethernet 0/0`	(Optional) Specifies the IP address from the interface. The IP address is used as the source IP address for the UDP datagrams that are sent by NetFlow data export to the destination host.
Step 6	**ip flow-export version 9** [**origin-as** | **peer-as**] [**bgp-nexthop**] **Example:** `Router(config)# ip flow-export version 9`	(Optional) Enables the export of information in NetFlow cache entries. • The **version 9** keyword specifies that the export packet uses the Version 9 format. • The **origin-as** keyword specifies that export statistics include the originating autonomous system for the source and destination. • The **peer-as** keyword specifies that export statistics include the peer autonomous system for the source and destination. • The **bgp-nexthop** keyword specifies that export statistics include BGP next hop-related information. **Caution** Entering this command on a Cisco 12000 series Internet router causes packet forwarding to stop for a few seconds while NetFlow reloads the RP and LC Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 7	**ip flow-export interface-names** **Example:** `Router(config)# ip flow-export interface-names`	Configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system. **Caution** If you are using traditional NetFlow, you can import only up to 1200 interface names. The device might crash if more than 1200 interface names are exported. To export more than 1200 interface names, use Flexible NetFlow.
Step 8	**ip flow-export template refresh-rate** *packets*	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations.

	Command or Action	Purpose
	Example: `Router(config)# ip flow-export template refresh-rate 15` **Example:**	• The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are re-sent. You can specify from 1 to 600 packets. The default is 20.
Step 9	**ip flow-export template timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template timeout-rate 90`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies that the **timeout-rate** keyword applies to the template. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are re-sent. You can specify from 1 to 3600 minutes. The default is 30.
Step 10	**i p flow-export template options export-stats** **Example:** `Router(config)# ip flow-export template options export-stats`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **export-stats**keyword specifies that the export statistics include the total number of flows exported and the total number of packets exported.
Step 11	**ip flow-export template options refresh-rate** *packets* **Example:** `Router(config)# ip flow-export template options refresh-rate 25`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **refresh-rate** *packets*keyword-argument pair specifies the number of packets exported before the templates are re-sent. You can specify from 1 to 600 packets. The default is 20.
Step 12	**ip flow-export template options timeout-rate** *minutes* **Example:** `Router(config)# ip flow-export template options timeout-rate 120`	(Optional) Enables the export of information in NetFlow cache entries. • The **template** keyword specifies template-specific configurations. • The **options** keyword specifies template options. • The **timeout-rate** *minutes*keyword-argument pair specifies the time elapsed before the templates are re-sent. You can specify from 1 to 3600 minutes. The default is 30.
Step 13	**end** **Example:** `Router(config)# end`	Exits the current configuration mode and enters privileged EXEC mode.

Verifying that NetFlow Data Export Is Operational

Perform the steps in this optional task to verify that NetFlow data export is operational and to display the statistics for NetFlow data export.

SUMMARY STEPS

1. **show ip flow export**
2. **show ip flow export template**

DETAILED STEPS

Step 1 **show ip flow export**

Use this command to display statistics for the NetFlow data export, including statistics for the main cache and for all other enabled caches. The following is sample output from this command:

Example:

```
Router# show ip flow export
Flow export v9 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source interface Ethernet0/0
  Version 9 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Step 2 **show ip flow export template**

Use this command to display statistics for the NetFlow data export (such as the template timeout rate and the refresh rate) for template-specific configurations. The following is sample output from this command:

Example:

```
Router# show ip flow export template
   Template Options Flag = 1
   Total number of Templates added = 1
   Total active Templates = 1
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 1
   Option  Templates added = 1
   Template ager polls = 0
   Option Template ager polls = 140
Main cache version 9 export is enabled
 Template export information
   Template timeout = 90
   Template refresh rate = 15
 Option export information
```

```
   Option timeout = 120
   Option refresh rate = 25
Router#
```

Clearing NetFlow Statistics on the Router

Perform the steps in this optional task to clear NetFlow statistics on the router.

SUMMARY STEPS

1. **enable**
2. **clear ip flow stats**

DETAILED STEPS

Step 1 **enable**

Use this command to enter privileged EXEC mode on the router:

Example:

```
Router> enable
Router#
```

Step 2 **clear ip flow stats**

Use this command to clear the NetFlow statistics on the router. For example:

Example:

```
Router# clear ip flow stats
```

Customizing the NetFlow Main Cache Parameters

NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. A flow record is maintained within the NetFlow cache for all active flows. Each flow record in the NetFlow cache contains fields that can later be exported to a collection device, such as the NetFlow Collection Engine. NetFlow enables the accumulation of data on flows. Each flow is identified by unique characteristics such as the IP address, interface, application, and ToS.

To customize the parameters for the main NetFlow cache, perform the steps in this optional task.

NetFlow Cache Entry Management on a Routing Device

The routing device checks the NetFlow cache once per second and causes the flow to expire in the following instances:

- Flow transport is completed (TCP connections that have reached the end of the byte stream [FIN] or that have been reset [RST] are expired).
- The flow cache has become full.
- A flow becomes inactive. By default, a flow that is unaltered in the last 15 seconds is classified as inactive.
- An active flow has been monitored for a specified number of minutes. By default, active flows are flushed from the cache when they have been monitored for 30 minutes.

Routing device default timer settings are 15 seconds for the inactive timer and 30 minutes for the active timer. You can configure your own time interval for the inactive timer from 10 to 600 seconds. You can configure the time interval for the active timer from 1 to 60 minutes.

NetFlow Cache Size

After you enable NetFlow on an interface, NetFlow reserves memory to accommodate a number of entries in the NetFlow cache. Normally, the size of the NetFlow cache meets the needs of your NetFlow traffic rates. The cache default size is 64K flow cache entries. Each cache entry requires 64 bytes of storage. About 4 MB of DRAM are required for a cache with the default number of entries. You can increase or decrease the number of entries maintained in the cache, if required. For environments with a large amount of flow traffic (such as an Internet core router), Cisco recommends a larger value such as 131072 (128K). To obtain information on your flow traffic, use the **show ip cache flow command.**

A NetFlow cache can be resized depending on the platform and the amount of DRAM on a line card. For example, the NetFlow cache size is configurable for software-based platforms such as Cisco 75xx and 72xx series routers. The amount of memory on a Cisco 12000 line card determines how many flows are possible in the cache.

Using the **ip flow-cache entries** command, configure the size of your NetFlow cache from 1024 entries to 524,288 entries. Use the **cache entries** command (after you configure NetFlow aggregation) to configure the size of the NetFlow aggregation cache from 1024 entries to 524,288 entries.

Caution Cisco recommends that you not change the values for NetFlow cache entries. Improper use of this feature could cause network problems. To return to the default value for NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Note If you modify any parameters for the NetFlow main cache after you enable NetFlow, the changes will not take effect until you reboot the router or disable NetFlow on every interface it is enabled on, and then re-enable NetFlow on the interfaces.

>

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **no ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 for every interface that has NetFlow enabled on it.
7. **ip flow-cache entries** *number*
8. **ip flow-cache timeout active** *minutes*
9. **ip flow-cache timeout inactive** *seconds*
10. **interface** *type number*
11. **ip flow** {**ingress** | **egress**}
12. **exit**
13. Repeat Steps 10 through 12 for every interface that previously had NetFlow enabled on it.
14. **end**

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`	(Required if NetFlow is already enabled on the interface) Specifies the interface that you want to disable NetFlow on and enters interface configuration mode.
Step 4	**no ip flow** {**ingress**	**egress**} **Example:** `Router(config-if)# no ip flow ingress` **Example:**	(Required if NetFlow is enabled on the interface) Disables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface

	Command or Action	Purpose
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you need to disable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 for every interface that has NetFlow enabled on it.	This step is required if NetFlow is enabled on any other interfaces. --
Step 7	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 131072`	(Optional) Changes the number of entries maintained in the NetFlow cache. • The *number* argument is the number of entries to be maintained. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).
Step 8	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 20`	(Optional) Specifies flow cache timeout parameters. • The **active** keyword specifies the active flow timeout. • The *minutes* argument specifies the number of minutes that an active flow remains in the cache before the flow times out. The range is from 1 to 60. The default is 30.
Step 9	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 130`	(Optional) Specifies flow cache timeout parameters. • The **inactive** keyword specifies the inactive flow timeout. • The *seconds* argument specifies the number of seconds that an inactive flow remains in the cache before it times out. The range is from 10 to 600. The default is 15.
Step 10	**interface** *type number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 11	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress` **Example:**	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface

	Command or Action	Purpose
Step 12	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You need to use this command only if you need to enable NetFlow on another interface.
Step 13	Repeat Steps 10 through 12 for every interface that previously had NetFlow enabled on it.	This step is required for any other interfaces that you need to enable NetFlow on.
Step 14	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and enters privileged EXEC mode.

Configuration Examples for Configuring NetFlow and NetFlow Data Export

Example Configuring Egress NetFlow Accounting

The following example shows how to configure Egress NetFlow Accounting as described in the Egress NetFlow Accounting Benefits NetFlow Accounting Simplified, on page 48:

```
configure terminal
!
interface ethernet 0/0
 ip flow egress
!
```

Example Configuring NetFlow Subinterface Support

The following examples show how to configure NetFlow Subinterface Support as described in the NetFlow Subinterface Support Benefits Fine-Tuning Your Data Collection, on page 49:

NetFlow Subinterface Support for Ingress (Received) Traffic on a Subinterface

```
configure terminal
!
interface ethernet 0/0.1
 ip flow ingress
!
```

NetFlow SubInterface Support for Egress (Transmitted) Traffic on a Subinterface

```
configure terminal
!
interface ethernet 1/0.1
 ip flow egress
!
```

Note NetFlow performs additional checks for the status of each subinterface that requires more CPU processing time and bandwidth. If you have several subinterfaces configured and you want to configure NetFlow data capture on all of them, we recommend that you configure NetFlow on the main interface instead of on the individual subinterfaces.

Example Configuring NetFlow Multiple Export Destinations

The following example shows how to configure the NetFlow Multiple Export Destinations feature as described in the NetFlow Multiple Export Destinations Benefits, on page 49:

```
configure terminal
!
ip flow-export destination 10.10.10.10 9991
ip flow-export destination 172.16.10.2 9991
!
```

Note You can configure a maximum of two export destinations for the main cache and for each aggregation cache.

Example Configuring NetFlow Version 5 Data Export

The following example shows how to configure the NetFlow data export using the Version 5 export format with the peer autonomous system information:

```
configure terminal

!

ip flow-export version 5 peer-as
ip flow-export destination 172.16.10.2 99
exit
Router# show ip flow export
Flow export v5 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source IP address 172.16.6.1
  Version 5 flow records, peer-as
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Example Configuring NetFlow Version 1 Data Export

The following example shows how to configure the NetFlow data export using the Version 5 export format with the peer autonomous system information:

```
configure terminal

!

ip flow-export destination 172.16.10.2 99
exit
Router# show ip flow export
Flow export v1 is enabled for main cache
  Exporting flows to 172.16.10.2 (99)
  Exporting using source IP address 172.16.6.1
  Version 1 flow records
  0 flows exported in 0 udp datagrams
  0 flows failed due to lack of export packet
  0 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Note No autonomous system number or BGP next hop information is exported with the Version 1 export format.

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NetFlow Commands	*Cisco IOS NetFlow Command Reference*
NetFlow Version 9 Flow-Record Format	NetFlow Version 9 Flow-Record Format
NetFlow Services Solutions Guide	*NetFlow Services Solutions Guide*
NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for Configuring NetFlow and NetFlow Data Export

Table 13: Feature Information for Configuring NetFlow and NetFlow Data Export

Feature Name	Releases	Feature Information
Egress NetFlow Accounting	12.3(11)T 15.0(1)S	The Egress NetFlow Accounting feature allows NetFlow statistics to be gathered on egress traffic that is exiting the router. Previous versions of NetFlow allow statistics to be gathered only on ingress traffic that is entering the router. The following commands were introduced by this feature: **ip flow egress** and **ip flow-egress input-interface**. The following commands were modified by this feature: **flow-sampler**, **match**, **show ip cache flow**, **show ip cache verbose flow**, and **show ip flow interface**.
NetFlow Multiple Export Destinations	12.0(19)S 12.2(2)T 12.2(14)S 15.0(1)S	The NetFlow Multiple Export Destinations feature enables configuration of multiple destinations of the NetFlow data. The following commands were modified by this feature: **ip flow-aggregation cache**, **ip flow-export destination**, and **show ip flow export**.
NetFlow Subinterface Support	12.0(22)S 12.2(14)S 12.2(15)T 12.2(33)SB	The NetFlow Subinterface Support feature provides the ability to enable NetFlow on a per-subinterface basis. The following command was introduced by this feature: **ip flow ingress.** The following command was modified by this feature: **show ip interface**.

Feature Name	Releases	Feature Information
NetFlow v9 Export Format	12.0(24)S 12.2(18)S 12.2(27)SBC 12.2(18)SXF 12.3(1) 15.0(1)S	The NetFlow v9 Export Format, which is flexible and extensible, provides the versatility needed to support new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, MPLS, NAT, and BGP next hop. The following commands were modified by this feature: **debug ip flow export**, **export**, **ip flow-export**, and **show ip flow export**.
Support for interface names added to NetFlow data export[2]	12.4(2)T	The **interface-names** keyword for the **ip flow-export** command configures NetFlow data export to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.

2 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

Glossary

Autonomous system--A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

Cisco Express Forwarding--A layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used by a router to reach a certain destination.

distributed Cisco Express Forwarding--A type of Cisco Express Forwarding switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the Forwarding Information Base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --Type of packet built by a NetFlow-services-enabled device (for example, a router) that is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes (parses, aggregates, and stores information on IP flows) the packet.

fast switching --A Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type of service, and with the same interface on which the flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

MPLS --Multiprotocol Label Switching. An industry standard for the forwarding of packets along a normally routed path (sometimes called MPLS hop-by-hop forwarding).

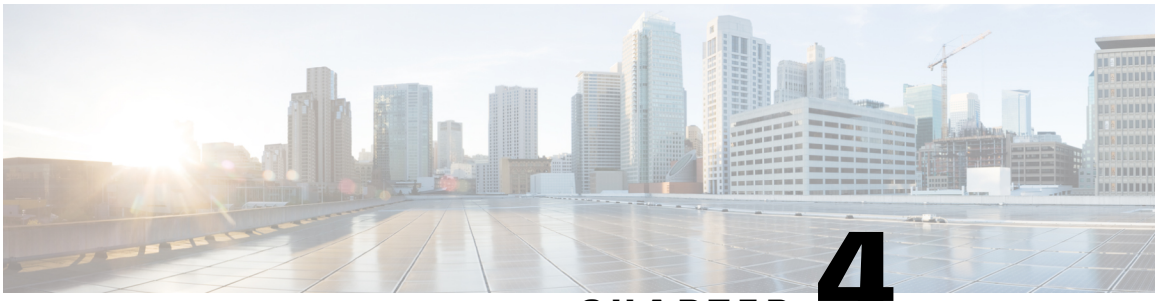
NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on a Cisco IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

RP --Route Processor. A processor module in the Cisco 7000 series routers that contains the CPU, system software, and most of the memory components that are used in the router. It is sometimes called a Supervisory Processor.



CHAPTER 4

Configuring NetFlow Aggregation Caches

This module contains information about and instructions for configuring NetFlow aggregation caches. The NetFlow main cache is the default cache used to store the data captured by NetFlow. By maintaining one or more extra caches, called aggregation caches, the NetFlow Aggregation feature allows limited aggregation of NetFlow data export streams on a router. The aggregation scheme that you select determines the specific kinds of data that are exported to a remote host.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

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 Configuring NetFlow Aggregation Caches

Before you enable NetFlow, you must:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources

If you intend to use Version 8 export format with an aggregation cache, configure Version 5 export format for the main cache.

If you need autonomous system (AS) information from the aggregation, make sure to specify either the **peer-as**or **origin-as** keyword in your export command if you have not configured an export format version.

You must explicitly enable each NetFlow aggregation cache by entering the **enabled** keyword from aggregation cache configuration mode.

Router-based aggregation must be enabled for minimum masking.

Restrictions for Configuring NetFlow Aggregation Caches

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface.

Memory Impact

During times of heavy traffic, the additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Performance Impact

Configuring Egress NetFlow accounting with the **ip flow egress** command might adversely affect network performance because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router.

NetFlow Data Export

Restrictions for NetFlow Version 9 Data Export

- Backward compatibility--Version 9 is not backward-compatible with Version 5 or Version 8. If you need Version 5 or Version 8, you must configure it.

- Export bandwidth--Export bandwidth use increases for Version 9 (because of template flowsets) versus Version 5. The increase in bandwidth usage versus Version 5 varies with the frequency with which template flowsets are sent. The default is to resend templates every 20 packets, which has a bandwidth cost of about 4 percent. If necessary, you can lower the resend rate with the **ip flow-export template refresh-rate** *packets* command.
- Performance impact--Version 9 slightly decreases overall performance, because generating and maintaining valid template flowsets require additional processing.

Restrictions for NetFlow Version 8 Export Format

Version 8 export format is available only for aggregation caches, and it cannot be expanded to support new features.

Information About Configuring NetFlow Aggregation Caches

NetFlow Aggregation Caches

NetFlow Cache Aggregation Benefits

Aggregation of export data is typically performed by NetFlow collection tools on management workstations. Router-based aggregation allows limited aggregation of NetFlow export records to occur on the router. Thus, you can summarize NetFlow export data on the router before the data is exported to a NetFlow data collection system, which has the following benefits:

- Reduces the bandwidth required between the router and the workstations
- Reduces the number of collection workstations required
- Improves performance and scalability on high flow-per-second routers

NetFlow Cache Aggregation Schemes

Cisco IOS NetFlow aggregation maintains one or more extra caches with different combinations of fields that determine which flows are grouped together. These extra caches are called aggregation caches. The combinations of fields that make up an aggregation cache are referred to as schemes. As flows expire from the main cache, they are added to each enabled aggregation cache.

You can configure each aggregation cache with its individual cache size, cache ager timeout parameter, export destination IP address, and export destination UDP port. As data flows expire in the main cache (depending on the aggregation scheme configured), relevant information is extracted from the expired flow and the corresponding flow entry in the aggregation cache is updated. The normal flow ager process runs on each active aggregation cache the same way it runs on the main cache. On-demand aging is also supported. Each aggregation cache contains different field combinations that determine which data flows are grouped. The default aggregation cache size is 4096 bytes.

You configure a cache aggregation scheme through the use of arguments to the **ip flow-aggregation cache** command. NetFlow supports the following five non-ToS based cache aggregation schemes:

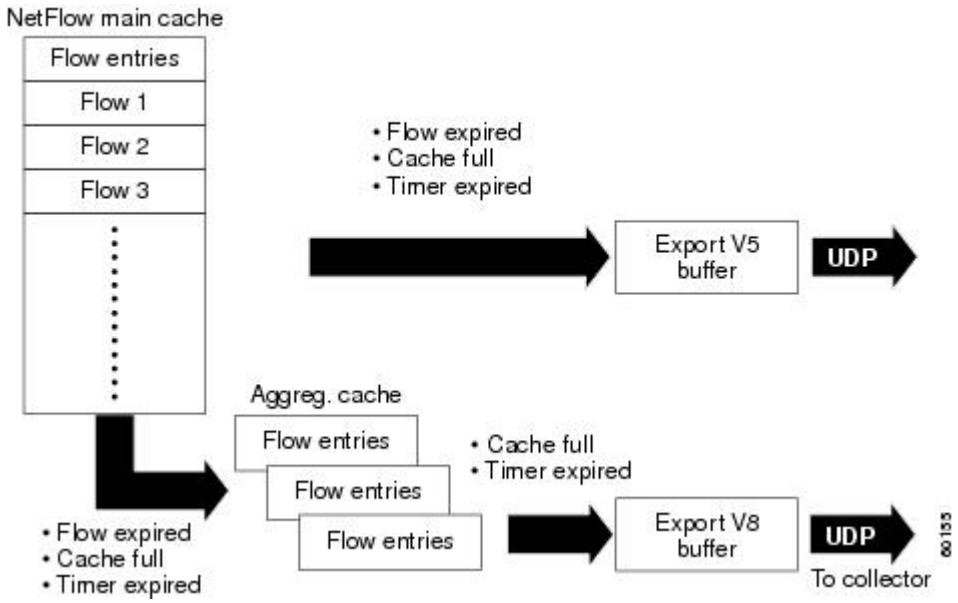
- Autonomous system (AS) aggregation scheme
- Destination prefix aggregation scheme
- Prefix aggregation scheme
- Protocol port aggregation scheme
- Source prefix aggregation scheme

The NetFlow Type of Service (ToS)-Based Router Aggregation feature introduced support for additional cache aggregation schemes, all of which include the ToS byte as one of the fields in the aggregation cache. The following are the six ToS-based aggregation schemes:

- AS-ToS aggregation scheme
- Destination prefix-ToS aggregation scheme
- Prefix-port aggregation scheme
- Prefix-ToS aggregation scheme
- Protocol-port-ToS aggregation scheme
- Source prefix-ToS aggregation scheme

The figure below shows an example of how the main NetFlow cache can be aggregated into multiple aggregation caches based upon user-configured aggregation schemes.

Figure 11: Building a NetFlow Aggregation Cache



Note NetFlow Aggregation Scheme Fields, on page 73 through NetFlow Cache Aggregation Schemes, on page 71 illustrate the Version 8 export formats of the aggregation schemes listed above. Additional export formats (for instance, Version 9) are also supported. If you are using Version 9, the formats will be different from those shown in the figures. For more information about Version 9 export formats, see Configuring NetFlow and NetFlow Data Export.

NetFlow Aggregation Scheme Fields

Each cache aggregation scheme contains field combinations that differ from any other cache aggregation scheme. The combination of fields determines which data flows are grouped and collected when a flow expires from the main cache. A flow is a set of packets that has common fields, such as the source IP address, destination IP address, protocol, source and destination ports, type-of-service, and the same interface on which the flow is monitored. To manage flow aggregation on your router, you need to configure the aggregation cache scheme that groups and collects the fields from which you want to examine data. The tables below show the NetFlow fields that are grouped and collected for non-ToS and ToS based cache aggregation schemes.

The table below shows the NetFlow fields used in the non-TOS based aggregation schemes.

Table 14: NetFlow Fields Used in the Non-ToS Based Aggregations Schemes

Field	AS	Protocol Port	Source Prefix	Destination Prefix	Prefix
Source prefix			X		X
Source prefix mask			X		X
Destination prefix				X	X
Destination prefix mask				X	X
Source app port		X			
Destination app port		X			
Input interface	X		X		X
Output interface	X			X	X
IP protocol		X			
Source AS	X		X		X
Destination AS	X			X	X

Field	AS	Protocol Port	Source Prefix	Destination Prefix	Prefix
First time stamp	X	X	X	X	X
Last time stamp	X	X	X	X	X
Number of flows	X	X	X	X	X
Number of packets	X	X	X	X	X
Number of bytes	X	X	X	X	X

The table below shows the NetFlow fields used in the TOS based aggregation schemes.

Table 15: NetFlow Fields Used in the ToS Based Aggregation Schemes

Field	AS-ToS	Protocol Port-ToS	Source Prefix-ToS	Destination Prefix-ToS	Prefix-ToS	Prefix-Port
Source prefix			X		X	X
Source prefix mask			X		X	X
Destination prefix				X	X	X
Destination prefix mask				X	X	X
Source app port		X				X
Destination app port		X				X
Input interface	X	X	X		X	X
Output interface	X	X		X	X	X
IP protocol		X				X
Source AS	X		X		X	

Field	AS-ToS	Protocol Port-ToS	Source Prefix-ToS	Destination Prefix-ToS	Prefix-ToS	Prefix-Port
Destination AS	X			X	X	
ToS	X	X	X	X	X	X
First time stamp	X	X	X	X		X
Last time stamp	X	X	X	X		X
Number of flows	X	X	X	X		X
Number of packets	X	X	X	X		X
Number of bytes	X	X	X	X		X

NetFlow AS Aggregation Scheme

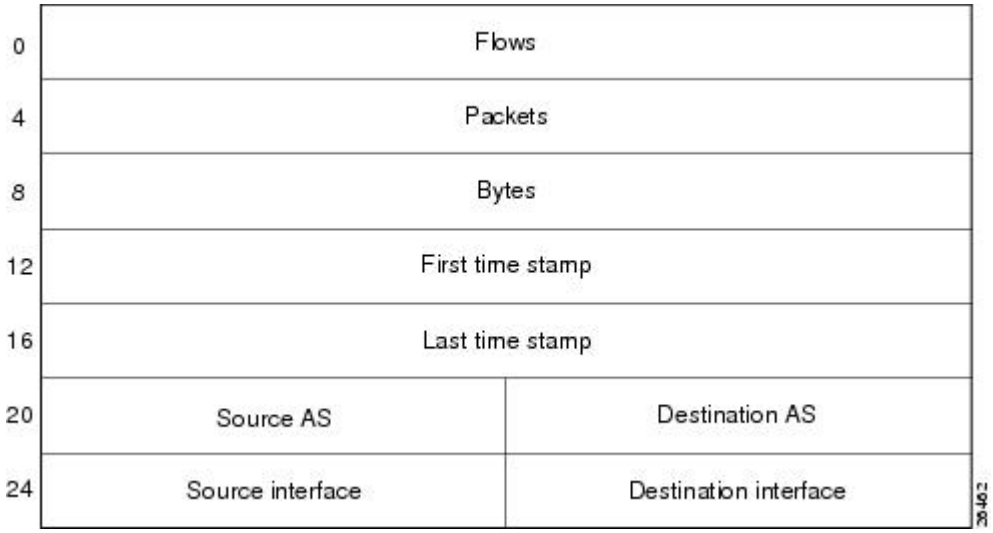
The NetFlow AS aggregation scheme reduces NetFlow export data volume substantially and generates AS-to-AS traffic flow data. The scheme groups data flows that have the same source BGP AS, destination BGP AS, input interface, and output interface.

The aggregated NetFlow data export records report the following:

- Source and destination BGP AS
- Number of packets summarized by the aggregated record
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Source interface
- Destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the AS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 12: Data Export Format for AS Aggregation Scheme



The table below lists definitions for the data export record fields used in the AS aggregation scheme.

Table 16: Data Export Record Field Definitions for AS Aggregation Scheme

Field	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

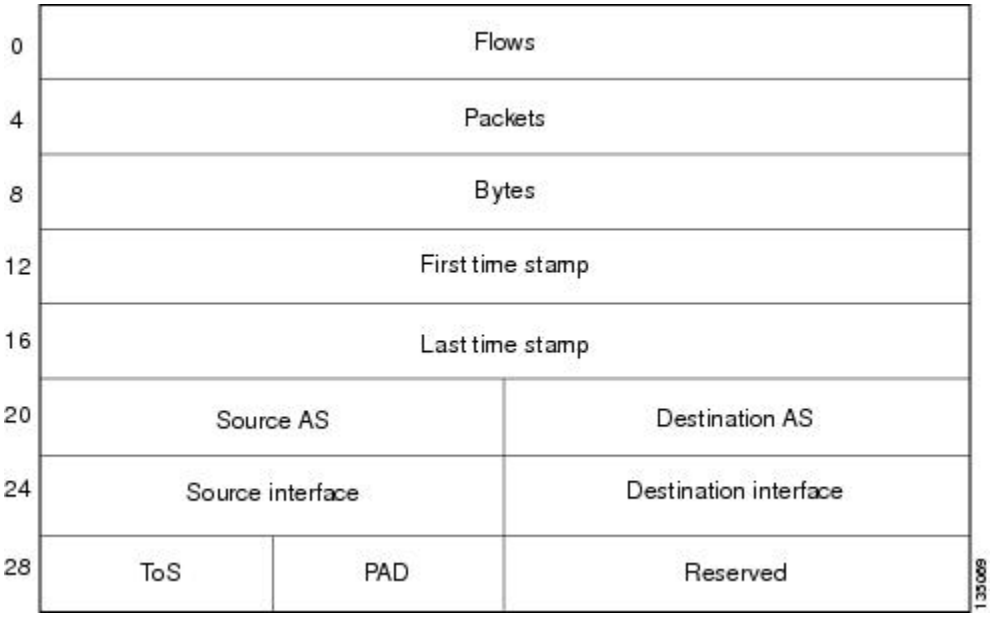
NetFlow AS-ToS Aggregation Scheme

The NetFlow AS-ToS aggregation scheme groups flows that have the same source BGP AS, destination BGP AS, source and destination interfaces, and ToS byte. The aggregated NetFlow export record based on the AS-ToS aggregation scheme reports the following:

- Source BGP AS
- Destination BGP AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by this aggregated record
- Number of packets summarized by this aggregation record
- Source and destination interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for generating AS-to-AS traffic flow data, and for reducing NetFlow export data volume substantially. The figure below shows the data export format for the AS-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 13: Data Export Format for AS-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the AS-ToS aggregation scheme.

Table 17: Data Export Record Term Definitions for AS-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface
ToS	Type of service byte
PAD	Zero field
Reserved	Zero field

NetFlow Destination Prefix Aggregation Scheme

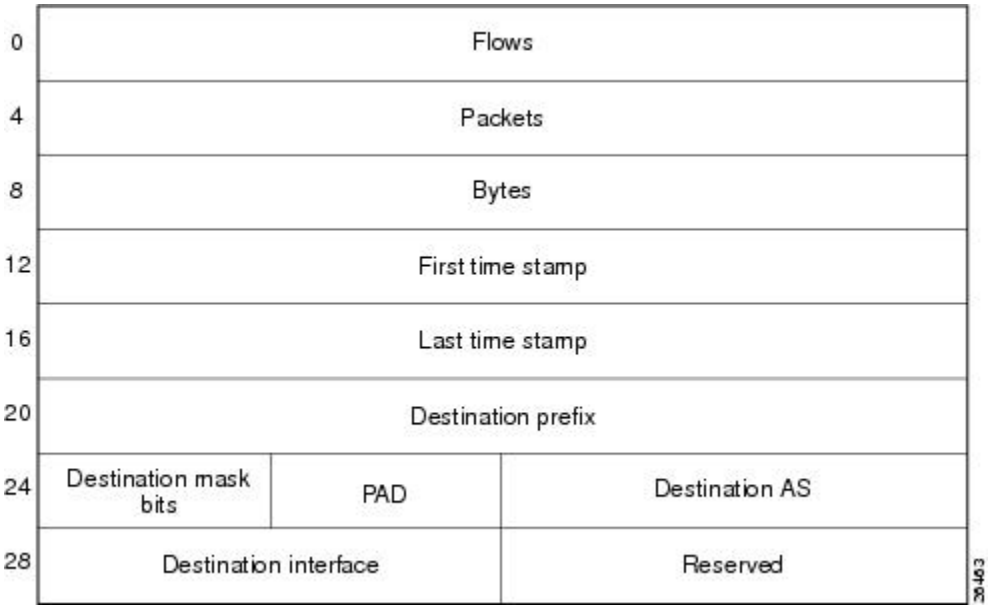
The destination prefix aggregation scheme generates data so that you can examine the destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same destination prefix, destination prefix mask, destination BGP AS, and output interface.

The aggregated NetFlow data export records report the following:

- Destination prefix
- Destination prefix mask
- Destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the destination prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 14: Destination Prefix Aggregation Data Export Record Format



The table below lists definitions for the data export record terms used in the destination prefix aggregation scheme.

Table 18: Data Export Record Term Definitions for Destination Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Destination prefix	Destination IP address ANDed with the destination prefix mask
Destination mask bits	Number of bits in the destination prefix
PAD	Zero field
Destination AS	Autonomous system of the destination IP address (peer or origin)

Term	Definition
Destination interface	SNMP index of the output interface
Reserved	Zero field

NetFlow Destination Prefix-ToS Aggregation Scheme

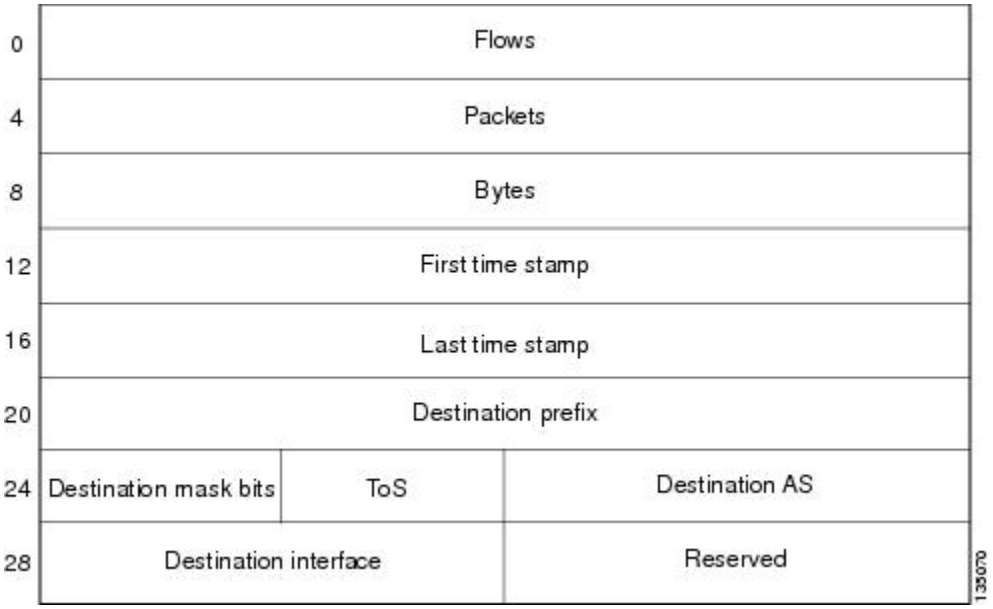
The NetFlow destination prefix-ToS aggregation scheme groups flows that have the same destination prefix, destination prefix mask, destination BGP AS, ToS byte, and output interface. The aggregated NetFlow export record reports the following:

- Destination IP address
- Destination prefix mask
- Destination AS
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Output interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the data export format

for the Destination prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 15: Data Export Format for Destination Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the destination prefix-ToS aggregation scheme.

Table 19: Data Export Record Term Definitions for Destination Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Destination prefix	Destination IP address ANDed with the destination prefix mask
Dest mask bits	Number of bits in the destination prefix
ToS	Type of service byte
Destination AS	Autonomous system of the destination IP address (peer or origin)

Term	Definition
Destination interface	SNMP index of the output interface
Reserved	Zero field

NetFlow Prefix Aggregation Scheme

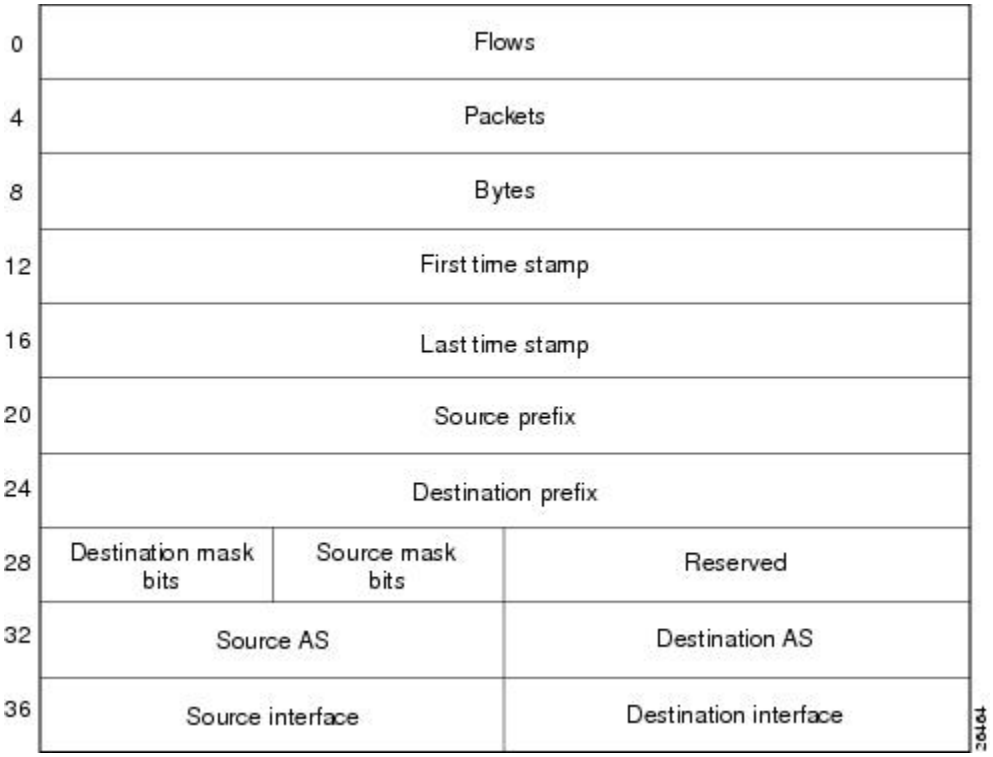
The NetFlow prefix aggregation scheme generates data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, destination prefix, source prefix mask, destination prefix mask, source BGP AS, destination BGP AS, input interface, and output interface.

The aggregated NetFlow data export records report the following:

- Source and destination prefix
- Source and destination prefix mask
- Source and destination BGP AS
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input and output interfaces
- Time stamp when the first packet is switched and time stamp when the last packet is switched

The figure below shows the data export format for the prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 16: Data Export Format for Prefix Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix aggregation scheme.

Table 20: Data Export Record Terms and Definitions for Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
Reserved	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Prefix-Port Aggregation Scheme

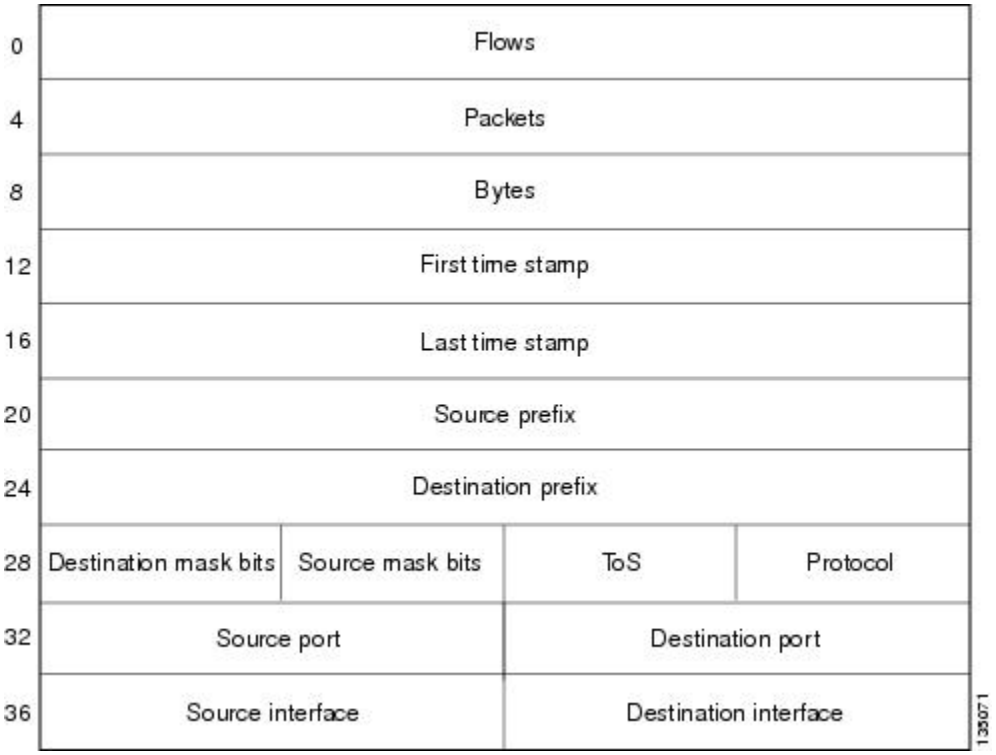
The NetFlow prefix-port aggregation scheme groups flows that have a common source prefix, source mask, destination prefix, destination mask, source port and destination port when applicable, input interface, output interface, protocol, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source port
- Destination port
- Source interface
- Destination interface
- Protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data with which you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below shows the

data export record for the prefix-port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 17: Data Export Record for Prefix-Port Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix-port aggregation scheme.

Table 21: Data Export Record Term Definitions for Prefix-Port Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Protocol	IP protocol byte
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Prefix-ToS Aggregation Scheme

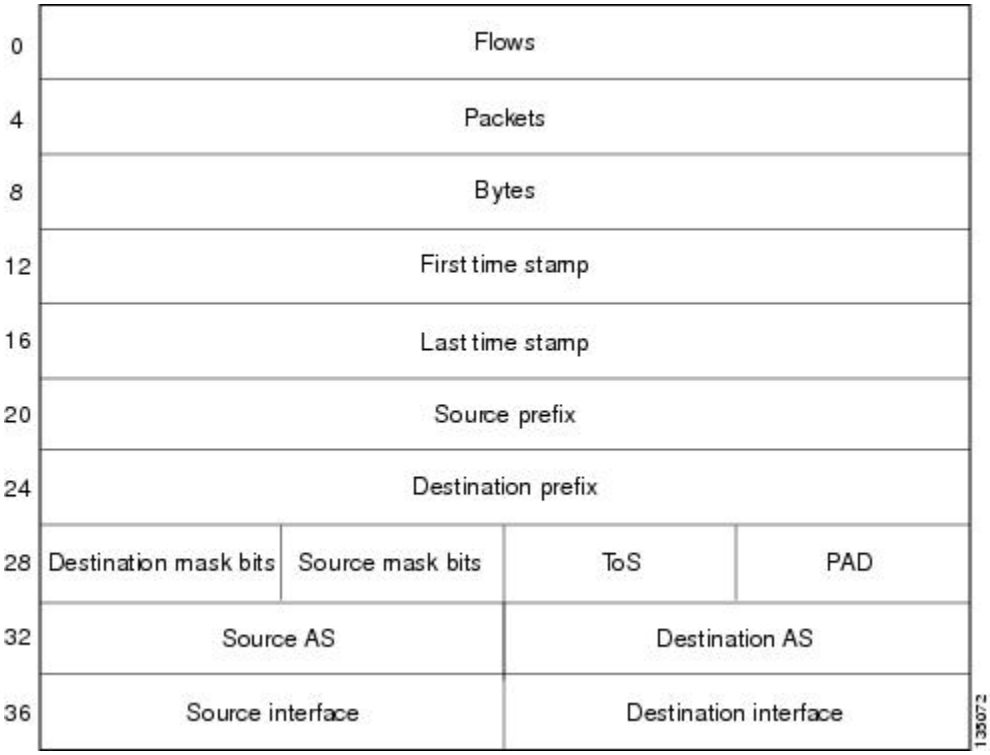
The NetFlow prefix-tos aggregation scheme groups together flows that have a common source prefix, source mask, destination prefix, destination mask, source BGP AS, destination BGP AS, input interface, output interface, and ToS byte. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Destination prefix
- Destination prefix mask
- Source AS
- Destination AS
- Source interface
- Destination interface
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources and destinations of network traffic passing through a NetFlow-enabled device. The figure below displays the data

export format for the prefix-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 18: Data Export Format for Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the prefix-ToS aggregation scheme.

Table 22: Data Export Record Term Definitions for Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Destination prefix	Destination IP address ANDed with the destination prefix mask

Term	Definition
Destination mask bits	Number of bits in the destination prefix
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Pad	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)
Destination AS	Autonomous system of the destination IP address (peer or origin)
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Protocol Port Aggregation Scheme

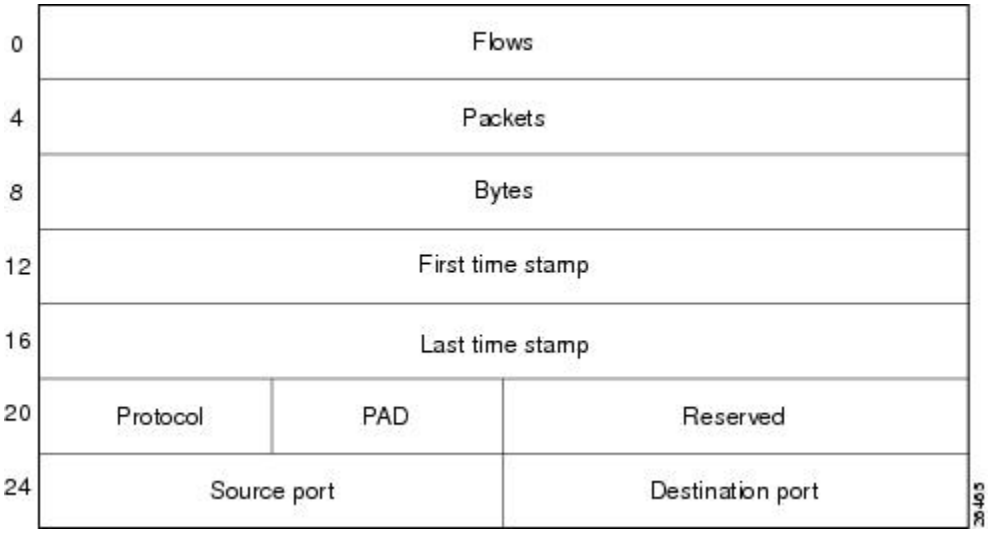
The NetFlow protocol port aggregation scheme captures data so that you can examine network usage by traffic type. The scheme groups data flows with the same IP protocol, source port number, and (when applicable) destination port number.

The aggregated NetFlow data export records report the following:

- Source and destination port numbers
- IP protocol (where 6 = TCP, 17 = UDP, and so on)
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below shows the data export format for the protocol port aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 19: Data Export Format for Protocol Port Aggregation Scheme



The table below lists definitions for the data export record terms used in the protocol port aggregation scheme.

Table 23: Data Export Record Term Definitions for Protocol Port Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Protocol	IP protocol byte
PAD	Zero field
Reserved	Zero field
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number

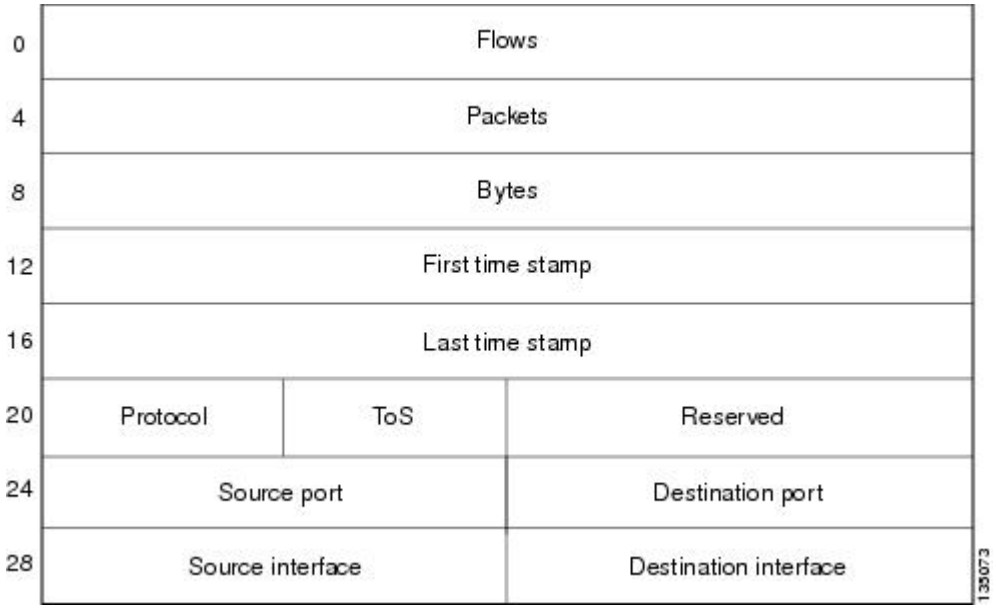
NetFlow Protocol-Port-ToS Aggregation Scheme

The NetFlow protocol-port-tos aggregation scheme groups flows that have a common IP protocol, ToS byte, source and (when applicable) destination port numbers, and source and destination interfaces. The aggregated NetFlow Export record reports the following:

- Source application port number
- Destination port number
- Source and destination interface
- IP protocol
- ToS byte
- Number of flows summarized by the aggregated record
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine network usage by type of traffic. The figure below shows the data export format for the protocol-port-tos aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 20: Data Export Format for Protocol-Port-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the protocol-port-ToS aggregation scheme.

Table 24: Data Export Record Term Definitions for Protocol-Port-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Protocol	IP protocol byte
ToS	Type of service byte
Reserved	Zero field
Source port	Source UDP or TCP port number if applicable
Destination port	Destination User Datagram Protocol (UDP) or TCP port number
Source interface	SNMP index of the input interface
Destination interface	SNMP index of the output interface

NetFlow Source Prefix Aggregation Scheme

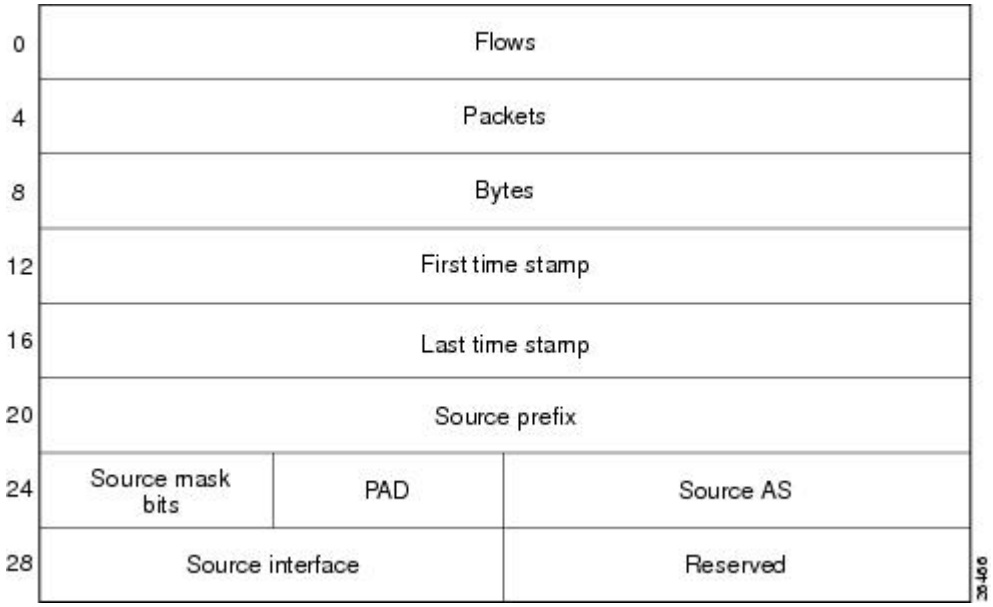
The NetFlow source prefix aggregation scheme captures data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The scheme groups data flows that have the same source prefix, source prefix mask, source BGP AS, and input interface.

The aggregated NetFlow data export records report the following:

- Source prefix
- Source prefix mask
- Source BGP AS
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregated record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

The figure below show the data export format for the source prefix aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Figure 21: Data Export Format for Source Prefix Aggregation Scheme



The table below lists definitions for the data export record terms used in the source prefix aggregation scheme.

Table 25: Data Export Record Term Definitions for Source Prefix Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs
Source mask bits	Number of bits in the source prefix
PAD	Zero field
Source AS	Autonomous system of the source IP address (peer or origin)

Term	Definition
Source interface	SNMP index of the input interface
Reserved	Zero field

NetFlow Source Prefix-ToS Aggregation Scheme

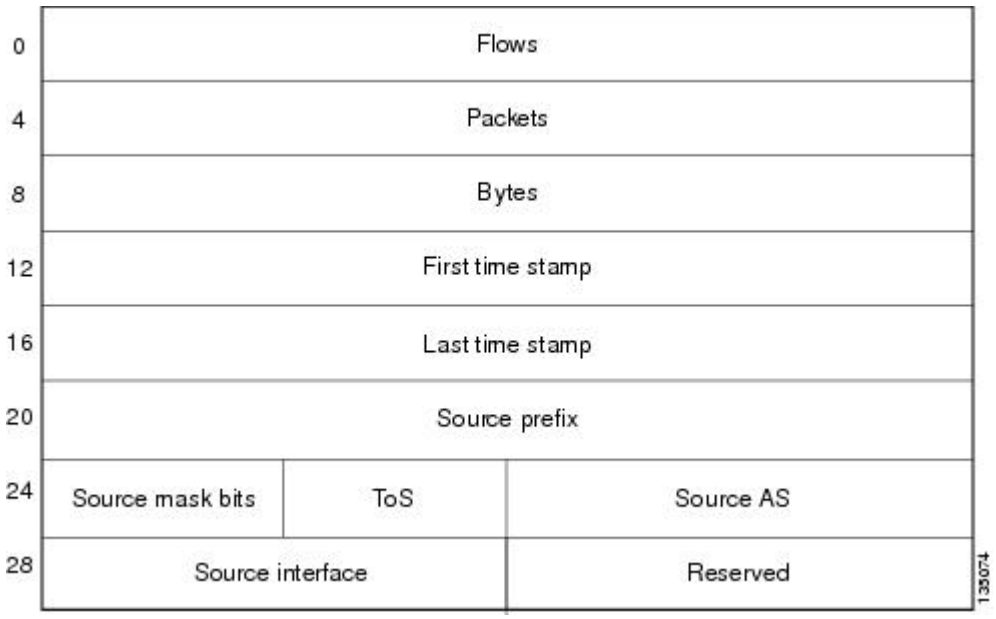
The NetFlow source prefix-ToS aggregation scheme groups flows that have a common source prefix, source prefix mask, source BGP AS, ToS byte, and input interface. The aggregated NetFlow export record reports the following:

- Source prefix
- Source prefix mask
- Source AS
- ToS byte
- Number of bytes summarized by the aggregated record
- Number of packets summarized by the aggregation record
- Input interface
- Time stamp when the first packet was switched and time stamp when the last packet was switched

This aggregation scheme is particularly useful for capturing data so that you can examine the sources of network traffic passing through a NetFlow-enabled device. The figure below show the data export format for the source prefix-ToS aggregation scheme. For a definition of the data export terms used in the aggregation scheme, see the table below.

Note When a router does not have a prefix for the source IP address in the flow, NetFlow uses 0.0.0.0 with 0 mask bits rather than making /32 entries. This prevents DOS attacks that use random source addresses from thrashing the aggregation caches. This is also done for the destination in the destination prefix-ToS, the prefix-ToS, and prefix-port aggregation schemes.

Figure 22: Data Export Format for Source Prefix-ToS Aggregation Scheme



The table below lists definitions for the data export record terms used in the source prefix-ToS aggregation scheme.

Table 26: Data Export Record Term Definitions for Source Prefix-ToS Aggregation Scheme

Term	Definition
Flows	Number of main cache flows that were aggregated
Packets	Number of packets in the aggregated flows
Bytes	Number of bytes in the aggregated flows
First time stamp	System uptime when the first packet was switched
Last time stamp	System uptime when the last packet was switched
Source prefix	Source IP address ANDed with the source prefix mask, or the prefix to which the source IP address of the aggregated flows belongs

Term	Definition
Source mask bits	Number of bits in the source prefix
ToS	Type of service byte
Source AS	Autonomous system of the source IP address (peer or origin)
Source interface	SNMP index of the input interface
Reserved	Zero field

NetFlow Data Export Format Versions 9 and 8 for NetFlow Aggregation Caches Overview

Export formats available for NetFlow aggregation caches are the Version 9 export format and the Version 8 export format.

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as Multicast, Multiprotocol Label Switching (MPLS), and Border Gateway Protocol (BGP) next hop. Version 9 export format enables you to use the same version for main and aggregation caches, and the format is extendable, so you can use the same export format with future features.
- Version 8--A format added to support data export from aggregation caches. Export datagrams contain a subset of the usual Version 5 export data, which is valid for the particular aggregation cache scheme. Version 8 is the default export version for aggregation caches when data export is configured.

The Version 9 export format is flexible and extensible, which provides the versatility needed for the support of new fields and record types. You can use the Version 9 export format for both main and aggregation caches.

The Version 8 export format was added to support data export from aggregation caches. This format allows export datagrams to contain a subset of the Version 5 export data that is valid for the cache aggregation scheme.

Refer to the NetFlow Data Export, on page 70 section for more details.

How to Configure NetFlow Aggregation Caches

Configuring NetFlow Aggregation Caches

Perform the steps in this required to enable NetFlow and configure a NetFlow aggregation cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-aggregation cache** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
4. **cache entries** *number*
5. **cache timeout active** *minutes*
6. **cache timeout inactive** *seconds*
7. **export destination** {{*ip-address* | *hostname*} *udp-port*}
8. Repeat Step 7 once to configure a second export destination.
9. **export version** [**9** | **8**]
10. **enabled**
11. **exit**
12. **interface** *interface-type interface-number*
13. **ip flow** {**ingress** | **egress**}
14. **exit**
15. Repeat Steps 12 through 14 to enable NetFlow on other interfaces
16. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-aggregation cache** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**} **Example:**	(Required) Specifies the aggregation cache scheme and enables aggregation cache configuration mode. • The **as** keyword configures the AS aggregation cache. • The **as-tos**keyword configures the AS ToS aggregation cache. • The **bgp-nexthop-tos** keyword configures the BGP nexthop aggregation cache. • The **destination-prefix** keyword configures the destination prefix aggregation cache.

	Command or Action	Purpose
	Example: `Router(config)# ip flow-aggregation cache destination-prefix`	• The **destination-prefix-tos** keyword configures the destination prefix ToS aggregation cache. • The **prefix** keyword configures the prefix aggregation cache. • The **prefix-port** keyword configures the prefix port aggregation cache. • The **prefix-tos** keyword configures the prefix ToS aggregation cache. • The **protocol-port** keyword configures the protocol port aggregation cache. • The **protocol-port-tos** keyword configures the protocol port ToS aggregation cache. • The **source-prefix** keyword configures the source prefix aggregation cache. • The **source-prefix-tos** keyword configures the source prefix ToS aggregation cache.
Step 4	**cache entries** *number* **Example:** `Router(config-flow-cache)# cache entries 2048`	(Optional) Configures aggregation cache operational parameters. • The **entries** *number* keyword-argument pair is the number of cached entries allowed in the aggregation cache. The range is from 1024 to 524288. The default is 4096.
Step 5	**cache timeout active** *minutes* **Example:** `Router(config-flow-cache)# cache timeout active 15`	(Optional) Configures aggregation cache operational parameters. • The **timeout** keyword dissolves the session in the aggregation cache. • The **active** *minutes* keyword-argument pair specifies the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 6	**cache timeout inactive** *seconds* **Example:** `Router(config-flow-cache)# cache timeout inactive 300`	(Optional) Configures aggregation cache operational parameters. • The **timeout** keyword dissolves the session in the aggregation cache. • The **inactive** *seconds*keyword-argument pair specifies the number of seconds that an inactive entry stays in the aggregation cache before the entry times out. The range is from 10 to 600 seconds. The default is 15 seconds.
Step 7	**export destination** {{*ip-address* | *hostname*} *udp-port*} **Example:** `Router(config-flow-cache)# export destination 172.30.0.1 991`	(Optional) Enables the exporting of information from NetFlow aggregation caches. • The *ip-address* | *hostname*argument is the destination IP address or hostname. • The *port* argument is the destination UDP port.

	Command or Action	Purpose
Step 8	Repeat Step 7 once to configure a second export destination.	(Optional) You can configure a maximum of two export destinations for each NetFlow aggregation cache.
Step 9	**export version** [**9** | **8**] **Example:** `Router(config-flow-cache)# export version 9`	(Optional) Specifies data export format Version. • The **version 9** keyword specifies that the export packet uses the Version 9 format.
Step 10	**enabled** **Example:** `Router(config-flow-cache)# enabled`	(Required) Enables the aggregation cache.
Step 11	**exit** **Example:** `Router(config-if)# exit`	(Required) Exits NetFlow aggregation cache configuration mode and returns to global configuration mode.
Step 12	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 13	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	(Required) Enables NetFlow on the interface. • **ingress** --captures traffic that is being received by the interface • **egress** --captures traffic that is being transmitted by the interface.
Step 14	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 15	Repeat Steps 12 through 14 to enable NetFlow on other interfaces	(Optional) --
Step 16	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Aggregation Cache Configuration

Perform the steps in this optional task to verify that:

- The NetFlow aggregation cache is operational
- NetFlow Data Export for the aggregation cache is operational
- To view the aggregation cache statistics.

SUMMARY STEPS

1. **show ip cache flow aggregation** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}
2. **show ip flow export**

DETAILED STEPS

Step 1 **show ip cache flow aggregation** {**as** | **as-tos** | **bgp-nexthop-tos** | **destination-prefix** | **destination-prefix-tos** | **prefix** | **prefix-port** | **prefix-tos** | **protocol-port** | **protocol-port-tos** | **source-prefix** | **source-prefix-tos**}

Use the **show ip cache flow aggregation destination-prefix** command to verify the configuration of an destination-prefix aggregation cache. For example:

Example:

```
Router# show ip cache flow aggregation destination-prefix
IP Flow Switching Cache, 139272 bytes
  5 active, 2043 inactive, 9 added
  841 ager polls, 0 flow alloc failures
  Active flows timeout in 15 minutes
  Inactive flows timeout in 300 seconds
IP Sub Flow Cache, 11144 bytes
  5 active, 507 inactive, 9 added, 9 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
Dst If         Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Null           0.0.0.0         /0   0         5    13    52   138.9
Et0/0.1        172.16.6.0      /24  0         1     1    56     0.0
Et1/0.1        172.16.7.0      /24  0         3    31K 1314   187.3
Et0/0.1        172.16.1.0      /24  0        16   104K 1398   188.4
Et1/0.1        172.16.10.0     /24  0         9    99K 1412   183.3
Router#
```

Use the **show ip cache verbose flow aggregation source-prefix**command to verify the configuration of a source-prefix aggregation cache. For example:

Example:

```
Router# show ip cache verbose flow aggregation source-prefix
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  51 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
```

```
  4 active, 1020 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Et1/0.1        172.16.10.0     /24  0         4    35K 1391    67.9
Et0/0.1        172.16.6.0      /24  0         2     5    88    60.6
Et1/0.1        172.16.7.0      /24  0         2  3515  1423    58.6
Et0/0.1        172.16.1.0      /24  0         2    20K 1416    71.9
Router#
```

Use the **show ip cache verbose flow aggregation protocol-port** command to verify the configuration of a protocol-port aggregation cache. For example:

Example:

```
Router# show ip cache verbose flow aggregation protocol-port
IP Flow Switching Cache, 278544 bytes
  4 active, 4092 inactive, 4 added
  158 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
  0x01       0x0000      0x0000      6       52K     1405        104.3
  0x11       0x0208      0x0208      1        3        52         56.9
  0x01       0x0000      0x0800      2      846      1500         59.8
  0x01       0x0000      0x0B01      2       10        56         63.0
Router#
```

Step 2 **show ip flow export**

Use the **show ip flow export** command to verify that NetFlow Data Export is operational for the aggregation cache. For example:

Example:

```
Router# show ip flow export
Flow export v1 is disabled for main cache
  Version 1 flow records
  Cache for protocol-port aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for source-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  Cache for destination-prefix aggregation:
    Exporting flows to 172.16.20.4 (991) 172.30.0.1 (991)
    Exporting using source IP address 172.16.6.2
  40 flows exported in 20 udp datagrams
  0 flows failed due to lack of export packet
  20 export packets were sent up to process level
  0 export packets were dropped due to no fib
  0 export packets were dropped due to adjacency issues
  0 export packets were dropped due to fragmentation failures
  0 export packets were dropped due to encapsulation fixup failures
Router#
```

Configuration Examples for Configuring NetFlow Aggregation Caches

Configuring an AS Aggregation Cache Example

The following example shows how to configure an AS aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal
!
ip flow-aggregation cache as
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Destination Prefix Aggregation Cache Example

The following example shows how to configure a destination prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Prefix Aggregation Cache Example

The following example shows how to configure a prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Protocol Port Aggregation Cache Example

The following example shows how to configure a protocol port aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache protocol-port
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Source Prefix Aggregation Cache Example

The following example shows how to configure a source prefix aggregation cache with a cache size of 2046, an inactive timeout of 200 seconds, a cache active timeout of 45 minutes, an export destination IP address of 10.42.42.1, and a destination port of 9992:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 cache entries 2046
 cache timeout inactive 200
 cache timeout active 45
 export destination 10.42.42.1 9992
```

```
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring an AS-ToS Aggregation Cache Example

The following example shows how to configure an AS-ToS aggregation cache with a cache active timeout of 20 minutes, an export destination IP address of 10.2.2.2, and a destination port of 9991:

```
configure terminal

!

ip flow-aggregation cache as-tos
 cache timeout active 20
 export destination 10.2.2.2 9991
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring a Prefix-ToS Aggregation Cache Example

The following example shows how to configure a prefix-ToS aggregation cache with an export destination IP address of 10.4.4.4 and a destination port of 9995:

```
configure terminal

!

ip flow-aggregation cache prefix-tos
 export destination 10.4.4.4 9995
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache prefix
 mask source minimum 24
 mask destination minimum 28
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Destination Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a destination prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache destination-prefix
 mask destination minimum 32
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring the Minimum Mask of a Source Prefix Aggregation Scheme Example

The following example shows how to configure the minimum mask for a source prefix aggregation scheme:

```
configure terminal

!

ip flow-aggregation cache source-prefix
 mask source minimum 30
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring NetFlow Version 9 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 9 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export template refresh-rate 10
 export version 9
 export template timeout-rate 60
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Configuring NetFlow Version 8 Data Export for Aggregation Caches Example

The following example shows how to configure NetFlow Version 8 data export for an AS aggregation cache scheme:

```
configure terminal
!
ip flow-aggregation cache as
 export destination 10.42.42.2 9991
 export destination 10.42.41.1 9991
 export version 8
 enabled
!
interface Ethernet0/0
 ip flow ingress
!
 end
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow

Related Topic	Document Title
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBS are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Aggregation Caches

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 . An account on Cisco.com is not required.

Table 27: Feature Information for Configuring NetFlow Aggregation Caches

Feature Name	Releases	Feature Configuration Information
NetFlow ToS-Based Router Aggregation	12.0(15)S 12.2(4)T 12.2(14)S 15.0(1)S	The NetFlow ToS-Based Router Aggregation feature enables you to limit router-based type of service (ToS) aggregation of NetFlow export data. The aggregation of export data provides a summarized NetFlow export data that can be exported to a collection device. The result is lower bandwidth requirements for NetFlow export data and reduced platform requirements for NetFlow data collection devices. The following commands were modified by this feature: **ip flow-aggregation cache**, **show ip cache verbose flow aggregation**, and **show ip flow export**.

Feature Name	Releases	Feature Configuration Information
NetFlow Minimum Prefix Mask for Router-Based Aggregation	12.0(11)S 12.1(2)T	The NetFlow Minimum Prefix Mask for Router-Based Aggregation feature allows you to set a minimum mask size for prefix aggregation, destination prefix aggregation, and source prefix aggregation schemes. The following commands were modified by this feature: **ip flow-aggregation cache**, **mask destination**, **mask source**, and **show ip cache flow aggregation**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --Distributed Cisco Express Forwarding. Type of CEF switching in which line cards maintain an identical copy of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --Type of packet built by a device (for example, a router) with NetFlow services enabled. The packet contains NetFlow statistics and is addressed to another device (for example, the NetFlow Collection Engine). The other device processes the packet (parses, aggregates, and stores information on IP flows).

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

flowset --Collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two different types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

NetFlow --Cisco IOS accounting feature that maintains per-flow information.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router

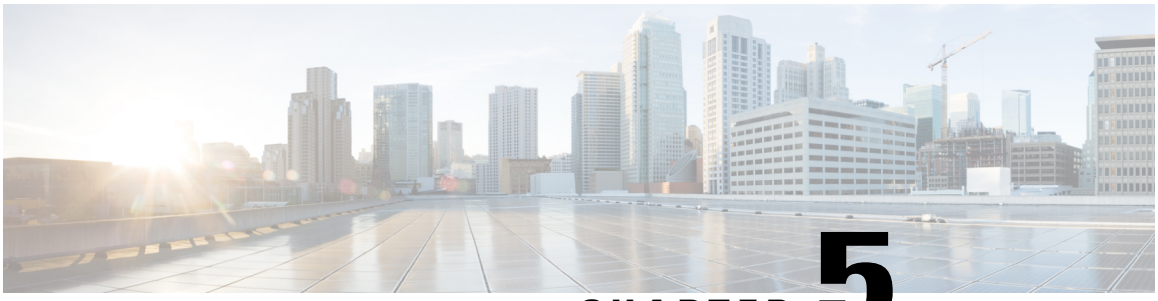
that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

QoS --quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

template flowset --One or more template records that are grouped in an export packet.

ToS --type of service. The second byte in the IP header. It indicates the desired quality of service (QoS) for a particular datagram.



CHAPTER 5

Using NetFlow Filtering or Sampling to Select the Network Traffic to Track

This module contains information about and instructions for selecting the network traffic to track through the use of NetFlow filtering or sampling. The NetFlow Input Filtering and Random Sampled NetFlow features, described in this module, allow you to collect data from specific subsets of traffic.

- The NetFlow Input Filters feature provides NetFlow data for a specific subset of traffic by letting you create filters to select flows for NetFlow processing. For example, you can select flows from a specific group of hosts.
- The Random Sampled NetFlow feature provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter).

NetFlow is a Cisco IOS application that provides statistics on packets that flow through the router. It is emerging as a primary network accounting and security technology.

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 NetFlow Filtering or Sampling to Select Network Traffic to Track

Prerequisites for NetFlow Input Filters

Before you can configure the NetFlow Input Filters feature, you must:

- Configure the router for IP routing.
- Configure Cisco Express Forwarding (CEF) switching or distributed Cisco Express Forwarding (dCEF) switching on the router and on the interfaces that you want to enable NetFlow Input Filters on (fast switching is not supported).
- Create traffic classes and define NetFlow sampler maps.

Note The NetFlow Input Filters feature is supported in the Version 5 and Version 9 NetFlow export formats.

Prerequisites for Random Sampled NetFlow

Before you can configure the Random Sampled NetFlow feature, you must:

- Configure the router for IP routing.
- Configure Cisco Express Forwarding (CEF) switching or distributed CEF (dCEF) switching on the router and on the interfaces that you want to enable Random Sampled NetFlow on (fast switching is not supported).
- Configure NetFlow Version 5 or Version 9 data export if you want to export NetFlow data (otherwise, NetFlow data is visible in the cache, but is not exported).
- Configure NetFlow Version 9 if you want to use sampler option templates or view NetFlow sampler IDs.

Restrictions for Using NetFlow Filtering or Sampling to Select Network Traffic to Track

Restrictions for NetFlow Input Filters

On Cisco 7500 platforms, the NetFlow Input Filters feature is supported only in distributed mode.

Restrictions for Random Sampled NetFlow

If full NetFlow is enabled on an interface, it takes precedence over Random Sampled NetFlow (which will thus have no effect). This means that you should disable full NetFlow on an interface before enabling Random Sampled NetFlow on that interface.

Enabling Random Sampled NetFlow on a physical interface does not automatically enable Random Sampled NetFlow on subinterfaces; you must explicitly configure it on subinterfaces. Also, disabling Random Sampled NetFlow on a physical interface (or a subinterface) does not enable full NetFlow. This restriction prevents the transition to full NetFlow from overwhelming the physical interface (or subinterface). If you want full NetFlow, you must explicitly enable it.

If you enable Random Sampled NetFlow with Version 5 data export, sampler option templates are not exported, and sampler IDs are exported in the least significant three bits of the last byte of the Version 5 record pad field. Use NetFlow Version 9 if you want to use sampler option templates or view NetFlow sampler IDs.

Information About Using NetFlow Filtering or Sampling to Select Network Traffic to Track

Roadmap Using NetFlow Filtering or Sampling to Select the Network Traffic to Track

The table below provides a roadmap that includes links to associated information and configuration instruction for selecting traffic of interest.

Table 28: Roadmap: Selecting the Network Traffic to Track Using Sampling and Filtering

Traffic of Interest	Links to Associated Information and Configuration Instructions
A specific subset of NetFlow traffic for the purpose of class-based traffic analysis and monitoring (including on-network or off-network traffic)	Associated information: Configuration instructions:
Statistical sampling of network traffic for traffic engineering or capacity planning purposes	Associated information: Configuration instructions:

Filtering and Sampling of NetFlow Traffic

NetFlow provides highly granular per-flow traffic statistics in a Cisco router. A flow is a unidirectional stream of packets that arrive at the router on the same subinterface, have the same source and destination IP addresses, Layer 4 protocol, TCP/UDP source and destination ports, and the same type of service (ToS) byte in the IP headers. The router accumulates NetFlow statistics in a NetFlow cache and can export them to an external device (such as the Cisco Networking Services (CNS) NetFlow Collection Engine) for further processing.

Full NetFlow accounts for all traffic entering the subinterface on which it is enabled. But in some cases, you might gather NetFlow data on only a subset of this traffic. The Random Sampled NetFlow feature and the NetFlow Input Filters feature each provide ways to limit incoming traffic to only traffic of interest for NetFlow processing. Random Sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets. The NetFlow Input Filters feature provides the capability to gather NetFlow data on only a specific user-defined subset of traffic.

Note Random Sampled NetFlow is more statistically accurate than Sampled NetFlow. NetFlow's ability to sample packets was first provided by a feature named Sampled NetFlow. The methodology that the Sampled NetFlow feature uses is *deterministic* sampling, which selects every nth packet for NetFlow processing on a per-interface basis. For example, if you set the sampling rate to 1 out of 100 packets, then Sampled NetFlow samples the 1st, 101st, 201st, 301st, and so on packets. Sampled NetFlow does not allow random sampling and thus can make statistics inaccurate when traffic arrives in fixed patterns.

Note The Random Sampled NetFlow algorithms are applied after input filtering.

The table below compares the NetFlow Input Filters feature and the NetFlow Random Sampled feature.

Table 29: Comparison of the NetFlow Input Filters Feature and the Random Sampled NetFlow Feature

Comparison Category	NetFlow Input Filters Feature	Random Sampled NetFlow Feature
Brief description	This feature enables you to gather NetFlow data on only a specific subset of traffic. You do this by creating filters to select flows for NetFlow processing. For example, you can select flows from a specific group of hosts. This feature also lets you select various sampling rates for selected flows.	This feature provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter). Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets).
Main uses	You can use this feature for class-based traffic analysis and monitoring on-network or off-network traffic.	You can use this feature for traffic engineering, capacity planning, and applications where full NetFlow is not needed for an accurate view of network traffic.
Export format support	This feature is supported in the Version 5 and Version 9 NetFlow export formats.	This feature is supported in the Version 5 and Version 9 NetFlow export formats.

Comparison Category	NetFlow Input Filters Feature	Random Sampled NetFlow Feature
Cisco IOS release support	12.3(4)T.	12.3(2)T, 12.2(18)S, and 12.0(26)S.
Subinterface support	You can configure NetFlow Input Filters per subinterface as well as per physical interface. You can select more than one filter per subinterface and have all of the filters run simultaneously.	You can configure the Random Sampled NetFlow feature per subinterface as well as per physical interface. Traffic is collected only on the subinterfaces on which Random Sampled NetFlow is configured. As with full NetFlow, enabling Random Sampled NetFlow on a physical interface does not enable Random Sampled NetFlow on subinterfaces automatically--you must explicitly configure it on the subinterfaces.
Memory impact	This feature requires no additional memory. It allows you to use a smaller NetFlow cache than full NetFlow, because it significantly reduces the number of flows. This feature requires an insignificant amount of memory for each configured NetFlow sampler.	This feature allows a smaller NetFlow cache than full NetFlow, because it significantly reduces the number of flows. This feature requires an insignificant amount of memory for each configured NetFlow sampler.
Performance impact	Accounting of classified traffic saves router resources by reducing the number of flows being processed and exported. The amount of bandwidth saved depends on the usage and the class-map criteria. However, performance might degrade depending on the number and complexity of class maps configured in a policy.	Statistical traffic sampling substantially reduces consumption of router resources (especially CPU resources) while providing valuable NetFlow data. This feature substantially reduces the impact of NetFlow data export on interface traffic. For example, a sampling rate of 1 out of 100 packets reduces the export of NetFlow data by about 50 percent.

NetFlow Input Filters Flow Classification

For the NetFlow Input Filters feature, classification of packets can be based on any of the following: IP source and destination addresses, Layer 4 protocol and port numbers, incoming interface, MAC address, IP Precedence, DSCP value, Layer 2 information (such as Frame-Relay DE bits or Ethernet 802.1p bits), and Network-Based Application Recognition (NBAR) information. The packets are classified (filtered) on the above criteria, and flow accounting is applied to them on subinterfaces.

The filtering mechanism uses the Modular QoS Command-Line Interface (MQC) to classify flows. You can create multiple filters with matching samplers on a per-subinterface basis. For example, you can subdivide subinterface traffic into multiple classes based on type of service (ToS) values or destination prefixes (or both). For each class, you can also configure sampling at a different rate, using higher rates for higher-priority classes of traffic and lower rates for lower-priority ones.

MQC has many policies (actions) such as bandwidth rate and queuing management. These policies are applied only if a packet matches a criterion in a class map that is applied to the subinterface. A class map contains a set of match clauses and instructions on how to evaluate the clauses and acts as a filter for the policies, which are applied only if a packet's content satisfies the match clause. The NetFlow Input Filters feature adds NetFlow accounting to the MQC infrastructure, which means that flow accounting is done on a packet only if it satisfies the match clauses.

Two types of filter are available:

- ACL-based flow-mask filters
- Fields of filter (source IP address, destination IP address, source application port, destination application port, port protocol, ToS bits, and TCP flags)

Random Sampled NetFlow Sampling Mode

Sampling mode makes use of an algorithm that selects a subset of traffic for NetFlow processing. In the random sampling mode that the Random Sampled NetFlow feature uses, incoming packets are randomly selected so that one out of each n sequential packets is selected *on average* for NetFlow processing. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th packet and then the 120th, 199th, 302nd, and so on. This sample configuration provides NetFlow data on 1 percent of total traffic. The n value is a parameter from 1 to 65535 packets that you can configure.

Random Sampled NetFlow The NetFlow Sampler

A NetFlow sampler map defines a set of properties (such as the sampling rate and NetFlow sampler name) for NetFlow sampling. Each NetFlow sampler map can be applied to one or many subinterfaces as well as physical interfaces. You can define up to eight NetFlow sampler maps.

For example, you can create a NetFlow sampler map named mysampler1 with the following properties: random sampling mode and a sampling rate of 1 out of 100 packets. This NetFlow sampler map can be applied to any number of subinterfaces, each of which would refer to mysampler1 to perform NetFlow sampling. Traffic from these subinterfaces is merged (from a sampling point of view). This introduces even more "randomness" than random per-subinterface NetFlow sampling does, but statistically it provides the same sampling rate of 1 out of 100 packets for each participating subinterface.

The sampling in random sampled NetFlow is done by NetFlow samplers. A NetFlow sampler is defined as an instance of a NetFlow sampler map that has been applied to a physical interface or subinterface. If full NetFlow is configured on a physical interface, it overrides random sampled NetFlow on all subinterfaces of this physical interface.

How to Configure NetFlow Filtering or Sampling

Note You need to configure input filtering before you apply the random sampled NetFlow algorithms.

Configuring NetFlow Input Filters to Reduce the Impact of NetFlow Data Export

Perform the following tasks to configure NetFlow input filters. Configuring NetFlow input filters reduces the impact of NetFlow data export.

Creating a Class Map for a Policy Map for NetFlow Input Filtering

Perform the following steps to create a class map for a policy map for NetFlow input filtering.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** *class-map-name* [**match-all** | **match-any**]
4. **match access-group** *access-group*
5. **end**

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	**class-map** *class-map-name* [**match-all** | **match-any**] **Example:** `Router(config)# class-map my_high_importance_class`	Creates a class map to be used for matching packets to a specified class. • The *class-map-name* argument is the name of the class for the class map. The name can be a maximum of 40 alphanumeric characters. The class name is used for both the class map and for configuring policy for the class in the policy map. • The **match-all | match-any**keywords determine how packets are evaluated when multiple match criteria exist. Packets must either meet all of the match criteria (**match-all)** or only one of the match criteria (**match-any**) to be considered a member of the class. Entering the **class-map**command enables class-map configuration mode, in which you can enter one of the match commands to configure the match criteria for this class.

	Command or Action	Purpose
Step 4	**match access-group** *access-group* **Example:** `Router(config-cmap)# match access-group 101`	Configures the match criteria for a class map on the basis of the specified access control list (ACL). • The *access-group* argument is a numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
Step 5	**end** **Example:** `Router(config-cmap)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Creating a Sampler Map for a Policy Map for NetFlow Input Filtering

Perform the following steps to create a sampler map for a policy map for NetFlow input filtering.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random** *one-out-of* **packet-interval**
5. **end**

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-sampler-map** *sampler-map-name*	Defines a statistical sampling NetFlow export flow sampler map.

	Command or Action	Purpose
	Example: `Router(config)# flow-sampler-map my_high_sampling`	• The *sampler-map-name* argument is the name of the flow sampler map to be defined. Entering the **flow-sampler-map** command enables the flow sampler configuration mode.
Step 4	**mode random** *one-out-of* **packet-interval** **Example:** `Router(config-sampler-map)# mode random one-out-of 100`	Specifies a statistical sampling NetFlow export random sampling mode and a packet interval. • The **random** keyword specifies that sampling uses the random sampling mode. • The *one-out-of* **packet-interval** argument-keyword pair specifies the packet interval (one out of every *n*packets) from which to sample. For *n*, you can specify from 1 to 65535 (packets).
Step 5	**end** **Example:** `Router(config-sampler-map)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Creating a Class-Based Policy Containing NetFlow Sampling Actions

Perform thefollowing steps to create a class-based policy that contains NetFlow sampling actions.

You can assign only one NetFlow input filters sampler to a class. Assigning a subsequent NetFlow input filters sampler to a class overwrites the previous sampler. Removing a NetFlow sampler map also removes the NetFlow input filters sampler from the corresponding policy map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** *policy-map-name*
4. **class** {*class-name* | **class-default**}
5. **netflow-sampler** *sampler-map-name*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enables privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map mypolicymap`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. • The *policy-map-name* argument is the name of the policy map. The name can be a maximum of 40 alphanumeric characters. Entering the **policy-map**command enables quality of service (QoS) policy-map configuration mode, in which you can configure or modify the class policies for that policy map.
Step 4	**class** {*class-name* | **class-default**} **Example:** `Router(config-pmap)# class my_high_importance_class`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • The *class-name* argument is the name of the class for which you want to configure or modify policy. • The **class-default** keyword specifies the default class so that you can configure or modify its policy. Entering the **class** command enables QoS policy-map class configuration mode.
Step 5	**netflow-sampler** *sampler-map-name* **Example:** `Router(config-pmap-c)# netflow-sampler high_sampling`	Enables a NetFlow input filter sampler. • The *sampler-map-name* argument is the name of the NetFlow sampler map to apply to the class. You can assign only one NetFlow input filter sampler to a class. Assigning another NetFlow input filter sampler to a class overwrites the previous one.
Step 6	**end** **Example:** `Router(config-pmap-c)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Applying a Policy Containing NetFlow Sampling Actions to an Interface

Perform the following steps to apply a policy containing NetFlow sampling actions to an interface.

After you define a service policy with the **policy-map**command, you use the **service-policy** command in interface configuration mode to attach it to one or more interfaces, thus specifying the service policy for those interfaces. Although you can assign the same service policy to multiple interfaces, each interface can have only one service policy attached. You can apply the service policy only in the input direction.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **service-policy** {**input** | **output**} *policy-map-name*
5. **end**

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** *interface-type interface-number* **Example:** `Router(config)# interface POS 1/0`	Specifies the interface and enters interface configuration mode.
Step 4	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-if)# service-policy input mypolicymap`	Attaches a policy map to an input interface or virtual circuit (VC), or an output interface or VC, to be used as the service policy for that interface or VC. • The **input** keyword attaches the specified policy map to the input interface or input VC. • The **output** keyword attaches the specified policy map to the output interface or output VC. • The *policy-map-name* is the name of a service policy map (created through use of the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.

	Command or Action	Purpose
Step 5	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **debug flow-sampler class-based**command to display debugging output for NetFlow input filters.

Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export

Perform the following tasks to configure and verify the configuration for the Random Sampled NetFlow feature:

Defining a NetFlow Sampler Map

Perform the following task to define a NetFlow sampler map.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random one-out-of** *sampling-rate*
5. **end**

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	**flow-sampler-map** *sampler-map-name* **Example:** `Router(config)# flow-sampler-map mysampler1`	Defines a NetFlow sampler map and enters flow sampler map configuration mode. • The *sampler-map-name* argument is the name of the NetFlow sampler map to be defined.
Step 4	**mode random one-out-of** *sampling-rate* **Example:** `Router(config-sampler)# mode random one-out-of 100`	Enables random mode and specifies a sampling rate for the NetFlow sampler. • The **random** keyword specifies that sampling uses the random mode. • The **one-out-of** *sampling-rate* keyword-argument pair specifies the sampling rate (one out of every *n* packets) from which to sample. For *n*, you can specify from 1 to 65535 (packets).
Step 5	**end** **Example:** `Router(config-sampler)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Applying a NetFlow Sampler Map to an Interface

Perform the following task to apply a NetFlow sampler map to an interface.

You can apply a NetFlow sampler map to a physical interface (or a subinterface) to create a NetFlow sampler.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **flow-sampler** *sampler-map-name*
5. **end**

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** *interface-type interface-number* **Example:** `Router(config)# ethernet 1/0.2`	Specifies the interface and enters interface configuration mode.
Step 4	**flow-sampler** *sampler-map-name* **Example:** `Router(config-if)# flow-sampler mysampler1`	Applies a NetFlow sampler map to the interface to create the NetFlow sampler. • The *sampler-map-name* argument is the name of the NetFlow sampler map to apply to the interface.
Step 5	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Verifying the Configuration of Random Sampled NetFlow

Perform the following tasks to verify the configuration of the Random Sampled NetFlow feature.

SUMMARY STEPS

1. **show flow-sampler**
2. **show ip cache verbose flow**
3. **show ip flow export template**

DETAILED STEPS

Step 1 **show flow-sampler**

Use this command to display attributes (including mode, sampling rate, and number of sampled packets) of one or all Random Sampled NetFlow samplers to verify the sampler configuration. For example:

Example:

```
Router# show flow-sampler
Sampler : mysampler1, id : 1, packets matched : 10, mode : random sampling mode
  sampling interval is : 100
 Sampler : myflowsampler2, id : 2, packets matched : 5, mode : random sampling mode
  sampling interval is : 200
```

To verify attributes for a particular NetFlow sampler, use the **show flow-sampler** *sampler-map-name*command. For example, enter the following for a NetFlow sampler named mysampler1:

Example:

```
Router# show flow-sampler mysampler1
Sampler : mysampler1, id : 1, packets matched : 0, mode : random sampling mode
  sampling interval is : 100
```

Step 2 **show ip cache verbose flow**

Use this command to display additional NetFlow fields in the header when Random Sampled NetFlow is configured. For example:

Example:

```
Router# show ip cache verbose flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
BGP: BGP NextHop
Et1/0          8.8.8.8         Et0/0*         9.9.9.9         01 00  10       3
0000 /8  302                   0800 /8  300   3.3.3.3              100     0.1
BGP: 2.2.2.2         Sampler: 1  Class: 1  FFlags: 01
```

This example shows the NetFlow output of the **show ip cache verbose flow** command in which the sampler, class-id, and general flags are set. What is displayed for a flow depends on what flags are set in the flow. If the flow was captured by a sampler, the output shows the sampler ID. If the flow was marked by MQC, the display includes the class ID. If any general flags are set, the output includes the flags.

NetFlow flags (FFlags) that might appear in the **show ip cache verbose flow** command output are:

- FFlags: 01 (#define FLOW_FLAGS_OUTPUT 0x0001)--Egress flow
- FFlags: 02 (#define FLOW_FLAGS_DROP 0x0002)--Dropped flow (for example, dropped by an ACL)
- FFlags: 04 (#define FLOW_FLAGS_MPLS 0x0004)--MPLS flow
- FFlags: 08 (#define FLOW_FLAGS_IPV6 0x0008)--IPv6 flow
- FFlags: 10 (#define FLOW_FLAGS_RSVD 0x0010)--Reserved

IPv6 and RSVD FFlags are seldom used. If FFlags is zero, the line is omitted from the output. If multiple flags are defined (logical ORed together), then both sets of flags are displayed in hexadecimal format.

Step 3 **show ip flow export template**

Use this command to display the statistics for the NetFlow data export (such as template timeout and refresh rate) for the template-specific configurations. For example:

Example:

```
Router# show ip flow export template
Template Options Flag = 0
   Total number of Templates added = 0
   Total active Templates = 0
   Flow Templates active = 0
   Flow Templates added = 0
   Option Templates active = 0
   Option Templates added = 0
   Template ager polls = 0
   Option Template ager polls = 0
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
 Option export information
   Option timeout = 30
   Option refresh rate = 20
```

Troubleshooting Tips

Use the **debug flow-sampler**command to display debugging output for the Random Sampled NetFlow feature.

Configuration Examples for Configuring NetFlow Filtering and Sampling

Example Configuring NetFlow Input Filters to Reduce the Impact of NetFlow Data Export

Example Creating a Class Map for a Policy Map for NetFlow Input Filtering

The following example shows how to create a class map for a policy map for NetFlow input filtering. In the example, class maps named my_high_importance_class and my_medium_importance_class are created.

```
configure terminal
!
class-map my_high_importance_class
 match access-group 101
 exit
!
class-map my_medium_importance_class
 match access-group 102
 end
```

Example Creating a Sampler Map for a Policy Map for NetFlow Input Filtering

The following example shows how to create a sampler map for a policy map for NetFlow input filtering. In the following example, sampler maps called my_high_sampling, my_medium sampling, and my_low_samplng are created for use with a policy map for NetFlow input filtering.

```
configure terminal
!
flow-sampler-map my_high_sampling
 mode random one-out-of 1
 exit
!
flow-sampler-map my_medium_sampling
 mode random one-out-of 100
 exit
!
flow-sampler-map my_low_sampling
 mode random one-out-of 1000
 end
```

Example Creating a Policy Containing NetFlow Sampling Actions

The following example shows how to create a class-based policy containing three NetFlow sampling actions. In this example, a sampling action named my_high_sampling is applied to a class named my_high_importance_class, a sampling action named my_medium_sampling is applied to a class named my_medium_importance_class, and a sampling action named my_low_sampling is applied to the default class.

```
configure terminal
!
policy-map mypolicymap
 class my_high_importance_class
 netflow sampler my_high_sampling
 exit
!
class my_medium_importance_class
 netflow-sampler my_medium_sampling
 exit
!
class class-default
 netflow-sampler my_low_sampling
end
```

Example Applying a Policy to an Interface

The following example shows how to apply a policy containing NetFlow sampling actions to an interface. In this example, a policy named mypolicymap is attached to interface POS1/0 and also to interface ATM2/0.

```
configure terminal
!
interface POS1/0
 service-policy input mypolicymap
 exit
!
interface ATM2/0
 service-policy input mypolicymap
 end
```

Example Configuring Random Sampled NetFlow to Reduce the Impact of NetFlow Data Export

Example Defining a NetFlow Sampler Map

The following example shows how to define a NetFlow sampler map named mysampler1:

```
configure terminal
!
flow-sampler-map mysampler1
 mode random one-out-of 100
 end
```

Example Applying a NetFlow Sampler Map to an Interface

The following example shows how to enable CEF switching and apply a NetFlow sampler map named mysampler1 to Ethernet interface 1 to create a NetFlow sampler on that interface:

```
configure terminal
!
ip cef
!
interface ethernet 1/0
 flow-sampler mysampler1
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NetFlow commands	*Cisco IOS NetFlow Command Reference*
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis

Related Topic	Document Title
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	"Configuring NetFlow Multicast Accounting"
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

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

MIBs

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

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature.	--

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 Using NetFlow Filtering or Sampling to Select Network Traffic to Track

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 . An account on Cisco.com is not required.

Table 30: Feature Information for Using NetFlow Filtering or Sampling to Select Network Traffic to Track

Feature Name	Releases	Feature Information
NetFlow Input Filters	12.3(4)T, 12.2(25)S 12.2(27)SBC 15.0(1)S	The NetFlow Input Filters feature provides NetFlow data for a specific subset of traffic by letting you create filters to select flows for NetFlow processing. For example, you can select flows from a specific group of hosts. This feature also lets you select various sampling rates for selected flows. The NetFlow Input Filters feature is used, for example, for class-based traffic analysis and monitoring on-network or off-network traffic. The following commands were introduced or modified by this feature: **netflow-sampler** and **debug flow-sampler**.

Feature Name	Releases	Feature Information
Random Sampled NetFlow	12.3(4)T, 12.2(18)S, 12.0(26)S, 12.2(27)SBC 12.2(33)SRC	Random Sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter). Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets). Statistical traffic sampling substantially reduces consumption of router resources (especially CPU resources) while providing valuable NetFlow data. The main uses of Random Sampled NetFlow are traffic engineering, capacity planning, and applications where full NetFlow is not needed for an accurate view of network traffic. In Cisco IOS Release 12.2(33)SRC, this feature was enhanced to support IPv6 unicast and IPv4 multicast functionality. The following commands were introduced by this feature: **debug flow-sampler**, **flow-sampler**, **flow-sampler-map**, **mode** (**flow sampler map configuration**), and **show flow-sampler**. The following command was modified by this feature: **ip flow-export**.

Glossary

ACL --Access control list. A roster of users and groups of users kept by a router. The list is used to control access to or from the router for a number of services.

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a certain destination.

CEF --Cisco Express Forwarding. Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --Distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

fast switching --Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --Unidirectional stream of packets between a given source and destination. Source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers.

MQC --Modular QoS command-line interface. A CLI structure that lets you create traffic polices and attach them to interfaces. A traffic policy contains a traffic class and one or more QoS features. The QoS features in the traffic policy determine how the classified traffic is treated.

NBAR --Network-Based Application Recognition. A classification engine in Cisco IOS software that recognizes a wide variety of applications, including web-based applications and client/server applications that dynamically assign Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) port numbers. After the application is recognized, the network can invoke specific services for that application. NBAR is a key part of the Cisco Content Networking architecture and works with QoS features to let you use network bandwidth efficiently.

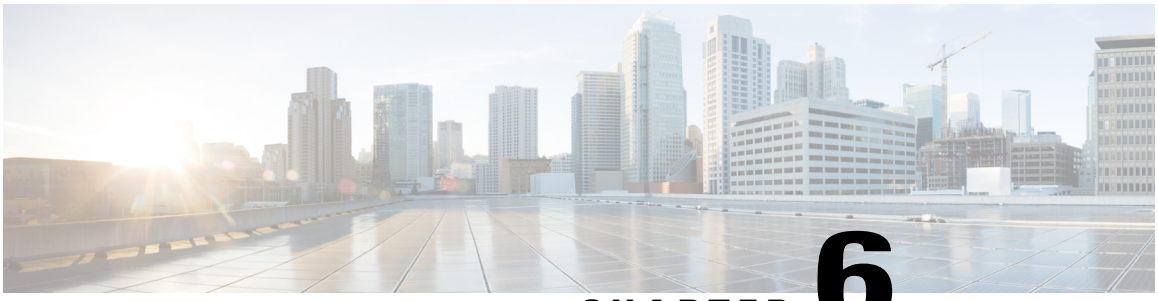
NetFlow --Cisco IOS security and accounting feature that maintains per-flow information.

NetFlow sampler --A set of properties that are defined in a NetFlow sampler map that has been applied to at least one physical interface or subinterface.

NetFlow sampler map --The definition of a set of properties (such as the sampling rate) for NetFlow sampling.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

ToS --type of service. Second byte in the IP header that indicates the desired quality of service for a specific datagram.



CHAPTER 6

Configuring NetFlow BGP Next Hop Support for Accounting and Analysis

This document provides information about and instructions for configuring NetFlow Border Gateway Protocol (BGP) next hop support. This feature lets you measure network traffic on a per BGP next hop basis. NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

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 NetFlow BGP Next Hop Support

Before you can configure the NetFlow BGP Next Hop Support feature, you must:

- Configure the router for IP routing
- Configure Cisco Express Forwarding (formerly known as CEF) switching or distributed Cisco Express Forwarding (formerly known as dCEF) switching on the router and on the interfaces that you want to enable NetFlow on (fast switching is not supported)
- Configure NetFlow v9 (Version 9) data export (if only Version 5 is configured, then BGP next hop data is visible in the caches, but is not exported)
- Configure BGP

Restrictions for NetFlow BGP Next Hop Support

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later releases the **ip flow ingress** command is used to enable NetFlow on an interface.

Recursive Load Sharing

The NetFlow cache does not capture the BGP next hop when the route to that BGP next hop is recursively load-shared via several IGP links. Instead, the NetFlow cache captures (as the BGP next hop) the effective simple next hop from among a random selection of the load-shared routes to which the BGP route recurses.

Memory Impact

For BGP-controlled routes, the NetFlow BGP Next Hop Support feature adds 16 bytes to each NetFlow flow record. This increases memory requirements by 16 bytes times the number of flow cache entries that have BGP-controlled prefixes.

Performance Impact

Because the BGP next hop is fetched from the Cisco Express Forwarding path only once per flow, the performance impact of the NetFlow BGP Next Hop Support feature is minimal.

IPv6 and BGP Next Hop

When connected at Layer 3 using an IPv6 address, BGP installs a link-local next hop and a null BGP next hop in Cisco Express Forwarding. NetFlow uses the IPv6 predefined record "netflow ipv6 bgp-nexhop" or a user-defined record containing the match field "routing next-hop address ipv6 bgp" and matches the link-local next hop and a null BGP next hop with the switching software installed on the router.

Information About NetFlow BGP Next Hop Support

NetFlow BGP Next Hop Support Benefits

Without the NetFlow BGP Next Hop Support feature, NetFlow exports only IP next hop information (which provides information for only the next router). This feature adds BGP next hop information to the data export.

The NetFlow BGP Next Hop Support feature lets you find out through which service provider the traffic is going. This functionality is useful if you have arrangements with several other service providers for fault-protected delivery of traffic. The feature lets you charge customers more per packet when traffic has a more costly destination--you can pass on some of the cost associated with expensive transoceanic links or charge more when traffic is sent to another ISP with which you have an expensive charge agreement.

This feature requires the NetFlow Version 9 export format for its data export.

NetFlow BGP Next Hop Support and NetFlow Aggregation

The Cisco IOS NetFlow Aggregation feature summarizes NetFlow export data on a router before the data is exported to the NetFlow Collection Engine (formerly called the NetFlow FlowCollector). The NetFlow BGP Next Hop Support feature provides the BGP next hop and its related aggregation scheme and provides BGP next hop information within each NetFlow record.

How to Configure NetFlow BGP Next Hop Support

Configuring NetFlow BGP Next Hop Accounting

Perform this task to configure NetFlow BGP next hop accounting for the main cache and aggregation caches. You can enable the export of origin autonomous system (AS) information or peer AS information, but not both.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export version 9** [**origin-as** | **peer-as**] **bgp-nexthop**
4. **ip flow-aggregation cache bgp-nexthop-tos**
5. **enabled**
6. **exit**
7. **interface** *interface-type interface-number*
8. **ip flow** {**ingress** | **egress**}
9. **exit**
10. Repeat Steps 7 through 9 to enable NetFlow on other interfaces.

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	**ip flow-export version 9** [**origin-as** | **peer-as**] **bgp-nexthop** **Example:** `Router(config)# ip flow-export version 9 origin-as bgp-nexthop`	Enables the export of information in NetFlow cache entries. • **version 9--** Specifies that the export packet uses the Version 9 format. • **origin-as** --Includes the origin autonomous system (AS) for the source and destination in the export statistics. • **peer-as--** Includes the peer AS for the source and destination in the export statistics. • **bgp-nexthop** --Includes BGP next hop-related information in the export statistics. This command enables the export of origin AS information and BGP next hop information from the NetFlow main cache. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 4	**ip flow-aggregation cache bgp-nexthop-tos** **Example:** `Router(config)# ip flow-aggregation cache bgp-nexthop-tos`	(Optional) Enables NetFlow aggregation cache schemes and enters aggregation cache configuration mode. • **bgp-nexthop-tos** --Configures the BGP next hop type of service (ToS) aggregation cache scheme.
Step 5	**enabled** **Example:** `Router(config-flow-cache)# enabled`	Enables the aggregation cache.

	Command or Action	Purpose
Step 6	**exit** **Example:** `Router(config)# exit`	Exits aggregation cache configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on an interface.
Step 7	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.
Step 8	**ip flow** {**ingress** | **egress**} **Example:** `Router(config-if)# ip flow ingress`	Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface. • **egress** --Captures traffic that is being transmitted by the interface.
Step 9	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 10	Repeat Steps 7 through 9 to enable NetFlow on other interfaces.	(Optional) --

Troubleshooting Tips

If there are no BGP-specific flow records in the NetFlow cache, make sure that Cisco Express Forwarding or distributed Cisco Express Forwarding switching is enabled and that the destination for NetFlow data export is configured. Check the routing table for BGP routes also.

Verifying the Configuration

Perform this task to verify the configuration of NetFlow BGP next hop accounting.

SUMMARY STEPS

1. **enable**
2. **show ip cache verbose flow**
3. **show ip cache flow aggregation bgp-nexthop-tos**
4. **exit**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if required. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show ip cache verbose flow**

Use this command to verify successful configuration of NetFlow BGP next hop accounting. For example:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (120 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 17826816 bytes
  8 active, 262136 inactive, 8 added
  26 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 1081480 bytes
  8 active, 65528 inactive, 8 added, 8 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk   Active
MUL:M_Opaks  M_Obytes BGP:BGP_NextHop
Et0/0/2        12.0.0.2        Et0/0/4        13.0.0.5        01 00  10   20
0000 /8  0                     0800 /8  0     11.0.0.6             100   0.0
BGP:26.0.0.6
Et0/0/2        12.0.0.2        Et0/0/4        15.0.0.7        01 00  10   20
0000 /8  0                     0800 /8  0     11.0.0.6             100   0.0
BGP:26.0.0.6
Et0/0/2        12.0.0.2        Et0/0/4        15.0.0.7        01 00  10   20
0000 /8  0                     0000 /8  0     11.0.0.6             100   0.0
BGP:26.0.0.6
```

This command displays a detailed summary of NetFlow statistics (including additional NetFlow fields in the header when NetFlow Version 9 data export is configured).

Step 3 **show ip cache flow aggregation bgp-nexthop-tos**

Use this command to verify the configuration of a BGP next hop ToS aggregation cache. For example:

Example:

```
Router# show ip cache flow aggregation bgp-nexthop-tos
IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 1 added
  8 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17224 bytes
  1 active, 1023 inactive, 1 added, 1 added to flow
```

```
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
Src If         Src AS  Dst If         Dst AS  TOS Flows   Pkts  B/Pk
Active
BGP NextHop
Et0/0/2        0       Et0/0/4           0     00    9     36     40
8.2
BGP:26.0.0.6
```

Step 4 **exit**

Return to user EXEC mode. For example:

Example:

```
Router# exit
Router>
```

Configuration Examples for NetFlow BGP Next Hop Support

Example Configuring NetFlow BGP Next Hop Accounting

The following example shows how to configure NetFlow BGP next hop accounting with origin AS and BGP next hop statistics for the main cache:

```
configure terminal
!
ip flow-export version 9 origin-as bgp-nexthop
ip flow-export destination 172.16.10.2 991
!
interface ethernet 0/0
 ip flow ingress
!
end
```

The following example shows how to configure a NetFlow BGP next hop ToS aggregation cache scheme:

```
configure terminal

!

 ip flow-aggregation cache bgp-nexthop-tos
 export destination 172.16.10.2 991
 enabled
!
interface ethernet 0/0
 ip flow ingress
!
 end
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
NetFlow commands	*Cisco IOS NetFlow Command Reference*
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
Configuring NetFlow and NetFlow Data Export	Configuring NetFlow and NetFlow Data Export

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
None	--

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 NetFlow BGP Next Hop Support

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

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

Table 31: Feature Information for NetFlow BGP Next Hop Support

Feature Name	Software	Feature Configuration Information
NetFlow BGP Next Hop Support	12.0(26)S 12.2(18)S 12.2(27)SBC 12.3(1) 15.0(1)S	The NetFlow Border Gateway Protocol (BGP) Next Hop Support feature lets you measure network traffic on a per BGP next hop basis. Without the NetFlow BGP Next Hop Support feature, NetFlow exports only IP next hop information (which provides only the address of the next router). This feature adds BGP next hop information to the data export. The following commands were introduced or modified: **ip flow-aggregation cache**, **ip flow-export**, **show ip cache flow aggregation**, **show ip cache verbose flow**.

Glossary

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). BGP exchanges reachability information with other BGP systems. It is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a specific destination.

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

fast switching --Cisco feature in which a route cache expedites packet switching through a router.

FIB --forwarding information base. A table containing the information needed to forward IP datagrams. At a minimum, this table contains the interface identifier and next hop information for each reachable destination network prefix. The FIB is distinct from the routing table (also called the routing information base), which holds all routing information received from routing peers.

flow --(NetFlow) A set of packets with the same source IP address, destination IP address, source and destination ports, and type of service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

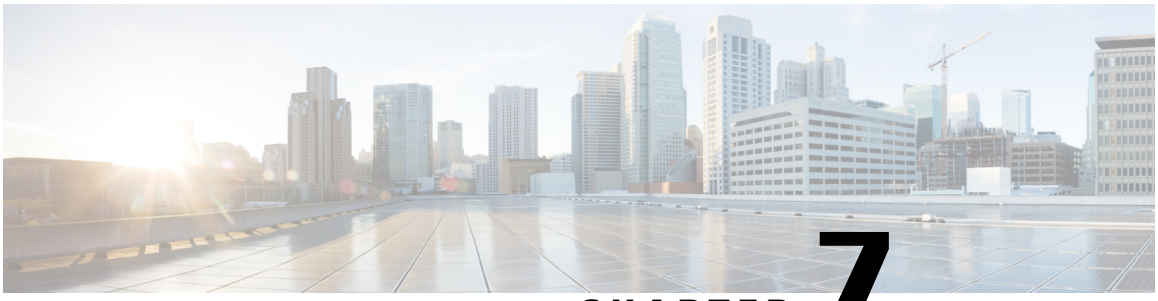
NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

ToS --type of service byte. Second byte in the IP header that indicates the desired quality of service for a particular datagram.



CHAPTER 7

Configuring MPLS Egress NetFlow Accounting and Analysis

This module contains information about and instructions for configuring the MPLS Egress NetFlow Accounting feature. The MPLS Egress NetFlow Accounting feature allows you to capture IP flow information for packets that are undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS packets and that are transmitted as IP packets.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

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 Configuring MPLS Egress NetFlow Accounting

The network must support the following Cisco IOS features before you enable the MPLS Egress NetFlow Accounting feature:

- Multiprotocol label switching (MPLS)

Before you can configure the MPLS Egress NetFlow Accounting feature, you must:

- Configure the router for IP routing
- Configure Cisco Express Forwarding (CEF) switching or distributed CEF (dCEF) switching on the router and on the interfaces that you want to enable MPLS Egress NetFlow Accounting on (fast switching is not supported)

Restrictions for Configuring MPLS Egress NetFlow Accounting

The MPLS Egress NetFlow Accounting feature is not supported in Cisco IOS Release 12.2(25)S and later. Use the Egress NetFlow Accounting feature, which captures either IP or MPLS packets as they leave the router.

Capturing Flows from Sites that Connect to the Same PE Router

The captured egress flows must originate from different sites of the same Virtual Private Network (VPN), and they cannot connect to the same provider edge (PE) router. If both source and destination VPN sites are connected to the PE router, the MPLS egress NetFlow accounting feature does not capture these egress flows. You can capture these flows by enabling ingress NetFlow on the incoming customer edge (CE)-PE link of the PE router. For example, in the figure below, traffic from site 3 (VPN1 destined for site 2) is captured by an ingress NetFlow enabled on the PE2-CE3 link of PE2.

Memory Impact

During times of heavy traffic, the additional flows can fill up the global flow hash table. If you need to increase the size of the global flow hash table, increase the memory of the router.

Performance Impact

MPLS egress NetFlow accounting might adversely affect network performance because of the additional accounting-related computations that occur in the traffic-forwarding path of the router.

Information About Configuring MPLS Egress NetFlow Accounting

MPLS Egress NetFlow Accounting Benefits Enhanced Network Monitoring and More Accurate Accounting Statistics

Enhanced Network Monitoring for Complete Billing Solution

You can now capture flows on the egress and ingress router interfaces and obtain complete end-to-end usage information on network traffic. The accounting server uses the collected data for various levels of aggregation for accounting reports and application programming interface (API) accounting information, thus providing a complete billing solution.

More Accurate Accounting Statistics

NetFlow data statistics provided by the MPLS Egress NetFlow Accounting feature can account for all packets that are dropped in the core of the service provider network, thus providing more accurate traffic statistics and patterns.

MPLS VPN Flow Capture with MPLS Egress NetFlow Accounting

The MPLS Egress NetFlow Accounting feature allows you to capture IP flow information for packets that arrive on a router as MPLS packets and are transmitted as IP packets.

This feature allows you to capture the MPLS Virtual Private Network (VPN) IP flows that are traveling through the service provider backbone from one site of a VPN to another site of the same VPN.

Formerly, you could capture flows only for IP packets on the ingress interface of a router. You could not capture flows for MPLS encapsulated frames, which were switched through CEF from the input port. Therefore, in an MPLS VPN environment, you captured flow information when packets were received from a customer edge (CE) router and forwarded to the backbone. However, you could not capture flow information when packets were transmitted to a CE router because those packets were received as MPLS frames.

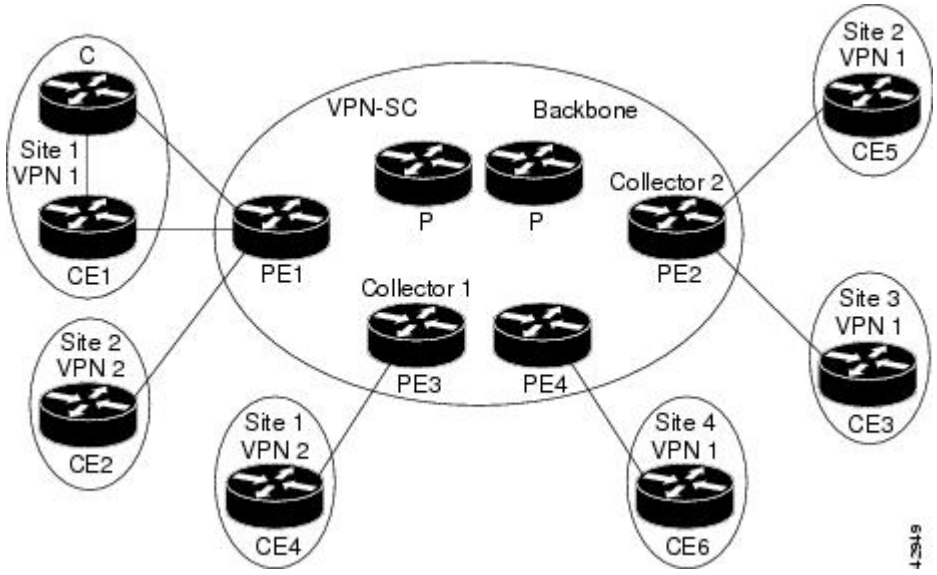
The MPLS Egress NetFlow Accounting feature lets you capture the flows on the outgoing interfaces.

The figure below shows a sample MPLS VPN network topology that includes four VPN 1 sites and two VPN 2 sites. If MPLS egress NetFlow is enabled on an outgoing PE interface, you can capture IP flow information for packets that arrive at the PE as MPLS packets (from an MPLS VPN) and that are transmitted as IP packets. For example,

- To capture the flow of traffic going to site 2 of VPN 1 from any remote VPN 1 sites, you enable MPLS egress NetFlow 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 MPLS egress NetFlow on link PE3-CE4 of the provider edge router PE3.

The flows are stored in a global flow cache maintained by the router. You can use the **show ip cache flow** command or other aggregation flow commands to view the egress flow data.

Figure 23: Sample MPLS VPN Network Topology with MPLS Egress NetFlow Accounting



The PE routers 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 Configure MPLS Egress NetFlow Accounting

Configuring MPLS Egress NetFlow Accounting

Perform the steps in this required task to configure MPLS egress NetFlow accounting.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *interface-type interface-number*
4. **mpls netflow egress**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *interface-type interface-number* **Example:** `Router(config)# interface ethernet 1/4`	(Required) Specifies the interface and enters interface configuration mode.
Step 4	**mpls netflow egress** **Example:** `Router(config-if)# mpls netflow egress`	(Required) Enables the MPLS Egress NetFlow Accounting feature on the egress router interface.
Step 5	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

To display debug messages for MPLS egress NetFlow accounting, use the **debug mpls netflow**command.

Verifying MPLS Egress NetFlow Accounting Configuration

Perform the steps in this optional task to verify that the MPLS Egress NetFlow Accounting configuration is as you expect.

SUMMARY STEPS

1. **show ip cache flow**
2. **show mpls forwarding-table detail**
3. **show mpls interfaces internal**

DETAILED STEPS

Step 1 **show ip cache flow**

Use this command to verify that the MPLS Egress NetFlow Accounting configuration is as you expect. For example:

Example:

```
Router# show ip cache flow
IP packet size distribution (10 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 1.00 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 4456704 bytes
  1 active, 65535 inactive, 2 added
  26 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 1      0.0         5   100      0.0       0.0      15.7
Total :              1      0.0         5   100      0.0       0.0      15.7
SrcIf         SrcIPaddress    DstIf         DstIPaddress  Pr SrcP DstP  Pkts
Et1/1         209.165.200.225 Et1/4         209.165.201.2  01 0000 0800     5
```

Step 2 **show mpls forwarding-table detail**

Use this command to verify the configuration of MPLS egress NetFlow accounting. Check that the quick flag is set for prefixes, which indicates capture by MPLS egress NetFlow accounting. For example:

Example:

```
Router# show mpls forwarding-table detail
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
16     Aggregate   34.0.0.0/8[V]     0
        MAC/Encaps=0/0, MTU=0, Tag Stack{}
        VPN route: vpn1
        Feature Quick flag set
```

Note As shown above, the quick flag is set for the first two prefixes; therefore, traffic destined for those prefixes is captured by MPLS egress NetFlow accounting.

Example:

```
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
17     Untagged    2.0.0.0/8[V]      0          Et0/0/2    34.0.0.1
        MAC/Encaps=0/0, MTU=1500, Tag Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
18     Untagged    42.42.42.42/32[V] 4185       Et0/0/2    34.0.0.1
        MAC/Encaps=0/0, MTU=1500, Tag Stack{}
        VPN route: vpn1
        Feature Quick flag set
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
19     2/33        41.41.41.41/32    0          AT1/0/0.1  point2point
        MAC/Encaps=4/8, MTU=4470, Tag Stack{2/33(vcd=2)}
        00028847 00002000
        No output feature configured
```

Note As shown above, the feature is not configured because MPLS egress NetFlow accounting is not enabled on the outgoing interface for this prefix.

Example:

```
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
20     Aggregate   39.39.39.39/32[V] 0
Local  Outgoing    Prefix            Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id      switched   interface
        MAC/Encaps=0/0, MTU=0, Tag Stack{}
        VPN route: vpn1
        No output feature configured
Per-packet load-sharing, slots: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15
Router#
```

Step 3 **show mpls interfaces internal**

Use this command to show whether or not MPLS egress NetFlow accounting is enabled on the interface. For example:

Example:

```
Router# show mpls interfaces internal
Interface Ethernet0/0/1:
        IP tagging enabled (tdp)
        TSP Tunnel tagging not enabled
        Tag Frame Relay Transport tagging not enabled
        Tagging operational
        IP to Tag Fast Feature Switching Vector
Tag Switching Turbo Feature Vector
        MTU = 1500, status=0x100043, appcount=1
        Output_feature_state=0x0
```

Note The "Output_feature_state=0x0" entry indicates that MPLS egress NetFlow accounting is disabled on interface Ethernet 0/0/1.

Example:

```
Tag VPI = 1, Control VC = 0/32
Interface Ethernet0/0/2:
        IP tagging enabled (tdp)
        TSP Tunnel tagging not enabled
        Tag Frame Relay Transport tagging not enabled
        Tagging operational
        IP to Tag Fast Feature Switching Vector
        Tag Switching Turbo Feature Vector
        MTU = 1500, status=0x100043, appcount=1
        Output_feature_state=0x1
```

Note The "Output_feature_state=0x1" entry indicates that MPLS egress NetFlow accounting is enabled on interface Ethernet 0/0/2.

Example:

```
Tag VPI = 1, Control VC = 0/32
Interface ATM1/0/0.1:
        IP tagging enabled (tdp)
```

Configuration Examples for Configuring MPLS Egress NetFlow Accounting

Enabling MPLS Egress NetFlow Accounting Example

This section contains a sample configuration for the MPLS Egress NetFlow Accounting feature.

The **show ip vrf**command lists the Virtual Private Network (VPN) routing and forwarding instances (VRFs) configured in the router:

```
Router# show ip vrf
  Name                             Default RD          Interfaces
  vpn1                             100:1               Ethernet1/4
                                                       Loopback1
  vpn3                             300:1               Ethernet1/2
                                                       Loopback2
```

In the following example, MPLS Egress NetFlow Accounting is enabled on interface Ethernet 1/4:

```
configure terminal
!
interface ethernet 1/4
 ip address 172.17.24.2 255.255.255.0
 mpls netflow egress
 exit
```

Enter the **show running-config**command to view the current configuration in the router:

```
Router# show running-config
Building configuration...
Current configuration:
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
ip cef
no ip domain-lookup
!
```

This section of the output shows the VRF being defined and shows that the MPLS Egress NetFlow Accounting feature is enabled:

```
ip vrf vpn1
 rd 100:1
 route-target export 100:1
 route-target import 100:1
!
interface Loopback0
 ip address 10.41.41.41 255.255.255.255
 no ip directed-broadcast
 no ip mroute-cache
!
interface Ethernet1/4
 ip vrf forwarding vpn1
 ip address 172.17.24.2 255.255.255.0
 no ip directed-broadcast
 mpls netflow egress
!
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIB	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 1163	*Border Gateway Protocol (BGP)*
RFC 1340	*Assigned Numbers*
RFC 1918	*Address Allocation For Private Internets*
RFC 2547	*BGP/MPLS VPNs*

Technical Assistance

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

Feature Information for Configuring MPLS Egress NetFlow Accounting

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 . An account on Cisco.com is not required.

Table 32: Feature Information for Configuring MPLS Egress NetFlow Accounting

Feature Name	Releases	Feature Configuration Information
MPLS Egress NetFlow Accounting	12.1(5)T 12.0(20)S	The MPLS Egress NetFlow Accounting feature allows you to capture IP flow information for packets that are undergoing MPLS label disposition; that is, packets that arrive on a router as MPLS packets and that are transmitted as IP packets. The following commands were introduced or modified by this feature: **debug mpls netflow**, **mpls netflow egress**, **show mpls forwarding-table**, and **show mpls interface**.

Glossary

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP/MPLS/VPN --A Virtual Private Network (VPN) solution that uses Multiprotocol Label Switching (MPLS) and Border Gateway Protocol (BGP) to allow multiple remote customer sites to be connected over an IP backbone. Refer to RFC 2547 for details.

CE router --A customer edge router. A router that is part of a customer network and interfaces to a provider edge (PE) router.

customer network --A network that is under the control of an end customer. A customer network can use private addresses as defined in RFC 1918. Customer networks are logically isolated from each other and from the provider network. A customer network is also known as a C network.

egress PE --The provider edge router through which traffic moves from the backbone to the destination Virtual Private Network (VPN) site.

flow --A set of packets with the same source IP address, destination IP address, source/destination ports, and type-of-service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

ingress PE --The provider edge router through which traffic enters the backbone (provider network) from a Virtual Private Network (VPN) site.

label --A short, fixed length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

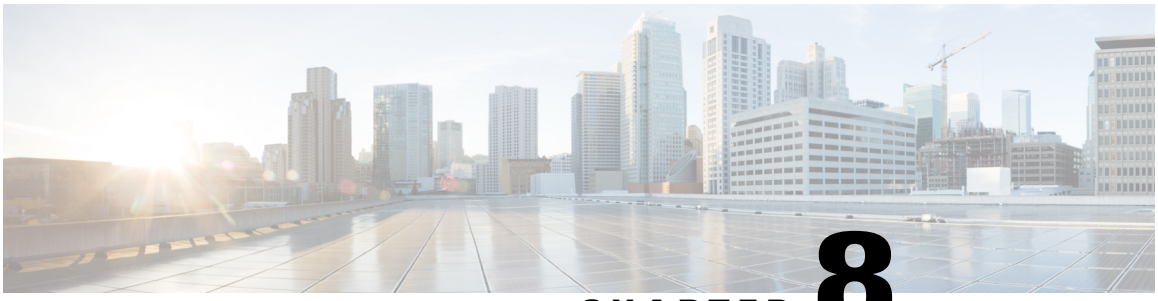
MPLS --Multiprotocol Label Switching. An emerging industry standard for the forwarding of packets along normally routed paths (sometimes called MPLS hop-by-hop forwarding).

PE route r--A provider edge router. A router at the edge of a provider network that interfaces to customer edge (CE) routers.

provider network --A backbone network that is under the control of a service provider and provides transport among customer sites. A provider network is also known as the P network.

VPN --Virtual Private Network. The result of a router configuration that enables IP traffic to use tunneling to travel securely over a public TCP/IP network.

VRF --Virtual Private Network (VPN) routing/forwarding instance. The VRF is a key element in the MPLS VPN technology. VRFs exist on PEs only. A VRF is populated with VPN routes and allows one PE to have multiple routing tables. One VRF is required per VPN on each PE in the VPN.



CHAPTER 8

Configuring MPLS-aware NetFlow

NetFlow is a Cisco NXOS application that provides statistics on packets flowing through the router. This module contains information about and instructions for configuring Multiprotocol Label Switching (MPLS)-aware NetFlow. MPLS-aware NetFlow is an extension of the NetFlow accounting feature that provides highly granular traffic statistics for Cisco routers.

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 Configuring MPLS-aware NetFlow

- Configure NetFlow on the label switch router (LSR).
- Configure MPLS on the LSR.

- Configure Cisco Express Forwarding or distributed CEF enabled on the LSR and the interfaces that you want to enable NetFlow on.

If you are exporting data to a Cisco NetFlow collector, the following requirements apply:

- NetFlow Version 9 export format configured on the LSR
- NetFlow collector and analyzer capable of using MPLS-aware NetFlow export packets in Version 9 format

The table below describes the Cisco 12000 series Internet router line card support for Cisco IOS 12.0 S releases of MPLS-aware NetFlow.

Table 33: Cisco 12000 Series Line Card Support for MPLS-aware NetFlow in Cisco IOS 12.0S Releases

Type	Line Card
Ethernet	1-Port GE[3] 8-Port FE 3-Port GE 1-Port 10-GE Modular GE
Packet over SONET (POS)	4-Port OC-3 POS[4] 1-Port OC-12 POS 1-Port OC-48 POS 4-Port OC-12 POS 4-Port OC-12 POS ISE 1-Port OC-48 POS ISE 4-Port OC-3 POS ISE 8-Port OC-3 POS ISE 16-Port OC-3 POS ISE 1-Port OC-192 POS ES (Edge Release) 4-Port OC-48 POS ES (Edge Release)
Channelized interfaces	1-Port CHOC-12 (DS3) 1-Port CHOC-12 (OC-3) 6-Port Ch T3 (DS1) 2-Port CHOC-3 1-Port CHOC-48 ISE 4-Port CHOC-12 ISE
Electrical interface	6-Port DS3 12-Port DS3 6-Port E3 12-Port E3

Type	Line Card
Dynamic packet transport	1-Port OC-12 DPT 1-Port OC-48 DPT 4-Port OC-48 DPT 1-Port OC-192 DPT
ATM	4-Port OC-3 ATM 1-Port OC-12 ATM 8-Port OC-3 STM-1 ATM

3 This Cisco 12000 series Internet router line card does not support MPLS-aware NetFlow.

4 This Cisco 12000 series Internet router line card supports MPLS-aware NetFlow enabled in either full or sampled mode. Line cards not marked with a footnote character support MPLS-aware NetFlow in sampled mode only. In general, Cisco 12000 line cards support MPLS-aware NetFlow in the same mode as they support NetFlow.

Restrictions for Configuring MPLS-aware NetFlow

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T, the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS Release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later releases, the **ip flow ingress** command is used to enable NetFlow on an interface.

MPLS-aware NetFlow

The following restrictions apply to the MPLS-aware NetFlow feature:

- Three MPLS labels can only be captured and exported.
- MPLS-aware NetFlow reports the following fields in MPLS flows as 0: IP next-hop, source and destination Border Gateway Protocol (BGP) autonomous system numbers, and source and destination prefix masks.
- For MPLS packets that contain non-IP packets under the MPLS label stack, MPLS-aware NetFlow reports the following flow fields as 0: source and destination IP addresses, protocol, ToS, ports, and TCP flags.
- The IP addresses associated with the top label for traffic engineering (TE) tunnel midpoints and Any Transport over MPLS (AToM) are reported as 0.0.0.0.
- The top label type and IP address are obtained at the moment of flow export. Either can be incorrect if the top label was deleted or reassigned after the creation of the flow in the NetFlow cache.
- The following points apply for the Cisco 12000 1-Port 10-GE, Modular GE, 1-Port OC-192 POS ES (Edge Release), and 4-Port OC-48 POS ES (Edge Release) line cards:
    - MPLS-aware NetFlow samples both IP and MPLS packets, but reports only MPLS packets that have one label per packet, ignoring all other packets (that is, IP and MPLS packets with more than one label).

- MPLS-aware NetFlow does not report application (TCP/UDP) port numbers.
- MPLS-aware NetFlow reports experimental bits in MPLS labels as 0.

- The Cisco 12000 1-Port OC-48 POS, 4-Port OC-12 POS, 16-Port OC-3 POS, 3-Port GE, and 1-Port OC-48 DPT line cards support MPLS-aware NetFlow in sampled mode in all microcode bundles that include IP-sampled NetFlow.
- Cisco 7600 series routers do not support the MPLS-aware NetFlow feature.

Information About Configuring MPLS-aware NetFlow

MPLS-aware NetFlow Overview

MPLS-aware NetFlow is an extension of the NetFlow accounting feature that provides highly granular traffic statistics for Cisco routers. MPLS-aware NetFlow collects statistics on a per-flow basis just as NetFlow does.

A flow is a unidirectional set of packets (IP or MPLS) that arrive at the router on the same subinterface, have the same source and destination IP addresses, the same Layer 4 protocol, the same TCP/UDP source and destination ports, and the same type of service byte in the IP header.

An MPLS flow contains up to three of the same incoming MPLS labels of interest with experimental bits and end-of-stack bits in the same positions in the packet label stack. MPLS-aware NetFlow captures MPLS traffic that contains both IP and non-IP packets. It reports non-IP packets, but sets the IP NetFlow fields to 0. It can also be configured to capture and report IP packets, setting to 0 the IP NetFlow fields. MPLS-aware NetFlow uses the NetFlow Version 9 export format. MPLS-aware NetFlow exports up to three labels of interest from the incoming label stack, the IP address associated with the top label, and traditional NetFlow data.

MPLS-aware NetFlow statistics can be used for detailed MPLS traffic studies and analysis that can provide information for a variety of purposes such as MPLS network management, network planning, and enterprise accounting.

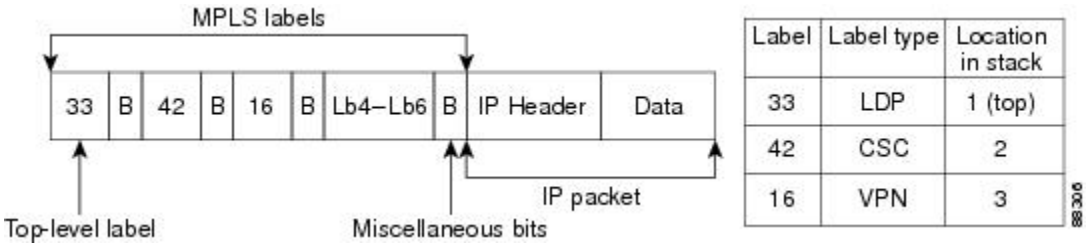
A network administrator can turn on MPLS-aware NetFlow inside an MPLS cloud on a subset of provider backbone (P) routers. These routers can export MPLS-aware NetFlow data to an external NetFlow collection device for further processing and analysis or you can display NetFlow cache data on a router terminal.

MPLS Label Stack

As packets move through an MPLS network, LSRs can add labels to the MPLS label stack. LSRs in an MPLS cloud can add up to six labels to the MPLS label stack. An LSR adds the MPLS labels to the top of the IP

packet. The figure below shows an example of an incoming MPLS label stack that LSRs added to an IP packet as it traversed an MPLS cloud.

Figure 24: Example of an MPLS Label Stack Added to an IP Packet in an MPLS Cloud



In the example of an MPLS label stack in the figure above:

- The 33 represents the top label of this packet.

This label was the last label added to the MPLS label stack and the label that MPLS-aware NetFlow captures if you indicate the label of interest as 1.

- The 42 represents the second label in the MPLS stack.

MPLS-aware NetFlow captures this label if you indicate 2 (second from the top) as a label of interest.

- The 16 represents the third label in the MPLS label stack.

MPLS-aware NetFlow captures this label if you indicate 3 (third from the top) as a label of interest.

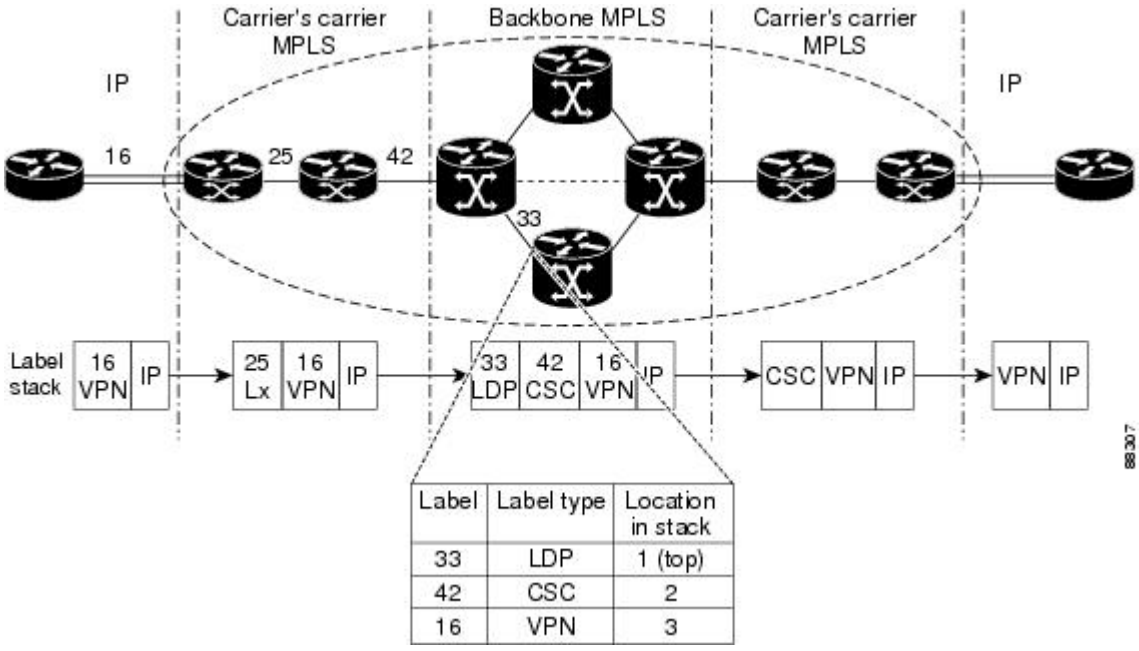
- Lb4-Lb6 represents the fourth to sixth labels in the MPLS stack. LSRs in an MPLS cloud add up to six labels to the MPLS label stack.

MPLS-aware NetFlow captures these labels if you indicate 4, 5, or 6 as labels of interest.

- The B represents miscellaneous bits. These include the following:
  - Exp--Three bits reserved for experimental use
  - S--End-of-stack bits, set to 1 for the last entry in the stack and to 0 for every other entry
  - Time to Live (TTL)--Eight bits used to encode a hop count (or time to live) value

The figure below shows a sample Carrier Supporting Carrier (CSC) topology and the incoming MPLS label stack on multiple LSRs as the packet travels through the network. The figure shows what the stack might look like at a provider core LSR.

Figure 25: Provider and Customer Networks and MPLS Label Imposition



Label	Label type	Location in stack
33	LDP	1 (top)
42	CSC	2
16	VPN	3

In the example in the figure above, a hierarchical VPN is set up between two customer edge (CE) routers.

- Traffic flows from the CE router to a provider edge (PE) router, possibly one belonging to an Internet service provider (ISP). Here, a VPN label (16) is imposed on the inbound IP packet.
- The ISP network eventually connects to an Internet backbone provider where a CSC label (42) is imposed on the label stack.
- As packets traverse the backbone network, a Label Distribution Protocol (LDP) label (33) is imposed on the label stack.

At the inbound interface shown in the figure above, MPLS-aware NetFlow captures the MPLS label stack and reports that the top label (33) is an LDP label, the second label (42) is a CSC label, and the third label (16) is a VPN label.

With NetFlow and MPLS-aware NetFlow enabled on the P router, you can determine the label type for the specified labels, and the IP address associated with the top label on the incoming interface (see the MPLS-aware NetFlow Capture of MPLS Labels, on page 162). Thus, you can track specific types of MPLS traffic, such as TE, LDP, or VPNs.

MPLS-aware NetFlow Capture of MPLS Labels

When you configure the MPLS-aware NetFlow feature, you select the MPLS label positions in the incoming label stack that you are interested in monitoring. You can capture up to three labels from positions 1 to 6 in the MPLS label stack. Label positions are counted from the top of the stack. For example, the position of the

top label is 1, the position of the next label is 2, and so on. You enter the stack location value as an argument to the following command:

```
ip flow-cache mpls label-positions
[label-position-1 [label-position-2 [label-position-3]]]
```

The *label-position-n* argument represents the position of the label on the incoming label stack. For example, the **ip flow-cache mpls label-positions 1 3 4** command configures MPLS-aware NetFlow to capture and export the first (top), third, and fourth labels. If you enter this command and the label stack consists of two MPLS labels, MPLS-aware NetFlow captures only the first (top) label. If some of the labels you requested are not available, they are not captured or reported.

In addition to capturing MPLS labels from the label stack, MPLS-aware NetFlow records the following MPLS label information:

- Type of top label--The type can be any of the following: unknown, TE tunnel midpoint, AToM, VPN, BGP, or LDP.
- The IP address associated with the top label--The route prefix to which the label maps.

Note The IP address for any TE tunnel midpoint or AToM top label is reported as 0.0.0.0.

MPLS-aware NetFlow is enabled globally on the router. However, NetFlow is enabled per interface and must be enabled in either full or sampled mode on the interfaces where you choose to capture and export MPLS and IP NetFlow data.

Note See the table below for information about Cisco 12000 series Internet router line card support for NetFlow (full and sampled modes).

MPLS-aware NetFlow Display of MPLS Labels

The MPLS-aware NetFlow feature allows the display of a snapshot of the NetFlow cache, including MPLS flows, on a terminal through the use of the **show ip cache verbose flow** command. For example, the following output from a provider core router (P router) shows position, value, experimental bits, and end-of-stack bit for each MPLS label of interest. It also shows the type of the top label and the IP address associated with the top label.

```
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
PO3/0          10.1.1.1        PO5/1          10.2.1.1        01 00  10       9
0100 /0  0                     0200 /0  0     0.0.0.0               100     0.0
Pos:Lbl-Exp-S 1:12305-6-0 (LDP/10.10.10.10) 2:12312-6-1
```

In this example from a P router:

- The value of the top label is 12305.
- The experimental bits value is 6 and the end-of-stack bit is 0.
- The label type is LDP and the IP address associated with the label is 10.10.10.10.

- The value of the second label is 12312, the experimental bits value is 6, and the end-of-stack bit is 1.

To fully understand and use the information gathered on the P router, you need information from the Label Forwarding Information Base (LFIB) on the PE router.

Note The MPLS application owner for a label is not reported by MPLS-aware NetFlow for any MPLS label except for the top label. IP information, the label number, and the MPLS application are reported for the top label. Only IP information and the label number are reported for labels other than the top label. Therefore, you need to understand your network if you are interested in identifying the MPLS application owner for labels other than the top MPLS label.

Using MPLS-aware NetFlow, you can monitor various labels in the MPLS label stack. You can also export this information to a NetFlow collector for further processing with a data analyzer and look at MPLS traffic patterns in your network.

Information Captured and Exported by MPLS-aware NetFlow

MPLS-aware NetFlow captures and reports on other information in addition to MPLS labels. It provides per-flow statistics for both incoming IP and MPLS traffic.

- For MPLS traffic, MPLS-aware NetFlow captures and reports up to three labels of interest and the label type and associated IP address of the top label, along with a subset of NetFlow data.
- For IP traffic, MPLS-aware NetFlow provides the regular NetFlow data.
- MPLS-aware NetFlow uses the Version 9 format to export both IP and MPLS NetFlow data.

MPLS-aware NetFlow provides the following traditional NetFlow per-flow statistics:

- Number of packets
- Number of bytes, counting either MPLS payload size only or MPLS payload size plus MPLS label stack size
- Time stamp of the first packet
- Time stamp of the last packet

In addition to these statistics, MPLS-aware NetFlow exports values for the following fields for each flow, using the Version 9 NetFlow export format:

- Regular NetFlow fields:
  - Source IP address
  - Destination IP address
  - Transport layer protocol
  - Source application port number
  - Destination application port number
  - IP ToS
  - TCP flags

- Input interface
- Output interface

Note With the exception of the input interface and output interface fields, these regular NetFlow fields are not included in a flow if the **no-ip-fields** keyword is specified in the **ip flow-cache mpls label-positions** command.

- Additional fields:
  - Up to three incoming MPLS labels with experimental bits and an end-of-stack bit
  - Positions of the MPLS labels in the label stack
  - Type of the top label
  - An address prefix associated with the top label specific to the label type: TE--This is always set to "0.0.0.0" because tunnel label addresses are not supported. LDP--The address prefix is the IP address of the next-hop. VPN--If the VRFs do not have overlapping IP addresses, the address prefix is the destination prefix. If the VRFs have overlapping IP addresses the destination prefix given may be ambiguous.

Note Unlike NetFlow, MPLS-aware NetFlow reports a 0 value for IP next-hop, source, and destination BGP autonomous system numbers, or source and destination prefix masks for MPLS packets.

Note If you are exporting MPLS data to a NetFlow collector or a data analyzer, the collector must support the NetFlow Version 9 flow export format, and you must configure NetFlow export in Version 9 format on the router.

Full and Sampled MPLS-aware NetFlow Support

The table below shows full and sampled MPLS-aware NetFlow support. Information in the table is based on the Cisco IOS release and includes the commands to implement the functionality on a supported platform.

Table 34: Full and Sampled MPLS-aware NetFlow Support

Cisco IOS Release	Full or Sampled NetFlow	Cisco 12000 Series Commands to Implement	Cisco 7500/7200 Series Commands to Implement[5]
12.0(24)S	Sampled	**ip route-cache flow sampled**	--
	Full	--	--

Cisco IOS Release	Full or Sampled NetFlow	Cisco 12000 Series Commands to Implement	Cisco 7500/7200 Series Commands to Implement[5]
12.0(26)S	Sampled	**ip route-cache flow sampled**	**flow-sampler-map** *sampler-map-name* **mode random one-of** *packet-interval* **interface** *type number* **flow-sampler** *sampler-map-name*
	Full	--	**ip route-cache flow**

5 NetFlow sampling on the Cisco 7500 and 7200 platforms is performed by a feature called Random Sampled NetFlow.

How to Configure MPLS-aware NetFlow

Configuring MPLS-aware NetFlow on a Router

Perform the following task to configure MPLS-aware NetFlow on a router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type /number*
4. **ip flow** {**ingress**}
5. **exit**
6. Repeat Steps 3 through 5 for each interface you want to configure NetFlow on.
7. **ip flow-export version 9** [**origin-as** | **peer-as**][**bgp-nexthop**]
8. **ip flow-cache mpls label-positions** [*label-position-1* [*label-position-2* [*label-position-3*]]] [**no-ip-fields**] [**mpls-length**]
9. **exit**

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 pos 3/0`	Specifies the interface and enters interface configuration mode.
Step 4	**ip flow** {**ingress**} **Example:** `Router(config-if)# ip flow ingress`	Enables NetFlow on the interface. • **ingress** --captures traffic that is being received by the interface
Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 for each interface you want to configure NetFlow on.	This step is optional.
Step 7	**ip flow-export version 9** [**origin-as** | **peer-as**][**bgp-nexthop**] **Example:** `Router(config)# ip flow-export version 9 origin-as`	(Optional) Enables the export of information in NetFlow cache entries. • The **version 9** keyword specifies that the export packet uses the Version 9 format. • The **origin-as** keyword specifies that export statistics include the origin autonomous system (AS) for the source and destination. • The **peer-as** keyword specifies that export statistics include the peer AS for the source and destination. • The **bgp-nexthop** keyword specifies that export statistics include BGP next hop-related information. **Caution** Entering this command on a Cisco 12000 series Internet router causes packet forwarding to stop for a few seconds while NetFlow reloads the Route Processor and line card Cisco Express Forwarding tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 8	**ip flow-cache mpls label-positions** [*label-position-1* [*label-position-2*	Enables MPLS-aware NetFlow.

	Command or Action	Purpose

	[*label-position-3*]]] [**no-ip-fields**] [**mpls-length**]
	
	Example:
	
	`Router(config)# ip flow-cache mpls label-positions 1 2 3`
		• The *label-position-n* argument identifies the position of an MPLS label of interest in the incoming label stack. Label positions are counted from the top of the stack, starting with 1.
		• The **no-ip-fields** keyword controls the capture and reporting of MPLS flow fields. If the **no-ip-fields** keyword is specified, the following IP-related flow fields are not included:
		  • Source IP address
		  • Destination IP address
		  • Transport layer protocol
		  • Source application port number
		  • Destination application port number
		  • IP type of service (ToS)
		  • TCP flag (the result of a bitwise OR of TCP)
		
		If the **no-ip-fields** keyword is not specified, the IP-related fields are captured and reported.
		• The **mpls-length** keyword controls the reporting of packet length. If the **mpls-length** keyword is specified, the reported length represents the sum of the MPLS packet payload length and the MPLS label stack length.
		
		If the **mpls-length** keyword is not specified, only the length of the MPLS packet payload is reported.

Step 9	**exit** **Example:** `Router(config)# exit`	Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Sampling for MPLS-aware NetFlow

Perform the following task to configure sampling for MPLS-aware NetFlow.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random one-out-of** *packet-interval*
5. **exit**
6. **interface** *type* / *number*
7. **flow-sampler** *sampler-map-name*
8. **end**

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-sampler-map** *sampler-map-name* **Example:** `Router(config)# flow-sampler-map mysampler`	Defines a named object representing a NetFlow sampler and enters sampler map configuration mode. • The *sampler-map-name* argument is the name of the NetFlow sampler.
Step 4	**mode random one-out-of** *packet-interval* **Example:** `Router(config-sampler-map)# mode random one-out-of 100`	Specifies the sampling mode for the NetFlow sampler. • The **random** keyword specifies the random sampling mode. • The **one-out-of** *packet-interval* keyword argument combination defines the interval selected for random sampling. The packet interval is from 1 to 65535.
Step 5	**exit** **Example:** `Router(config-sampler-map)# exit`	Exits sampler map configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 6	**interface** *type* / *number* **Example:** `Router(config)# interface ethernet 0/0`	Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.
Step 7	**flow-sampler** *sampler-map-name* **Example:** `Router(config-if)# flow-sampler mysampler`	Enables sampled NetFlow accounting on the interface. • The *sampler-map-name* argument is the name of the NetFlow sampler.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

Use the **show-sampler** *sampler-map-name* command to verify the configuration of NetFlow sampling, including the NetFlow sampling mode, sampling mode parameters, and number of packets sampled by the NetFlow sampler.

For more information about NetFlow export sampling, see the Using NetFlow Filtering or Sampling to Select the Network Traffic to Track module.

Verifying the NetFlow Sampler Configuration

Perform the following task to verify the NetFlow sampler configuration on your router:

SUMMARY STEPS

1. **show flow-sampler** [*sampler-map-name*]

DETAILED STEPS

show flow-sampler [*sampler-map-name*]
Use this command to verify the following information about a specific or all NetFlow samplers on the router: sampling mode, sampling parameters (such as packet sampling interval), and number of packets selected by the sampler for NetFlow processing. For example, the following command verifies the configuration for a specific NetFlow sampler:

Example:

```
Router# show flow-sampler mysampler
Sampler : mysampler, id : 1, packets matched : 10, mode : random sampling mode
  sampling interval is : 100
```

The following command verifies the configuration for all NetFlow samplers on the router:

Example:

```
Router# show flow-sampler
Sampler : mysampler, id : 1, packets matched : 10, mode : random sampling mode
  sampling interval is : 100
 Sampler : mysampler1, id : 2, packets matched : 5, mode : random sampling mode
  sampling interval is : 200
```

Displaying MPLS-aware NetFlow Information on a Router

Perform this task to display a snapshot of the MPLS-aware NetFlow cache on a router.

SUMMARY STEPS

1. **enable**
2. • **attach** *slot-number*
   • **if-con** *slot-number*
3. **show ip cache verbose flow**
4. **show ip cache flow**
5. **exit** (Cisco 12000 series routers only)

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if required. For example:

Example:

```
Router> enable
```

Step 2
- **attach** *slot-number*
- **if-con** *slot-number*

Example:

```
Router# attach 3
```

Example:

```
Router# if-con 3
```

Use the **attach** command to access the Cisco IOS software on the line card of a Cisco 12000 series Internet router.

Use the **if-con** command to access the Cisco IOS software on the line card of a Cisco 7500 series router.

Step 3 **show ip cache verbose flow**

Use this command to display IP and MPLS flow records in the NetFlow cache on a Cisco 12000 series Internet router or Cisco 7500 series router. For example:

Example:

```
Router# show ip cache verbose flow
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
PO3/0          10.1.1.1        PO5/1          10.2.1.1        01 00  10       9
0100 /0  0                     0200 /0  0     0.0.0.0               100     0.0
Pos:Lbl-Exp-S 1:12305-6-0 (LDP/10.10.10.10) 2:12312-6-1
```

In this example, the value of the top label is 12305, the experimental bits value is 6, and the end-of-stack bit is 0. The label is LDP and it has an associated IP address of 10.10.10.10. The value of the next from the top label is 12312, the experimental bits value is 6, and the end-of-stack bit is 1. The 1 indicates that this is the last MPLS label in the stack.

Use this command to display IP and MPLS flow records in the NetFlow cache on a Cisco 7200 series router. For example:

Example:

```
Router# show ip cache verbose flow
...
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
PO3/0          10.1.1.1        PO5/1          10.2.1.1        01 00  10       9
0100 /0  0                     0200 /0  0     0.0.0.0               100     0.0
Pos:Lbl-Exp-S 1:12305-6-0 (LDP/10.10.10.10) 2:12312-6-1
```

In this example, the value of the top label is 12305, the experimental bits value is 6, and the end-of-stack bit is 0. The label is LDP and has an associated IP address of 10.10.10.10. The value of the next from the top label is 12312, the experimental bits value is 6, and the end-of-stack bit is 1. The 1 indicates that this is the last MPLS label in the stack.

Step 4 **show ip cache flow**

Use this command to display a summary of the IP and MPLS flow records in the NetFlow cache on a Cisco 12000 series Internet router or Cisco 7500 series router. For example, the following output of the **show ip cache flow** command shows the IP portion of the MPLS flow record in the NetFlow cache:

Example:

```
Router# show ip cache flow
...
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO3/0         10.1.1.1        PO5/1         10.2.1.1        01 0100 0200     9
...
```

Use this command to display a summary of the IP and MPLS flow records in the NetFlow cache on a Cisco 7200 series router. For example:

Example:

```
Router# show ip cache flow
...
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
PO3/0         10.1.1.1        PO5/1         10.2.1.1        01 0100 0200     9
...
```

Step 5 **exit** (Cisco 12000 series routers only)
or

if-quit (Cisco 7500 series routers only)

Use the **exit** command to exit from the line card to privileged EXEC mode of a Cisco 12000 series Internet router. For example:

Example:

```
Router# exit
```

Use the **if-quit** command to exit from the line card to privileged EXEC mode of a Cisco 7500 series router. For example:

Example:

```
Router# if-quit
```

Configuration Examples for MPLS-aware NetFlow

Example Configuring MPLS-aware NetFlow on a Router

The following example shows MPLS-aware NetFlow configured globally and NetFlow enabled on an interface on a Cisco 12000 series P router with Cisco IOS Release 12.0(24)S and later releases:

```
configure terminal
!
interface pos 3/0
 ip address 10.10.10.2 255.255.255.0
 ip route-cache flow sampled
 exit
!
ip flow-export version 9 origin-as
ip flow-sampling-mode packet-interval 101
ip flow-cache mpls label-positions 1 2 3
exit
```

The following examples show MPLS-aware NetFlow configured globally and NetFlow enabled on an interface on a Cisco 7200 or Cisco 7500 series P router with Cisco IOS 12.0S releases:

```
configure terminal
```

```
!
interface pos 3/0
 ip address 10.10.10.2 255.255.255.0
 ip route-cache flow sampled
 exit
!
ip flow-export version 9 origin-as
ip flow-sampling-mode packet-interval 101
ip flow-cache mpls label-positions 1 2 3
exit
```

The following examples show MPLS-aware NetFlow configured globally and NetFlow enabled on an interface on a router with a Cisco IOS Release 12.2(14)S, 12.2(15)T, or 12.0(22)S or later releases:

```
configure terminal
!
interface pos 3/0
 ip address 10.10.10.2 255.255.255.0
 ip flow ingress
 exit
!
ip flow-export version 9 origin-as
ip flow-sampling-mode packet-interval 101
ip flow-cache mpls label-positions 1 2 3
exit
```

To export MPLS-aware NetFlow data from the router, you need to configure the NetFlow Version 9 export format. This example shows the NetFlow Version 9 export format configuration options for MPLS-aware NetFlow and IP NetFlow data export along with an explanation of what each command configures.

Table 35: NetFlow Version 9 Format Configuration Options

`configure terminal` ` ip flow-export version 9 origin-as`	Enters global configuration mode and requests Version 9 flow export, and reports origin-as for IP packets.
` ip flow-export template options sampling`	Specifies the template option sampling configuration.
` ip flow-export template options export-stats`	Reports the number of export packets sent and the number of flows exported.
` ip flow-export template options timeout 5`	Exports template options every 5 minutes.
` ip flow-export template timeout 5`	Resends templates to the collector every 5 minutes.
` ip flow-export destination 10.21.32.25 9996`	Specifies the export destination and UDP port.
` ip flow-export source Loopback0`	Specifies the export source.
` ip flow-sampling-mode packet-interval 101`	Configures the sampling mode packet interval.
`ip flow-cache mpls label-positions 1 2 3`	Configures the MPLS-aware NetFlow feature to report the top three labels.

`interface pos 3/0`
` ip route-cache flow [sampled]`
` end`
	Enables full or sampled IP and MPLS-aware NetFlow on interface POS 3/0 and returns to privileged EXEC mode.
	Note The combination of sampled IP and MPLS-aware NetFlow is supported on the Cisco 12000 series Internet router only.

Example Configuring Sampling for MPLS-aware NetFlow

The following examples show how to define a NetFlow sampler that randomly selects 1 out of 100 packets for NetFlow processing, and how to apply this sampler to an interface on a Cisco 7500 or Cisco 7200 series router.

Defining the NetFlow Sampler

The following example shows how to define a NetFlow sampler called mysampler that randomly selects 1 out of 100 packets for NetFlow processing:

```
configure terminal
!

flow-sampler-map mysampler

 mode random one-out-of 100


 end

exit
```

Applying the NetFlow Sampler to an Interface

The following example shows how to apply the NetFlow sampler named mysampler to an interface:

```
configure terminal
!
interface FastEthernet 2/0
 flow-sampler mysampler
 end
exit
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches

Related Topic	Document Title
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats with NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export with SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and Using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers Using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standard	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified 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

RFCs

RFC	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

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

Feature Information for Configuring MPLS-aware 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 . An account on Cisco.com is not required.

Table 36: Feature Information for Configuring MPLS-aware NetFlow

Feature Name	Releases	Feature Configuration Information
MPLS-aware NetFlow	12.0(24)S, 12.3(8)T	MPLS-aware NetFlow is an extension of the NetFlow accounting feature that provides highly granular traffic statistics for Cisco routers. MPLS-aware NetFlow collects statistics on a per-flow basis just as NetFlow does. MPLS-aware NetFlow uses the NetFlow Version 9 export format. The following commands were introduced or modified: **ip flow-cache mpls label-positions** and **show ip cache verbose flow**.

Glossary

AToM --Any Transport over MPLS. A protocol that provides a common framework for encapsulating and transporting supported Layer 2 traffic types over a Multiprotocol Label Switching (MPLS) network core.

BGP --Border Gateway Protocol. An interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. It is defined by RFC 1163.

CE router --customer edge router. A router that is part of a customer network and that interfaces to a provider edge (PE) router. CE routers do not have routes to associated VPNs in their routing tables.

core router --In a packet-switched star topology, a router that is part of the backbone and that serves as the single pipe through which all traffic from peripheral networks must pass on its way to other peripheral networks.

EGP --Exterior Gateway Protocol. Internet protocol for exchanging routing information between autonomous systems. It is documented in RFC 904. This term is not to be confused with the general term exterior gateway protocol. EGP is an obsolete protocol that was replaced by Border Gateway Protocol (BGP).

export packet --(NetFlow) A packet from a device (for example, a router) with NetFlow services enabled that is addressed to another device (for example, a NetFlow collector). This other device processes the packet (parses, aggregates, and stores information on IP flows).

FEC --Forward Equivalency Class. A set of packets that can be handled equivalently for the purpose of forwarding and thus is suitable for binding to a single label. The set of packets destined for an address prefix is one example of an FEC. A flow is another example.

flow --A unidirectional set of packets (IP or Multiprotocol Label Switching [MPLS]) that arrive at the router on the same subinterface and have the same source and destination IP addresses, the same Layer 4 protocol, the same TCP/UDP source and destination ports, and the same type of service (ToS) byte in the IP header.

IPv6 --IP Version 6. Replacement for the current version of IP (Version 4). IPv6 includes support for flow ID in the packet header, which can be used to identify flows. Formerly called IPng (next generation).

label --A short, fixed-length identifier that tells switching nodes how the data (packets or cells) should be forwarded.

label imposition --The act of putting a label or labels on a packet.

LDP --Label Distribution Protocol. A standard protocol that operates between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets. The Cisco proprietary version of this protocol is the Tag Distribution Protocol (TDP).

LFIB --Label Forwarding Information Base. A data structure and way of managing forwarding in which destinations and incoming labels are associated with outgoing interfaces and labels.

LSR --label switch router. A router that forwards packets in a Multiprotocol Label Switching (MPLS) network by looking only at the fixed-length label.

MPLS --Multiprotocol Label Switching. A switching method in which IP traffic is forwarded through use of a label. This label instructs the routers and the switches in the network where to forward the packets. The forwarding of MPLS packets is based on preestablished IP routing information.

MPLS flow --A unidirectional sequence of Multiprotocol Label Switching (MPLS) packets that arrive at a router on the same subinterface and have the same source and destination IP addresses, the same Layer 4 protocol, the same TCP/UDP source and destination ports, and the same type of service (ToS) byte in the IP header. A TCP session is an example of a flow.

packet header -- (NetFlow) The first part of an export packet that provides basic information about the packet, such as the NetFlow version, number of records contained within the packet, and sequence numbering. The header information enables lost packets to be detected.

PE router --provider edge router. A router that is part of a service provider's network connected to a customer edge (CE) router. All VPN processing occurs in the PE router.

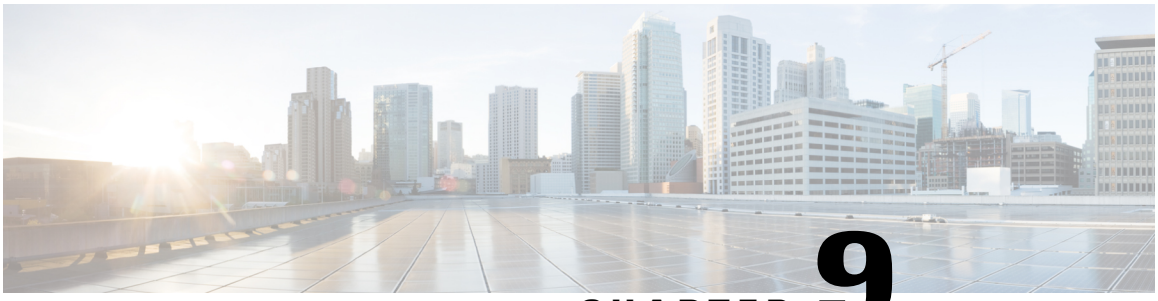
P router --provider core or backbone router. A router that is part of a service provider's core or backbone network and is connected to the provider edge (PE) routers.

TDP --Tag Distribution Protocol. The Cisco proprietary version of the protocol (label distribution protocol) between Multiprotocol Label Switching (MPLS)-enabled routers to negotiate the labels (addresses) used to forward packets.

TE --traffic engineering. Techniques and processes that cause routed traffic to travel through the network on a path other than the one that would have been chosen if standard routing methods were used.

TE tunnel --traffic engineering tunnel. A label-switched tunnel that is used for traffic engineering. Such a tunnel is set up through means other than normal Layer 3 routing; it is used to direct traffic over a path different from the one that Layer 3 routing could cause the tunnel to take.

VPN --Virtual Private Network. A secure IP-based network that shares resources on one or more physical networks. A VPN contains geographically dispersed sites that can communicate securely over a shared backbone.



CHAPTER 9

Configuring NetFlow Multicast Accounting

This document contains information about and instructions for configuring NetFlow multicast accounting. NetFlow multicast accounting allows you to capture multicast-specific data (both packets and bytes) for multicast flows.

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

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 Configuring NetFlow Multicast Accounting

Before you can configure NetFlow multicast accounting, you must:

- Configure the router for IP routing
- Configure Multicast fast switching or multicast distributed fast switching (MDFS); multicast Cisco Express Forwarding (CEF) switching is not supported.
- Configure Multicast routing.
- Configure NetFlow v9 (Version 9) data export (otherwise, multicast data is visible in the cache but is not exported).

Restrictions for Configuring NetFlow Multicast Accounting

Memory Impact

If traffic is heavy, the additional flows might fill the global flow hash table. If you must increase the size of the global flow hash table, you must also add memory to the router.

NetFlow has a maximum cache size of 65,536 flow record entries of 64 bytes each. To deduce the packet-replication factor, multicast accounting adds 16 bytes (for a total of 80 bytes) to each multicast flow record.

Performance Impact

Ingress multicast accounting does not greatly affect performance. Because of the additional accounting-related computation that occurs in the traffic-forwarding path of the router, egress NetFlow multicast accounting might degrade network performance slightly, but it does not limit the functionality of the router.

Multicast Addresses

NetFlow data cannot be exported to multicast addresses.

Information About Configuring NetFlow Multicast Accounting

NetFlow Multicast Benefits

NetFlow multicast allows you to capture multicast-specific data (both packets and bytes) for multicast flows. For example, you can capture the packet-replication factor for a specific flow as well as for each outgoing stream. NetFlow multicast provides complete end-to-end usage information about network traffic for a complete multicast traffic billing solution.

You can use NetFlow multicast accounting to identify and count multicast packets on the ingress side or the egress side (or both sides) of a router. Multicast ingress accounting provides information about the source and how many times the traffic was replicated. Multicast egress accounting monitors the destination of the traffic flow.

NetFlow multicast lets you enable NetFlow statistics to account for all packets that fail the reverse path forwarding (RPF) check and that are dropped in the core of the service provider network. Accounting for RPF-failed packets provides more accurate traffic statistics and patterns.

Multicast Ingress and Multicast Egress Accounting

NetFlow multicast lets you select either multicast ingress accounting, in which a replication factor (equal to the number of output interfaces) indicates the load, or multicast egress accounting, in which all outgoing multicast streams are counted as separate streams, or both multicast ingress and multicast egress accounting.

NetFlow multicast lets you collect information about how much data is leaving the interfaces of the router (egress and multicast ingress accounting) or how much multicast data is received (multicast ingress accounting).

On the ingress side, multicast packets are counted as with unicast packets, but with two additional fields (for number of replicated packets and byte count). With multicast ingress accounting, the destination interface field is set to null, and the IP next hop field is set to 0 for multicast flows.

NetFlow Multicast Flow Records

Multicast ingress accounting creates one flow record that indicates how many times each packet is replicated. Multicast egress accounting creates a unique flow record for each outgoing interface.

How to Configure NetFlow Multicast Accounting

Configuring NetFlow Multicast Accounting in Releases 12.4(12)

Perform the steps in this required task to configure NetFlow multicast accounting.

Before You Begin

You must have already configured IP multicast on the networking devices in your network. See the *Cisco IOS IP Multicast Configuration Guide* , for more information on configuring IP multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast netflow rpf-failure**
5. **ip multicast netflow output-counters**
6. **interface** *type number*
7. **ip flow ingress**
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable**	Enters privileged EXEC mode.

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing`	Enables IP multicast routing. • The **vrf** keyword supports the multicast Virtual Private Network (VPN) routing/forwarding instance (VRF). • The *vrf-name* argument is the name assigned to the VRF. • The **distributed** keyword enables Multicast Distributed Switching (MDS).
Step 4	**ip multicast netflow rpf-failure** **Example:** `Router(config)# ip multicast netflow rpf-failure`	Enables accounting for multicast data that fails the RPF check.
Step 5	**ip multicast netflow output-counters** **Example:** `Router(config)# ip multicast netflow output-counters`	Enables accounting for the number of bytes and packets forwarded.
Step 6	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies the interface and enters interface configuration mode.
Step 7	**ip flow ingress** **Example:** `Router(config-if)# ip flow ingress`	Enables NetFlow ingress accounting.
Step 8	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Configuring NetFlow Multicast Accounting in Cisco IOS Releases Prior to 12.4(12)

Configuring NetFlow Multicast Egress Accounting

Perform the steps in this required task to configure NetFlow multicast egress accounting.

Before You Begin

You must have already configured IP multicast on the networking devices in your network. See the *Cisco IOS IP Multicast Configuration Guide,* for more information on configuring IP multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast netflow rpf-failure**
5. **interface** *type number*
6. **ip multicast netflow egress**
7. **end**

DETAILED STEPS

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

	Command or Action	Purpose
Step 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing` **Example:**	Enables IP multicast routing. • The **vrf** keyword supports the multicast Virtual Private Network (VPN) routing/forwarding instance (VRF). • The *vrf-name* argument is the name assigned to the VRF. • The **distributed** keyword enables Multicast Distributed Switching (MDS).
Step 4	**ip multicast netflow rpf-failure** **Example:** `Router(config)# ip multicast netflow rpf-failure`	Enables accounting for multicast data that fails the RPF check.
Step 5	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies the interface and enters interface configuration mode.
Step 6	**ip multicast netflow egress** **Example:** `Router(config-if)# ip multicast netflow egress`	Enables NetFlow multicast egress accounting.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Configuring NetFlow Multicast Ingress Accounting

Perform the steps in this required task to configure NetFlow multicast ingress accounting.

Multicast ingress NetFlow accounting is enabled by default.

Before You Begin

You must have already configured IP multicast on the networking devices in your network. See the *Cisco IOS IP Multicast Configuration Guide,* for more information on configuring IP multicast.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip multicast-routing** [**vrf** *vrf-name*] [**distributed**]
4. **ip multicast netflow rpf-failure**
5. **interface** *type number*
6. **ip multicast netflow ingress**
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enters privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**ip multicast-routing** [**vrf** *vrf-name*] [**distributed**] **Example:** `Router(config)# ip multicast-routing` **Example:**	Enables IP multicast routing. • The **vrf** keyword supports the multicast VRF. • The *vrf-name* argument is the name assigned to the VRF. • The **distributed** keyword enables Multicast Distributed Switching (MDS).
Step 4	**ip multicast netflow rpf-failure** **Example:** `Router(config)# ip multicast netflow rpf-failure`	Enables accounting for multicast data that fails the RPF check.

	Command or Action	Purpose
Step 5	**interface** *type number* **Example:** `Router(config)# interface fastethernet 0/0`	Specifies the interface and enters interface configuration mode.
Step 6	**ip multicast netflow ingress** **Example:** `Router(config-if)# ip multicast netflow ingress`	Enables NetFlow multicast ingress accounting.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits the current configuration mode and returns to privileged EXEC mode.

Troubleshooting Tips

If there are no multicast flow records in the NetFlow cache, check the multicast switching counters for the existence of process-switched packets (NetFlow exports only fast-switched or MDFS-switched packets). If process-switched packets are present, check the MDFS routing table to help determine potential problems.

Verifying the NetFlow Multicast Accounting Configuration

Perform the steps in this optional task to verify the NetFlow multicast accounting configuration.

SUMMARY STEPS

1. **enable**
2. **show ip cache verbose flow**

DETAILED STEPS

Step 1 **enable**

Use this command to enable privileged EXEC mode. Enter your password if required. For example:

Example:

```
Router> enable
Router#
```

Step 2 **show ip cache verbose flow**

Use this command to verify that NetFlow multicast accounting is configured. Look for the two additional fields related to multicast data, that is, the number of IP multicast output packet and byte counts. For example:

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (5149 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .997 .002 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 14 added
  468 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25800 bytes
  1 active, 1023 inactive, 1 added, 1 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
UDP-other           12      0.0         1    52      0.0       0.1      15.6
Total:              12      0.0         1    52      0.0       0.1      15.6
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
IPM: OPkts    OBytes
Et0/0          10.1.1.1        Null           224.192.16.1    01 55  10    5164
0000 /0  0                     0000 /0  0     0.0.0.0                 20   262.8
IPM:    15K    309K
Et0/0          10.1.1.1        Null           255.255.255.255 11 C0  10       1
0208 /0  0                     0208 /0  0     0.0.0.0                 52     0.0
Router#
```

The Opkts column displays the number of IP multicast (IPM) output packets, the OBytes column displays the number of IPM output bytes, and the DstIPaddress column displays the destination IP address for the IPM output packets.

Configuration Examples for NetFlow Multicast Accounting

Configuring NetFlow Multicast Accounting in Original Releases

The following example shows how to configure multicast NetFlow accounting:

```
configure terminal
 ip multicast-routing
 ip multicast netflow rpf-failure
 ip multicast netflow output-counters
!
interface ethernet 0/0
 ip flow ingress
 end
```

Configuring NetFlow MC Accounting in Releases Prior to 12.2(33)SRB

Configuring NetFlow Multicast Egress Accounting Example

The following example shows how to configure multicast egress NetFlow accounting on the egress Ethernet 0/0 interface:

```
configure terminal
 ip multicast-routing
 ip multicast netflow rpf-failure
!
interface ethernet 0/0
 ip multicast netflow egress
 end
```

Configuring NetFlow Multicast Ingress Accounting Example

The following example shows how to configure multicast ingress NetFlow accounting on the ingress Ethernet 1/0 interface:

```
configure terminal
 ip multicast-routing
 ip multicast netflow rpf-failure
!
interface ethernet 1/0
 ip multicast netflow ingress
 end
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track

Related Topic	Document Title
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBS are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Multicast Accounting

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 . An account on Cisco.com is not required.

Table 37: Feature Information for Configuring NetFlow Multicast Accounting

Feature Name	Releases	Feature Configuration Information
NetFlow Multicast Support	12.3(1), 12.2(18)S, 12.2(27)SBC, 12.2(33)SXF, 12.2(33)SRB	The NetFlow Multicast Support feature lets you capture multicast-specific data (both packets and bytes) for multicast flows. For example, you can capture the packet-replication factor for a specific flow as well as for each outgoing stream. This feature provides complete end-to-end usage information about network traffic for a complete multicast traffic billing solution. The following commands were introduced by this feature: **ip multicast netflow egress**, **ip multicast netflow ingress**, and **ip multicast netflow rpf-failure**.
NetFlow Multicast Support[6]	12.4(11)T, 12.4(12), 12.(33)SRB, 12.2(33)SB, 12.2(33)SXH	The **ip multicast netflow** [**ingress** | **egress**] interface configuration command was replaced by the **ip multicast netflow output-counters** global configuration command.

6 This was a minor modification to the existing NetFlow Multicast Support feature. Minor feature modifications are not included in Feature Navigator.

Glossary

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

egress traffic --Traffic leaving the network.

fast switching --Cisco feature in which a route cache is used for expediting packet switching through a router.

ingress traffic --Traffic entering the network.

multicast data --Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the Destination Address field.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

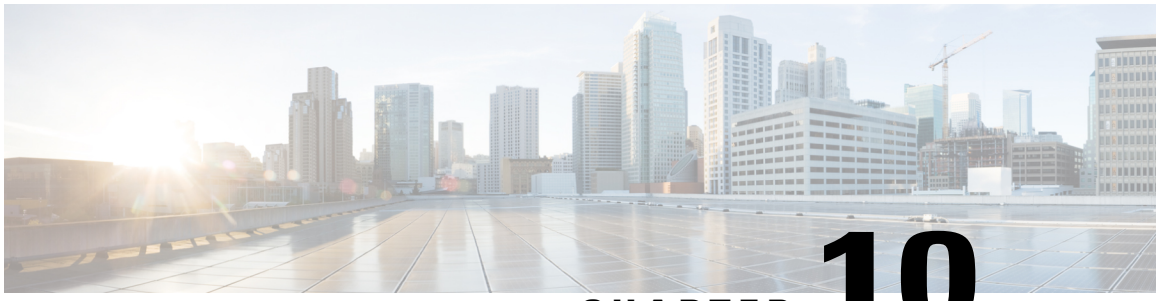
NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly called NetFlow FlowCollector)--A Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

RPF --Reverse Path Forwarding. Multicasting technique in which a multicast datagram is forwarded out of all but the receiving interface if the receiving interface is the one used to forward unicast datagrams to the source of the multicast datagram.

ToS byte --type of service byte. Second byte in the IP header that indicates the desired quality of service (QoS) for a particular datagram.



CHAPTER 10

Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data

NetFlow is a technology that provides highly granular per-flow statistics on traffic in a Cisco router. The NetFlow MIB feature provides MIB objects to allow users to configure NetFlow and to monitor flow cache information, the current NetFlow configuration, and statistics.

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 Configuring SNMP and the NetFlow MIB to Monitor NetFlow Data

Before you enable NetFlow you must:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources
- Configure SNMP on the router on which the NetFlow MIB feature is to be used. Refer to the Configuring the Router to use SNMP, on page 199 for more information. For more information on configuring an SNMP server, refer to the Configuring SNMP Support in the *Cisco IOS Network Management Configuration Guide* .

Restrictions for Configuring SNMP and the NetFlow MIB to Monitor NetFlow Data

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface.

Information About Configuring SNMP and the NetFlow MIB to Monitor NetFlow Data

NetFlow MIB Feature Benefits

NetFlow is a technology that collects traffic flow statistics on routing devices. NetFlow has been used for a variety of applications, including traffic engineering, usage-based billing, and denial of service (DoS) attack monitoring.

The NetFlow MIB feature is useful for obtaining IP flow information from a Cisco router when a NetFlow export operation is not possible. NetFlow exporting does not have to be enabled for the NetFlow MIB feature to be used. The NetFlow MIB feature can be implemented instantaneously at any point in the network to obtain flow information.

With the NetFlow MIB feature, system information that is stored in the flow cache can be accessed in real time by utilizing a MIB implementation based on SNMP. This information is accessed using **get** and **set**

commands entered on the network management system (NMS) workstation for which SNMP has been implemented. The NMS workstation is also known as the SNMP manager.

NetFlow MIB Overview

The Netflow MIB provides a simple and easy method to configure NetFlow, NetFlow aggregation caches, and NetFlow Data Export. You use the snmpget and snmpwalk tools to get NetFlow cache information and current NetFlow configuration information. The NetFlow MIB feature enables medium to small size enterprises to take advantage of NetFlow technology over SNMP at a reduced infrastructure cost. The MIB is created to provide Netflow information in these areas:

- Cache information and configuration.
- Export information and configuration.
- Export Statistics.
- Protocol Statistics.
- Version 9 Export Template information.
- Top Flows information.

Terminology Used

Flow

A flow is defined as an unidirectional sequence of packets between a given source and destination endpoints. Network flows are highly granular; flow endpoints are identified both by IP address as well as by transport layer application port numbers. NetFlow also utilizes the IP Protocol type, Type of Service (ToS) and the input interface identifier to uniquely identify flows.

Exporter

A device (for example, a router) with NetFlow services enabled. The exporter monitors packets entering an observation point and creates flows out of these packets. The information from these flows are exported in the form of Flow Records to the collector. You can configure NetFlow data export using the NetFlow MIB.

Flow Record

A Flow Record provides information about an IP Flow that exists on the Exporter. The Flow Records are commonly referred to as NetFlow Services data or NetFlow data.

Collector

The NetFlow Collector receives Flow Records from one or more Exporters. It processes the received export packet, i.e. parses, stores the Flow Record information. The flow records may be optionally aggregated before storing into the hard disk.

Template

NetFlow Version 9 Export format is template based. Version 9 record format consists of a packet header followed by at least one or more template or data FlowSets. A template FlowSet (collection of one or more

template) provides a description of the fields that will be present in future data FlowSets. 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.

One additional record type is also a part of Version 9 specification: an options template. Rather than supplying information about IP flows, options are used to supply meta-data about the NetFlow process itself.

Top Flows

This feature provides a mechanism which allows the top N flows in the NetFlow cache to be viewed in real time.

Criteria can be set to limit the feature to particular flows of interest, which can aid in DoS detection.

Only the number of flows (TopN) and the sort criteria (SortBy) need be set.

Top Flows is not intended as a mechanism for exporting the entire netflow cache.

For more information on the Top Flows and the NetFlow MIB refer to the Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands.

Egress flows

This feature analyzes traffic that is being forwarded by the router. This feature is often referred to as Egress NetFlow.

Using SNMP and MIBs to Extract NetFlow Information

SNMP has historically been used to collect network information. SNMP permits retrieval of critical information from network elements such as routers, switches, and workstations. The NetFlow MIB feature uses SNMP to configure NetFlow and to gather NetFlow statistics.

The NetFlow MIB feature allows NetFlow statistics and other NetFlow data for the managed devices on your system to be retrieved by SNMP. You can specify retrieval of NetFlow information from a managed device (for example, a router) either by entering commands on that managed device or by entering SNMP commands from the NMS workstation to configure the router via the MIB. If the NetFlow information is configured from the NMS workstation, no access to the router is required and all configuration can be performed via SNMP. The NetFlow MIB request for information is sent from an NMS workstation via SNMP to the router and is retrieved from the router. This information can then be stored or viewed, thus allowing NetFlow information to be easily accessed and transported across a multi-vendor programming environment.

Objects That are Used by the NetFlow MIB

The NetFlow MIB feature defines managed objects that enable a network administrator to remotely monitor the following NetFlow information:

- Flow cache configuration information
- NetFlow export information
- General NetFlow statistics

How to Configure SNMP and use the NetFlow MIB to Monitor NetFlow Data

Note Some of the tasks in this section include examples of the SNMP CLI syntax used to set configuration parameters on the router, and to read values from MIB objects on the router. These SNMP CLI syntax examples are taken from a Linux workstation using public domain SNMP tools. The SNMP CLI syntax for your workstation might be different. Refer to the documentation that was provided with your SNMP tools for the correct syntax for your network management workstation.

Configuring the Router to use SNMP

Before the NetFlow MIB feature can be used, the router must be configured to support SNMP. To enable SNMP on the router, perform this task.

Note The SNMP community read-only (RO) string for the examples is **public**. The SNMP community read-write (RW) string for the examples is **private**. You should use more complex strings for these values in your configurations.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* **ro**
4. **snmp-server community** *string* **rw**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

	Command or Action	Purpose
Step 3	**snmp-server community** *string* **ro** **Example:** `Router(config)# snmp-server community public ro`	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **ro** keyword specifies read-only access. SNMP management stations using this string can retrieve MIB objects.
Step 4	**snmp-server community** *string* **rw** **Example:** `Router(config)# snmp-server community private rw`	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **rw** keyword specifies read-write access. SNMP management stations using this string can retrieve and modify MIB objects. **Note** The *string* argument must be different from the read-only *string* argument specified in the preceding step (Step 3).
Step 5	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Options for the Main Cache

This optional task describes the procedure for modifying the parameters for the NetFlow main cache. Perform the steps in this optional task using either the router CLI commands or the SNMP commands to modify the parameters for the NetFlow main cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-cache entries** *number*
4. **ip flow-cache timeout active** *minutes*
5. **ip flow-cache timeout inactive** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 4000`	(Optional) Specifies the maximum number of entries to be captured for the main flow cache. **Note** The valid range for the *number* argument is from 1024 to 524288 entries.
Step 4	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 30`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the cache. • The **active** *minutes* keyword-argument pair is the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 5	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 100`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the main cache. • The **inactive** *seconds*keyword-argument pair is the number of seconds that an inactive entry will stay in the main cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.
Step 6	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Options for the Main Cache

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.type unsigned** *number*
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.type unsigned** *number*
3. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **ccnfCIInactiveTimeOut.type unsigned** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCICacheEntries.0 unsigned 4000`	(Optional) Defines the maximum number of entries to be captured for the main flow cache. • The value for the *type* argument in **cnfCICacheEntries**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCICacheEntries**.*typenumber* is the maximum number of cache entries. **Note** The valid range for the *number* argument is from 1024 to 524288 entries.
Step 2	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIActiveTimeOut.0 unsigned 60`	(Optional) Specifies the number of seconds that an active flow remains in the main cache before it times out. • The value for the *type* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is the number of seconds that an active flow remains in the cache before it times out. **Note** The range for the *number* argument is from 1 to 60 minutes. The default is 30 minutes.
Step 3	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **ccnfCIInactiveTimeOut.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIInactiveTimeOut.0 unsigned 30`	(Optional) Specifies the number of seconds that an inactive flow remains in the main cache before it times out. • The value for the *type* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is the number of seconds that an inactive flow remains in the main cache before it times out. **Note** The range for the *number* argument is from 10 to 600 seconds. The default is 15 seconds.

Identifying the Interface Number to use for Enabling NetFlow with SNMP

Before you can use SNMP to enable NetFlow on an interface, you must identify the correct SNMP interface number on the router. To identify the interface number for the interface that you want to enable NetFlow on, perform the steps in this task.

SUMMARY STEPS

1. **enable**
2. **show snmp mib ifmib ifindex** *type number*

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode. Enter the password if prompted.

Example:

```
Router> enable
```

Step 2 **show snmp mib ifmib ifindex** *type number*
Displays the SNMP interface number for the interface specified.

Example:

```
Router# show snmp mib ifmib ifindex fastethernet 0/0
Ethernet0/0: Ifindex = 1
```

Configuring NetFlow on an Interface

Perform the task using either the router CLI commands or the SNMP commands to enable NetFlow on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces.
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface fastethernet0/0`	(Required) Specifies the interface that you want to enable NetFlow on and enters interface configuration mode.

Step 4	**ip flow** {**ingress** | **egress**}
	
	Example:
	`Router(config-if)# ip flow ingress`
	
	Example:
	`and/or`
	
	Example:
	`Router(config-if)# ip flow egress`
		(Required) Enables NetFlow on the interface.
		• **ingress** --captures traffic that is being received by the interface
		• **egress** --captures traffic that is being transmitted by the interface.

Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. **Note** You only need to use this command if you want to enable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 to enable NetFlow on other interfaces.	(Optional) --
Step 7	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on an Interface

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] cnfCINetflowEnable.*interface-number* integer [0 | 1 | 2 | 3]
2. Repeat Step 1 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] cnfCINetflowEnable.*interface-number* integer [0 | 1 | 2 | 3] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.1 integer 1`	(Required) Configures NetFlow for an interface. **Note** The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode. The values for the *direction* argument are: • 0--Disable NetFlow • 1--Enable Ingress NetFlow • 2--Enable Egress NetFlow • 3--Enable Ingress and Egress NetFlow
Step 2	Repeat Step 1 to enable NetFlow on other interfaces	(Optional) --

Configuring the Destination-Prefix Aggregation Cache

This task describes the procedure for modifying the parameters for aggregation caches. The **destination-prefix** is used in this task. With the exception of specifying the aggregation cache that you want to modify, the steps are the same for modifying these parameters for the other aggregation caches.

Perform this task using either the router CLI commands or the SNMP commands to modify configuration parameters for an aggregation cache.

Before You Begin

You must enable NetFlow on at least one interface before configuring a NetFlow aggregation cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-aggregation cache destination-prefix**
4. **cache entries** *number*
5. **cache timeout active** *minutes*
6. **cache timeout inactive** *seconds*
7. enable
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-aggregation cache destination-prefix** **Example:** `Router(config)# ip flow-aggregation cache destination-prefix`	(Required) Enters aggregation cache configuration mode for the **destination-prefix**aggregation cache. • The **destination-prefix**keyword is equivalent to the *type* argument of 4 in Step 2 of the SNMP commands. **Note** For information on other keywords for this command, see the *Cisco IOS NetFlow Command Reference* .
Step 4	**cache entries** *number* **Example:** `Router(config-flow-cache)# cache entries 4000`	(Optional) Defines the number of entries that are allowed in the aggregation flow cache.
Step 5	**cache timeout active** *minutes* **Example:** `Router(config)# cache timeout active 30`	(Optional) Specifies the number of minutes that an active flow remains in the cache before it times out. **Note** The range is from 1 to 60 minutes. The default is 30 minutes.

	Command or Action	Purpose

Step 6	**cache timeout inactive** *seconds*
	
	Example:
	
	`Router(config-flow-cache)`
	`# cache timeout inactive 100`
		(Optional) Specifies the number of seconds that an inactive flow remains in the cache before it times out.
		
		Note The range is from 10 to 600 seconds. The default is 15 seconds.

Step 7	enable
	
	Example:
	
	`Router(config-flow-cache)`
	`# enable`
		(Required) Activates the **destination-prefix**aggregation cache.

Step 8	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring the Destination-Prefix Aggregation Cache

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEnable**.*type* **integer** *truth-value*
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.** *type* **unsigned** *number*
3. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.** *type* **unsigned** *number*
4. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **ccnfCIInactiveTimeOut.** *type* **unsigned** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cnfCICacheEnable**.*type* **integer** *truth-value* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCICacheEnable.4 integer 1`	(Required) Enables the aggregation cache. • Values for the *type* argument are: • Main--0 • AS--1 • Protocol Port--2 • Source Prefix--3 • Destination Prefix--4 • prefix--5

	Command or Action	Purpose
		• Destination Only--6 • Source Destination--7 • Full Flow--8 • AS ToS--9 • Protocol Port ToS--10 • Source Prefix ToS--11 • Destination Prefix Tos--12 • Prefix Tos--13 • Prefix Port--14 • BGP Nexthop Tos--15 • Values for *truth-value* in **cnfCICacheEnable**.*type* **integer** *truth-value*are: • 1--enable the aggregation cache • 2--disable the aggregation cache
Step 2	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.** *type* **unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCICacheEntries.4 unsigned 4000`	(Optional) Defines the maximum number of entries to be captured for the aggregation flow cache. • The value for the *type* argument in **cnfCICacheEntries**.*type* **unsigned** *number* is 4 for the **destination-prefix** cache. • The value for the *number* argument in **cnfCICacheEntries**.*type* **unsigned** *number* is the maximum number of cache entries. **Note** The valid range for the *number* argument is from 1024 to 524288 entries.
Step 3	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.** *type* **unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCIActiveTimeOut.4 unsigned 60`	(Optional) Specifies the number of seconds that an active flow remains in the cache before it times out. • The value for the *type* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is 4 for the **destination-prefix** cache. • The value for the *number* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is the number of seconds that an active flow remains in the cache before it times out. **Note** The range for the *number* argument is from 1 to 60 minutes. The default is 30 minutes.
Step 4	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIInactiveTimeOut.** *type* **unsigned** *number*	(Optional) Specifies the number of seconds that an inactive flow remains in the cache before it times out.

	Command or Action	Purpose
	Example: `workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCIInactiveTimeOut.4 unsigned 30`	• The value for the *type* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is 4 for the **destination-prefix** cache. • The value for the *number* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is the number of seconds that an inactive flow remains in the cache before it times out. **Note** The range for the *number* argument is from 10 to 600 seconds. The default is 15 seconds.

Configuring NetFlow Export from the Main NetFlow Cache using the Version 9 Export Format

The following example shows how to configure the router to export statistics from the NetFlow main cache (0), including peer autonomous system and BGP-related information using export Version 9.

Perform this task using either the router CLI commands or the SNMP commands to configure the router to export statistics from the main cache using the Version 9.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]**
4. **ip flow-export destination** {*ip-address* | *hostname*} *udp-port*}
5. Repeat Step 4 to add a second NetFlow collector
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip flow-export version 9 [origin-as | peer-as] [bgp-nexthop]** **Example:** `Router(config)# ip flow-export version 9 peer-as bgp-nexthop`	(Required) Enables the export of information in NetFlow cache entries. • The **version 9** keyword specifies that the export packet uses the Version 9 format. • The **origin-as** keyword specifies that export statistics include the originating AS for the source and destination. • The **peer-as** keyword specifies that export statistics include the peer AS for the source and destination. • The **bgp-nexthop** keyword specifies that export statistics include BGP next hop-related information. **Caution** Entering this command on a Cisco 12000 Series Internet Router causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card CEF tables. To avoid interruption of service to a live network, apply this command during a change window, or include it in the startup-config file to be executed during a router reboot.
Step 4	**ip flow-export destination** {*ip-address* | *hostname*} *udp-port*} **Example:** `Router(config)# ip flow-export destination 10.0.19.2 999`	(Required) Specifies the IP address, or hostname of the NetFlow collector, and the UDP port the NetFlow collector is listening on.
Step 5	Repeat Step 4 to add a second NetFlow collector	(Optional) --
Step 6	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow Export from the Main NetFlow Cache using the Version 9 Export Format

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfEIExportVersion**.*type* **unsigned** *version* **cnfEIPeerAS.** *type* **integer** *truth-value* **cnfEIBgpNextHop**.*type* **integer** *truth-value*
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfEICollectorStatus.** *type* **.** *address-type* **.** *ip-version* **.** *ip-address* **.** *port* **integer** [**4** | **6**]
3. Repeat Step 2 to add another collector

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfEIExportVersion**.*type* **unsigned** *version* **cnfEIPeerAS.** *type* **integer** *truth-value* **cnfEIBgpNextHop**.*type* **integer** *truth-value* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfEIExportVersion.0 unsigned 9 cnfEIPeerAS.0 integer 1 cnfEIBgpNextHop.0 integer 1`	(Required) Specifies the export format and that the export statistics include peer autonomous system and BGP-related information. • The values for the *type* argument are: • Main--0 • AS--1 • Protocol Port--2 • Source Prefix--3 • Destination Prefix--4 • prefix--5 • Destination Only--6 • Source Destination--7 • Full Flow--8 • AS ToS--9 • Protocol Port ToS--10 • Source Prefix ToS--11 • Destination Prefix Tos--12 • Prefix Tos--13 • Prefix Port--14 • BGP Nexthop Tos--15 • The values for the *version* argument are:

	Command or Action	Purpose
		• 5--Version 5 export format. The number of records stored in the datagram is a variable between 1 and 30 for the Version 5 export format. • 9--Version 9 export format. • The values for the *truth-value* argument are: • 1--enable the keyword • 2--disable the keyword
Step 2	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfEICollectorStatus.** *type* **.** *address-type* **.** *ip-version* **.** *ip-address* **.** *port* **integer** [**4** | **6**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfEICollectorStatus.0.1.4.10.0.19.2.3 integer 4`	(Required) Enables the exporting of information in NetFlow cache entries. • Values the *type* argument are: • Main--0 • AS--1 • Protocol Port--2 • Source Prefix--3 • Destination Prefix--4 • prefix--5 • Destination Only--6 • Source Destination--7 • Full Flow--8 • AS ToS--9 • Protocol Port ToS--10 • Source Prefix ToS--11 • Destination Prefix Tos--12 • Prefix Tos--13 • Prefix Port--14 • BGP Nexthop Tos--15 • The *address-type*, and *ip-version* arguments specify the type of IP address. • The *address-type* argument is 1. • The *ip-version* argument is the length in bytes of the address. Currently IPv4 is the only type that is supported, so the ip-version value should be 4 (four bytes in an IPv4 IP address). • The *ip-address* variable specifies the IPv4 IP address of the collector.

	Command or Action	Purpose

		• The *port* argument is the UDP port the collector is listening on for NetFlow data.
		• The [**4** | **6**] keywords create and remove the NetFlow collector.
		  • The 4 keyword creates the collector in the router's configuration, and activates the collector.
		  • The 6 keyword removes the collector from router's configuration.

Step 3	Repeat Step 2 to add another collector	(Optional) --

Configuration Examples using SNMP and the NetFlow MIB to Monitor NetFlow Data

Configuring the Minimum Mask for a Source Prefix Aggregation Scheme using SNMP Example

The following example enables a **Source-Prefix** aggregation cache and sets the source prefix mask to 16 bits.

```
workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCICacheEnable.3 integer 1
CISCO-NETFLOW-MIB::cnfCICacheEnable.sourcePrefix = INTEGER: true(1)
workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCIMinSourceMask.3 unsigned 16
CISCO-NETFLOW-MIB::cnfCIMinSourceMask.sourcePrefix = Gauge32: 16
```

Configuring NetFlow Data Export for the Source Prefix Aggregation Scheme using SNMP Example

The following example enables a **Source-Prefix** aggregation cache and configures NetFlow Data Export for the aggregation cache.

```
workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCICacheEnable.3 integer 1
CISCO-NETFLOW-MIB::cnfCICacheEnable.sourcePrefix = INTEGER: true(1)
workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfEICollectorStatus.3.1.4.10.0.19.2.3
 integer 4
CISCO-NETFLOW-MIB::cnfEICollectorStatus.sourcePrefix.ipv4."....".3 = INTEGER: createAndGo(4)
```

Configuring a NetFlow Minimum Mask for a Prefix Aggregation Cache using SNMP Example

The following example enables a **Prefix** aggregation cache and sets the prefix mask to 16 bits.

```
workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCICacheEnable.5 integer 1
CISCO-NETFLOW-MIB::cnfCICacheEnable.prefix = INTEGER: true(1)
workstation% snmpset -c private -m all -v2c 10.4.9.14 cnfCIMinSourceMask.5
 unsigned 16
CISCO-NETFLOW-MIB::cnfCIMinSourceMask.prefix = Gauge32: 16
```

Using SNMP to Gather Flow Information From the Router Example

The following examples show how to retrieve NetFlow status and statistics using SNMP.

Retrieving Netflow Statistics using SNMP

This command will retrieve the Netflow Statistics from the main cache using the MIB.

```
workstation% snmpget -c public -v2c 10.4.9.14 cnfPSPacketSizeDistribution.0
cnfPSPacketSizeDistribution.0 =
00 00  00 00   03 e8  00 00    00 00  00 00   00 00  00 00
00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00
00 00  00 00   00 00  00 00    00 00  00 00   00 00  00 00
00 00  00 00
```

The IP packet size distribution values are in the same order as shown in the CLI, with each pair of bytes representing a value of 1000 times the respective value in the CLI.

For example, for the packet range 65-96, the byte pair is 0x03e8 which is 1000 times 1. So to obtain the same values as the CLI, divide the value by 1000.

View the NetFlow Main Cache Timeout Values using SNMP

This command will retrieve the cache timeout values from the main cache using the MIB.

```
workstation% snmpget -c public -v2c 10.4.9.14 cnfCIActiveFlows.0 cnfCIInactiveFlows.0
cnfCIActiveTimeOut.0 cnfCIInactiveTimeOut.0
CISCO-NETFLOW-MIB::cnfCIActiveFlows.main = Gauge32: 1
CISCO-NETFLOW-MIB::cnfCIInactiveFlows.main = Gauge32: 3999
CISCO-NETFLOW-MIB::cnfCIActiveTimeOut.main = Gauge32: 60 minutes
CISCO-NETFLOW-MIB::cnfCIInactiveTimeOut.main = Gauge32: 30 seconds
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	"Cisco IOS NetFlow Overview"
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	"Getting Started with Configuring NetFlow and NetFlow Data Export"

Related Topic	Document Title
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	"Configuring NetFlow Aggregation Caches"
Tasks for configuring NetFlow BGP next hop support	"Configuring NetFlow BGP Next Hop Support for Accounting and Analysis"
Tasks for configuring NetFlow multicast support	"Configuring NetFlow Multicast Accounting"
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	"NetFlow Layer 2 and Security Monitoring Exports"
Tasks for configuring the NetFlow MIB and Top Talkers feature	"Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands"
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	"Cisco CNS NetFlow Collection Engine Documentation"

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
• CISCO-NETFLOW-MIB.my	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL (requires CCO login account): http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data

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 . An account on Cisco.com is not required.

Table 38: Feature Information for Configuring the NetFlow Top Talkers Feature using the Cisco IOS CLI or SNMP Commands

Feature Name	Releases	Feature Configuration Information
NetFlow MIB	12.3(7)T, 12.2(25)S 12.2(27)SBC 12.2(33)SRD	The NetFlow MIB feature provides MIB objects to allow users to monitor NetFlow cache information, the current NetFlow configuration, and statistics. The following command was introduced by this feature: **ip flow-cache timeout**.

Glossary

AS --autonomous system. A collection of networks under a common administration sharing a common routing strategy. Autonomous systems are subdivided by areas. An autonomous system must be assigned a unique 16-bit number by the Internet Assigned Numbers Authority (IANA).

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Gateway Protocol (EGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a specific destination.

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

MIB --Management Information Base. Database of network management information that is used and maintained by a network management protocol, such as Simple Network Management Protocol (SNMP) or the Common Management Information Protocol (CMIP). The value of a MIB object can be changed or retrieved using SNMP or CMIP commands, usually through a GUI network management system. MIB objects are organized in a tree structure that includes public (standard) and private (proprietary) branches.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--A Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

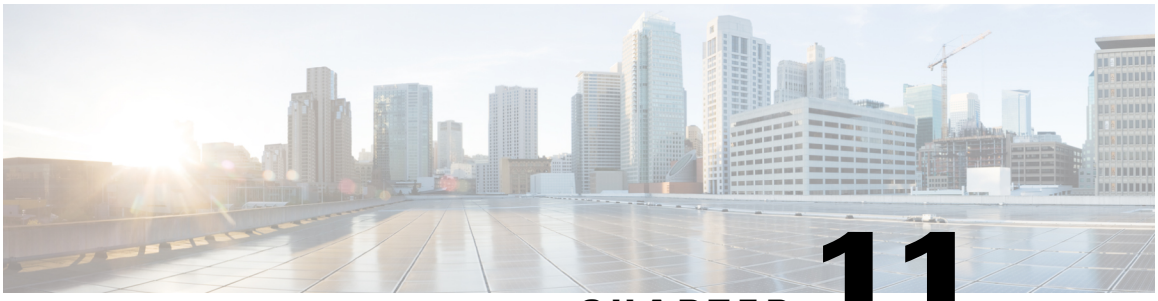
NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means for carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

NMS --network management system. A system responsible for managing at least part of a network. An NMS is generally a reasonably powerful and well-equipped computer, such as an engineering workstation. NMSs communicate with agents to help keep track of network statistics and resources.

SNMP --Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNMP communities --An authentication scheme that enables an intelligent network device to validate SNMP requests.

ToS byte --type of service byte. Second byte in the IP header that indicates the desired quality of service for a particular datagram.



CHAPTER 11

Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands

This module contains information about and instructions for configuring NetFlow Top Talkers feature. The NetFlow Top Talkers feature can be configured using the Cisco IOS command-line interface (CLI) or with SNMP commands using the NetFlow MIB. The NetFlow Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. The NetFlow MIB allows you to configure NetFlow and the NetFlow Top Talkers feature using SNMP commands from a network management workstation.

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 Configuring NetFlow Top Talkers

Before you enable NetFlow and NetFlow Top Talkers, you must:

- Configure the router for IP routing
- Ensure that one of the following is enabled on your router, and on the interfaces that you want to configure NetFlow on: Cisco Express Forwarding (CEF), distributed CEF, or fast switching
- Understand the resources required on your router because NetFlow consumes additional memory and CPU resources.

Restrictions for Configuring NetFlow Top Talkers

Cisco IOS Releases 12.2(14)S, 12.0(22)S, or 12.2(15)T

If your router is running a version of Cisco IOS prior to releases 12.2(14)S, 12.0(22)S, or 12.2(15)T the **ip route-cache flow** command is used to enable NetFlow on an interface.

If your router is running Cisco IOS release 12.2(14)S, 12.0(22)S, 12.2(15)T, or later the **ip flow ingress** command is used to enable NetFlow on an interface.

Cisco IOS Release 12.2(33)SXH

Some of the keywords and arguments for the commands used to configure the NetFlow MIB and Top Talkers feature are not supported in 12.2(33)SXH. See the syntax descriptions for the commands in the command reference (URL for the 12.2SX NF CR to be added later) for details.

Cisco IOS Release

Flexible NetFlow - Top Talker Aggregation is not support in this release.

Information About Configuring NetFlow Top Talkers

Overview of the NetFlow MIB and Top Talkers Feature

NetFlow collects traffic flow statistics on routing devices. NetFlow has been used for a variety of applications, including traffic engineering, usage-based billing, and monitoring for denial-of-service (DoS) attacks.

The flows that are generating the heaviest system traffic are known as the "top talkers."

The NetFlow Top Talkers feature allows flows to be sorted so that they can be viewed. The top talkers can be sorted by either of the following criteria:

- By the total number of packets in each top talker
- By the total number of bytes in each top talker

The usual implementation of NetFlow exports NetFlow data to a collector. The NetFlow MIB and Top Talkers feature performs security monitoring and accounting for top talkers and matches and identifies key users of the network. This feature is also useful for a network location where a traditional NetFlow export operation is not possible. The NetFlow MIB and Top Talkers feature does not require a collector to obtain information regarding flows. Instead, these flows are placed in a special cache where they can be viewed. The NetFlow MIB part of the NetFlow MIB and Top Talkers feature allows you to configure the NetFlow Top Talkers feature using SNMP.

In addition to sorting top talkers, you can further organize your output by specifying criteria that the top talkers must match, such as source or destination IP address or port. The **match** command is used to specify this criterion. For a full list of the matching criteria that you can select, refer to the **match**command in the Cisco IOS command reference documentation.

Benefits of the NetFlow MIB and Top Talkers Feature

Top talkers can be useful for analyzing network traffic in any of the following ways:

- Security--You can view the list of top talkers to see if traffic patterns consistent with DoS attack are present in your network.
- Load balancing--You can identify the most heavily used parts of the system and move network traffic over to less-used parts of the system.
- Traffic analysis--Consulting the data retrieved from the NetFlow MIB and Top Talkers feature can assist you in general traffic study and planning for your network.

An additional benefit of the NetFlow MIB and Top Talkers feature is that it can be configured for a router either by entering CLI commands or by entering SNMP commands on a network management system (NMS) workstation. The SNMP commands are sent to the router and processed by a MIB. You do not have to be connected to the router console to extract the list of top talkers information if an NMS workstation is configured to communicate using SNMP to your network device. For more information on configuring your network device to use MIB functionality for the NetFlow MIB and Top Talkers feature, see Configuring SNMP Support on the Networking Device, on page 222.

Cisco IOS Release 12.2(33)SXH on Cisco 6500 Series Switches

The **show ip flow top-talkers** command was modified in Cisco IOS Release 12.2(33)SXH for the Cisco 6500 Series switches to support displaying the top talkers for a specific module. The **show ip flow top-talkers module** *number* command displays the top talkers for that module. The **show ip flow top-talkers** command without the module keyword shows the top talkers in the hardware switched path (a merged list of top lists from all modules) and then software switched top talkers. The NetFlow MIB can be used to request the top talker list and to set and/or get the configuration parameters for the NetFlow MIB Top Talkers feature.

How to Configure NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands

Note Some of the tasks in this section include examples of the SNMP CLI syntax used to set configuration parameters on the router and to read values from MIB objects on the router. These SNMP CLI syntax examples are taken from a Linux workstation using public-domain SNMP tools. The SNMP CLI syntax for your workstation might be different. Refer to the documentation that was provided with your SNMP tools for the correct syntax for your network management workstation.

Configuring SNMP Support on the Networking Device

If you want to configure the NetFlow Top Talkers feature using the Cisco IOS CLI, you do not have to perform this task.

If you want to configure the NetFlow Top Talkers feature using the NetFlow MIB and SNMP, you must perform this task.

Before you can use SNMP commands to configure the Top Talkers feature you must configure SNMP support on your networking device. To enable SNMP support on the networking device perform the steps in this task.

Note The SNMP community read-only (RO) string for the examples is **public**. The SNMP community read-write (RW) string for the examples is **private**. You should use more complex strings for these values in your configurations.

Note For more information on configuring SNMP support on your networking device, refer to the "Configuring SNMP Support" chapter of the *Cisco IOS Configuration Fundamentals and Network Management Configuration Guide* .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **snmp-server community** *string* **ro**
4. **snmp-server community** *string* **rw**
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**snmp-server community** *string* **ro** **Example:** `Router(config)# snmp-server community public ro`	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **ro** keyword specifies read-only access. SNMP management stations using this string can retrieve MIB objects.
Step 4	**snmp-server community** *string* **rw** **Example:** `Router(config)# snmp-server community private rw`	(Required) Sets up the community access string to permit access to SNMP. • The *string* argument is a community string that consists of from 1 to 32 alphanumeric characters and functions much like a password, permitting access to the SNMP protocol. Blank spaces are not permitted in the community string. • The **rw** keyword specifies read-write access. SNMP management stations using this string can retrieve and modify MIB objects. **Note** The *string* argument must be different from the read-only *string* argument specified in the preceding step (Step 3).
Step 5	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Parameters for the NetFlow Main Cache

This optional task describes the procedure for modifying the parameters for the NetFlow main cache. Perform the steps in this optional task using either the router CLI commands or the SNMP commands to modify the parameters for the NetFlow main cache.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-cache entries** *number*
4. **ip flow-cache timeout active** *minutes*
5. **ip flow-cache timeout inactive** *seconds*
6. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-cache entries** *number* **Example:** `Router(config)# ip flow-cache entries 4000`	(Optional) Specifies the maximum number of entries to be captured for the main flow cache. • The range for the *number* argument is from 1024 to 524288 entries.
Step 4	**ip flow-cache timeout active** *minutes* **Example:** `Router(config)# ip flow-cache timeout active 30`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the cache. • The **active** *minutes* keyword-argument pair is the number of minutes that an entry is active. The range is from 1 to 60 minutes. The default is 30 minutes.
Step 5	**ip flow-cache timeout inactive** *seconds* **Example:** `Router(config)# ip flow-cache timeout inactive 100`	(Optional) Configures operational parameters for the main cache. • The **timeout** keyword dissolves the session in the main cache. • The **inactive** *seconds*keyword-argument pair is the number of seconds that an inactive entry will stay in the main cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

	Command or Action	Purpose
Step 6	**end** **Example:** `Router(config)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Parameters for the NetFlow Main Cache

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCICacheEntries.type unsigned** *number*
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCIActiveTimeOut.type unsigned** *number*
3. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **ccnfCIInactiveTimeOut.type unsigned** *number*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cnfCICacheEntries.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCICacheEntries.0 unsigned 4000`	(Optional) Defines the maximum number of entries to be captured for the main flow cache. • The value for the *type* argument in **cnfCICacheEntries**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCICacheEntries**.*type number* is the maximum number of cache entries. • The range for the *number* argument is from 1024 to 524288 entries.
Step 2	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **cnfCIActiveTimeOut.type unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIActiveTimeOut.0 unsigned 60`	(Optional) Specifies the number of seconds that an active flow remains in the main cache before it times out. • The value for the *type* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIActiveTimeout**.*type* **unsigned** *number* is the number of seconds that an active flow remains in the cache before it times out. • The range for the *number* argument is from 1 to 60 minutes. The default is 30 minutes.
Step 3	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] **ccnfCIInactiveTimeOut.type unsigned** *number*	(Optional) Specifies the number of seconds that an inactive flow remains in the main cache before it times out.

	Command or Action	Purpose
	Example: `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCIInactiveTimeOut.0 unsigned 30`	• The value for the *type* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is 0 for the main cache. • The value for the *number* argument in **cnfCIInactiveTimeout**.*type* **unsigned** *number* is the number of seconds that an inactive flow remains in the main cache before it times out. • The range for the *number* argument is from 10 to 600 seconds. The default is 15 seconds.

Identifying the Interface Number to Use for Enabling NetFlow with SNMP

If you want to configure the NetFlow Top Talkers feature using the Cisco IOS CLI, you do not have to perform this task.

If you want to configure the NetFlow Top Talkers feature using the NetFlow MIB and SNMP, you must perform this task.

Before you can use SNMP to enable NetFlow on an interface, you must identify the SNMP interface number on the router. To identify the interface number for the interface on which you want to enable NetFlow, perform the steps in this required task.

SUMMARY STEPS

1. **enable**
2. **show snmp mib ifmib ifindex** *type number*
3. Repeat Step 2 to identify the SNMP interface number for any other interfaces on which you plan to enable NetFlow.

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode. Enter the password if prompted.

Example:

```
Router> enable
```

Step 2 **show snmp mib ifmib ifindex** *type number*
Displays the SNMP interface number for the interface specified.

Example:

```
Router# show snmp mib ifmib ifindex GigabitEthernet6/2
Ethernet0/0: Ifindex = 60
```

Step 3 Repeat Step 2 to identify the SNMP interface number for any other interfaces on which you plan to enable NetFlow.

Configuring NetFlow on a Cisco 6500 Series Switch

To enable NetFlow on the switch, perform the steps in this required task using either the CLI commands or the SNMP commands.

Note This task provides the minimum information required to configure NetFlow on your Cisco 6500 series switch. See the Catalyst 6500 Series Cisco IOS Software Configuration Guide, for more information of configuring NetFlow on your switch.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}
4. **interface** *type number*
5. **ip flow** {**ingress** | **egress**}
6. **exit**
7. Repeat Steps 4 through 6 to enable NetFlow on other interfaces.
8. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

	Command or Action	Purpose
Step 3	**mls flow** {**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**} **Example:** `Router(config)# mls flow ip interface-full`	Specifies the NetFlow flow mask for IPv4 traffic.
Step 4	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet6/2`	(Required) Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.

Step 5	**ip flow** {**ingress** | **egress**}
	
	Example:
	`Router(config-if)# ip flow ingress`
	
	Example:
	
	Example:
	`and/or`
	
	Example:
	`Router(config-if)# ip flow egress`
		(Required) Enables NetFlow on the interface.
		• **ingress** --Captures traffic that is being received by the interface
		• **egress** --Captures traffic that is being transmitted by the interface.

Step 6	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. • Use this command only if you want to enable NetFlow on another interface.
Step 7	Repeat Steps 4 through 6 to enable NetFlow on other interfaces.	(Optional) --
Step 8	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on a Cisco 6500 Series Switch

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cseFlowIPFlowMask integer** [**1** | **2** | **3** | **4** | **5** | **6**]
2. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCINetflowEnable**.*interface-number* **integer** [**0** | **1** | **2** | **3**]
3. Repeat Step 2 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cseFlowIPFlowMask integer** [**1** | **2** | **3** | **4** | **5** | **6**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1`	Specifies the NetFlow flow mask for IPv4 traffic. • 1--destination-only • 2--source-destination • 3--full-flow • 4--source-only • 5--interface-source-destination • 6--interface-full

Step 2	**snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfCINetflowEnable**.*interface-number* **integer** [**0** | **1** | **2** | **3**]
	
	Example:
	
	`workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1`
		(Required) Configures NetFlow for an interface.
		• The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode.
		• The values for the *direction* argument are:
		  • 0--Disable NetFlow
		  • 1--Enable Ingress NetFlow
		  • 2--Enable Egress NetFlow
		  • 3--Enable Ingress and Egress NetFlow

Step 3	Repeat Step 2 to enable NetFlow on other interfaces	(Optional) --

Configuring NetFlow on Cisco Routers

To enable NetFlow on the router, perform the steps in this required task using either the CLI commands or the SNMP commands .

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip flow** {**ingress** | **egress**}
5. **exit**
6. Repeat Steps 3 through 5 to enable NetFlow on other interfaces.
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**interface** *type number* **Example:** `Router(config)# interface GigabitEthernet6/2`	(Required) Specifies the interface on which you want to enable NetFlow and enters interface configuration mode.
Step 4	**ip flow** {**ingress**	**egress**} **Example:** `Router(config-if)# ip flow ingress` **Example:**	(Required) Enables NetFlow on the interface. • **ingress** --Captures traffic that is being received by the interface • **egress** --Captures traffic that is being transmitted by the interface.

	Command or Action	Purpose

	Example:
	`and/or`
	Example:
	`Router(config-if)# ip flow egress`	

Step 5	**exit** **Example:** `Router(config-if)# exit`	(Optional) Exits interface configuration mode and returns to global configuration mode. • Use this command only if you want to enable NetFlow on another interface.
Step 6	Repeat Steps 3 through 5 to enable NetFlow on other interfaces.	(Optional) --
Step 7	**end** **Example:** `Router(config-if)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow on Cisco Routers

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] cnfCINetflowEnable.*interface-number* **integer** [**0** | **1** | **2** | **3**]
2. Repeat Step 1 to enable NetFlow on other interfaces

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c private -m all -v2c** [*ip-address*	*hostname*] cnfCINetflowEnable.*interface-number* **integer** [**0**	**1**	**2**	**3**] **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1`	(Required) Configures NetFlow for an interface. • The value for the *interface-number* argument is found by entering the router CLI command **show snmp mib ifmib ifindex** on the router in privileged EXEC mode. • The values for the *direction* argument are: • 0--Disable NetFlow

	Command or Action	Purpose
		• 1--Enable Ingress NetFlow • 2--Enable Egress NetFlow • 3--Enable Ingress and Egress NetFlow
Step 2	Repeat Step 1 to enable NetFlow on other interfaces	(Optional) --

Configuring NetFlow Top Talkers

This task describes the procedure for configuring the NetFlow Top Talkers feature. Perform the steps in this required task using either the router CLI commands or the SNMP commands to configure the NetFlow Top Talkers feature on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **top** *number*
5. **sort-by** [**bytes** | **packets**
6. **cache-timeout** *milliseconds*
7. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.

	Command or Action	Purpose
Step 3	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	(Required) Enters NetFlow Top Talkers configuration mode.
Step 4	**top** *number* **Example:** `Router(config-flow-top-talkers)# top 50`	(Required) Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The range for the *number* argument is from 1 to 200 entries.
Step 5	**sort-by** [**bytes** | **packets** **Example:** `Router(config-flow-top-talkers)# sort-by packets`	(Required) Specifies the sort criterion for the top talkers. • The top talkers can be sorted either by the total number of packets of each top talker or the total number of bytes of each top talker.
Step 6	**cache-timeout** *milliseconds* **Example:** `Router(config-flow-top-talkers)# cache-timeout 30000`	(Optional) Specifies the amount of time that the list of top talkers is retained. • Reentering the **top**, **sort-by**, or **cache-timeout** command resets the timeout period, and the list of top talkers is recalculated the next time they are requested. • The list of top talkers is lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers. • If this timeout value is too large, the list of top talkers might not be updated quickly enough to display the latest top talkers. If a request to display the top talkers is made more than once during the timeout period, the same results will be displayed for each request. To ensure that the latest information is displayed while conserving CPU time, configure a large value for the timeout period and change the parameters of the **cache-timeout**, **top**, or **sort-by** command when a new list of top talkers is required. • The range for the *number* argument is from 1 to 3,600,000 milliseconds. The default is 5000 (5 seconds).
Step 7	**end** **Example:** `Router(config-flow-top-talkers)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring NetFlow Top Talkers

SUMMARY STEPS

1. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTopN.0 unsigned** *number*
2. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsSortBy.0 integer** [**1** | **2** | **3**]
3. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsCacheTimeout.0 unsigned** *milliseconds*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTopN.0 unsigned** *number* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsTopN.0 unsigned 50`	(Required) Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The value for the *number* argument in **cnfTopFlowsTopN.0** *number* is the maximum number of top talkers that will be retrieved by a NetFlow top talkers query. • The range for the *number* argument is from 1 to 200 entries.

Step 2	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsSortBy.0 integer** [**1** | **2** | **3**]
	
	Example:
	`workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsSortBy.0 integer 2`
		(Required) Specifies the sort criteria for the top talkers.
		• Values for *sort-option*in **cnfTopFlowsSortBy.0** [**1** | **2** | **3**] are
		  • 1--No sorting will be performed and that the NetFlow MIB and Top Talkers feature will be disabled.
		  • 2--Sorting will be performed by the total number of packets of each top talker.
		  • 3--Sorting will be performed by the total number of bytes of each top talker.

Step 3	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsCacheTimeout.0 unsigned** *milliseconds* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsCacheTimeout.0 unsigned 30000`	(Optional) Specifies the amount of time that the list of top talkers is retained. • Reentering the **top**, **sort-by**, or **cache-timeout** command resets the timeout period, and the list of top talkers is recalculated the next time they are requested. • The list of top talkers will be lost when the timeout period expires. You should configure a timeout period for at least as long as it takes the network management system (NMS) to retrieve all the required NetFlow top talkers. • If this timeout value is too large, the list of top talkers might not be updated quickly enough to display the latest top talkers. If a request to display the top talkers is made more than once during the timeout period, the same results will be displayed for each request. To ensure that the latest

	Command or Action	Purpose
		information is displayed while conserving CPU time, configure a large value for the timeout period and change the parameters of the **cache-timeout**, **top**, or **sort-by** command when a new list of top talkers is required. • The range for the *number* argument is from 1 to 3,600,000 milliseconds. The default is 5000 (5 seconds).

Configuring NetFlow Top Talkers Match Criteria

You can limit the traffic that is displayed by the NetFlow Top Talkers feature by configuring match criteria. The match criteria are applied to data in the main cache. The data in the main cache that meets the match criteria is displayed when you enter the **show ip flow top-talkers** command. To limit the traffic that is displayed by the NetFlow MIB and Top Talkers feature, perform the steps in this optional task.

Before configuring NetFlow MIB and Top Talkers match criteria, you should understand the following:

NetFlow Top Talkers Match Criteria Specified by CLI Commands

You can use the **match** CLI command to specify match criteria to restrict the display of top talkers for the NetFlow MIB and Top Talkers feature. If you do not provide matching criteria, all top talkers are displayed.

Note When configuring a matching source, destination or nexthop address, both the address and a mask must be configured. The configuration will remain unchanged until both have been specified.

Note **cnfTopFlowsMatchSampler** matches flows from a named flow sampler. **cnfTopFlowsMatchClass** matches flows from a named class map.

Note When you are configuring the Top Talkers feature to match bytes and packets, the values that are matched are the total number of bytes and packets in the flow so far. For example, it is possible to match flows containing a specific number of packets, or flows with more or less than a set number of bytes.

For more information on using the match command, see the Cisco IOS NetFlow Command Reference.

NetFlow Top Talkers Match Criteria Specified by SNMP Commands

If you are using SNMP commands to configure NetFlow Top Talkers, see the table below for router CLI commands and equivalent SNMP commands.

Note Some of the SNMP match criteria options, such as the **cnfTopFlowsMatchSrcAddress** option, require that you enter more than one SNMP commands on the same line. For example, **snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal 172.16.10.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24**.

Table 39: Router CLI Commands and Equivalent SNMP Commands

Router CLI Command	SNMP Command
match source address [*ip-address*] [*mask* | */nn*]	**cnfTopFlowsMatchSrcAddress decimal** *ip-address* **cnfTopFlowsMatchSrcAddressType integer** *type* [7] **cnfTopFlowsMatchSrcAddressMask unsigned** *mask*
match destination address [*ip-address*][*mask* | */nn*]	**cnfTopFlowsMatchDstAddress decimal** *ip-address* **cnfTopFlowsMatchDstAddressType integer** *type1* **cnfTopFlowsMatchDstAddressMask unsigned** *mask*
match nexthop address [*ip-address*][*mask* | */nn*]	**cnfTopFlowsMatchNhAddress decimal** *ip-address* **cnfTopFlowsMatchNhAddressType integer** *type1* **cnfTopFlowsMatchNhAddressMask unsigned** *mask*
match source port min *port*	**cnfTopFlowsMatchSrcPortLo integer** *port*
match source port max *port*	**cnfTopFlowsMatchSrcPortHi integer** *port*
match destination port min *port*	**cnfTopFlowsMatchDstPortLo integer** *port*
match destination port max *port*	**cnfTopFlowsMatchDstPortHi integer** *port*
match source as *as-number*	**cnfTopFlowsMatchSrcAS integer** *as-number*
match destination as *as-number*	**cnfTopFlowsMatchDstAS integer** *as-number*
match input-interface *interface*	**cnfTopFlowsMatchInputIf integer** *interface*
match output-interface *interface*	**cnfTopFlowsMatchOutputIf integer** *interface*
match tos [*tos-value* | **dscp** *dscp-value* | **precedence** *precedence-value*]	**cnfTopFlowsMatchTOSByte integer** *tos-value* [8]

Router CLI Command	SNMP Command
match protocol [*protocol-number* | **tcp** | **udp**]	**cnfTopFlowsMatchProtocol integer** *protocol-number*
match flow-sampler *flow-sampler-name*	**cnfTopFlowsMatchSampler string** *flow-sampler-name*
match class-map *class*	**cnfTopFlowsMatchClass string** *class*
match packet-range min *minimum-range*	**cnfTopFlowsMatchMinPackets unsigned** *minimum-range*
match packet-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets unsigned** *maximum-range*
match byte-range min *minimum-range*	**cnfTopFlowsMatchMinBytes unsigned** *minimum-range*
match byte-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets unsigned** *maximum-range*

7 The only IP version type that is currently supported is IPv4 (type 1).

8 tos-value is 6 bits for DSCP, 3 bits for precedence, and 8 bits (one byte) for ToS.

Configuring Source IP Address Top Talkers Match Criteria

Perform the steps in this optional task using either the router CLI commands or the SNMP commands to add source IP address match criteria to the Top Talkers configuration.

For information on configuring other Top Talkers match criteria see the following resources:

- Cisco IOS NetFlow Command Reference.
- CISCO-NETFLOW-MIB at the following URL: http://www.cisco.com/go/mibs/ . Select SNMP Object Locator. Then select View & Download MIBs.

Before You Begin

You must configure NetFlow Top Talkers before you perform this task.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **match source address** {*ip-address/nn* | *ip-address mask*}
5. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	(Required) Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	(Required) Enters global configuration mode.
Step 3	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	(Required) Enters NetFlow Top Talkers configuration mode.
Step 4	**match source address** {*ip-address/nn* | *ip-address mask*} **Example:** `Router(config-flow-top-talkers)# match source address 172.16.10.0 /24`	(Required) Specifies a match criterion. • The **source address** keyword specifies that the match criterion is based on the source IP address. • The *ip-address*argument is the IP address of the source, destination, or next-hop address to be matched. • The *mask* argument is the address mask, in dotted decimal format. • The */nn* argument is the address mask as entered in CIDR format. The **match source address** *172.16.10.0/24* is equivalent to the **match source address** *172.16.10.0 255.255.255.0* command. **Note** You must configure at least one of the possible match criteria before matching can be used to limit the traffic that is displayed by the NetFlow Top Talkers feature. Additional match criteria are optional. **Note** For a full list of the matching criteria that you can select, refer to NetFlow Top Talkers Match Criteria Specified by CLI Commands, on page 235.
Step 5	**end** **Example:** `Router(config-flow-top-talkers)# end`	(Required) Exits the current configuration mode and returns to privileged EXEC mode.

Configuring Source IP Address Top Talkers Match Criteria

SUMMARY STEPS

1. **snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**snmpset -c** *private* **-m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask* **Example:** `workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddressType.0 integer 1 cnfTopFlowsMatchSrcAddress.0 decimal 172.16.10.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24`	(Required) Specifies a match criterion. • The IP address type of 1 in the **cnfTopFlowsMatchSrcAddressType.0 integer 1** command specifies an IP version 4 (IPv4) address for the IP address type. IPv4 is currently the only IP version that is supported. • The *ip-address* argument in **cnfTopFlowsMatchSrcAddress.0 decimal** *ip-address* is the IPv4 source IP address to match in the traffic that is being analyzed. • The *mask* argument in **cnfTopFlowsMatchSrcAddressMask.0 unsigned** *mask* is the number of bits in the mask for the IPv4 source IP address to match in the traffic that is being analyzed. **Note** You must configure at least one of the possible match criteria before matching can be used to limit the traffic that is displayed by the Top talkers feature. Additional match criteria are optional. **Note** To remove the **cnfTopFlowsMatchSrcAddress** match criterion from the configuration, specify an IP address type of 0 (unknown) with the cnfTopFlowsMatchSrcAddressType.0 integer 0 command. **Note** For a list of router CLI commands and their corresponding SNMP commands, see Configuring Source IP Address Top Talkers Match Criteria, on page 239.

Verifying the NetFlow Top Talkers Configuration

To verify the NetFlow Top Talkers configuration, perform the steps in this optional task using either the router CLI command or the SNMP commands.

SUMMARY STEPS

1. **show ip flow top-talkers**

DETAILED STEPS

show ip flow top-talkers
Use this command to verify that the NetFlow MIB and Top Talkers feature is operational. For example:

Example:

```
Router# show ip flow top-talkers
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et3/0         10.1.1.3        Local         10.1.1.2        01 0000 0000  4800
Et3/0         10.1.1.4        Local         10.1.1.2        01 0000 0000  4800
Et3/0         10.1.1.5        Local         10.1.1.2        01 0000 0000   800
3 of 10 top talkers shown. 3 flows processed.
```

Verifying the NetFlow Top Talkers Configuration

In this example, even though a maximum of ten top talkers is configured by the **top** command, only three top talkers were transmitting data in the network. Therefore, three top talkers are shown, and the "3 flows processed" message is displayed in the output. If you expect more top talkers to be displayed than are being shown, this condition may possibly be the result of matching criteria, specified by the **match** command, that are overly restrictive.

SUMMARY STEPS

1. **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsGenerate.0 integer 1**
2. **snmpget -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsReportAvailable**
3. **snmpwalk -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTable**

DETAILED STEPS

Step 1 **snmpset -c private -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsGenerate.0 integer 1**
Use this command to initiate a generation of the top talkers statistics:

Example:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsGenerate.0 integer 1
CISCO-NETFLOW-MIB::cnfTopFlowsGenerate.0 = INTEGER: true(1)
```

Step 2 **snmpget -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsReportAvailable**
Use this command to verify that the top talkers statistics are available:

Example:

```
workstation% snmpwalk -c public -m all -v2c 10.4.9.62 cnfTopFlowsReportAvailable
CISCO-NETFLOW-MIB::cnfTopFlowsReportAvailable.0 = INTEGER: true(1)
```

Step 3 **snmpwalk -c public -m all -v2c** [*ip-address* | *hostname*] **cnfTopFlowsTable**

Use this command to display the NetFlow top talkers:

Example:

```
workstation% snmpwalk -c public -m all -v2c 10.4.9.62 cnfTopFlowsTable
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddress.1 = Hex-STRING: 0A 04 09 08
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAddressMask.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddress.1 = Hex-STRING: 0A 04 09 A7
CISCO-NETFLOW-MIB::cnfTopFlowsDstAddressMask.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsNhAddressType.1 = INTEGER: ipv4(1)
CISCO-NETFLOW-MIB::cnfTopFlowsNhAddress.1 = Hex-STRING: 00 00 00 00
CISCO-NETFLOW-MIB::cnfTopFlowsSrcPort.1 = Gauge32: 32773
CISCO-NETFLOW-MIB::cnfTopFlowsDstPort.1 = Gauge32: 161
CISCO-NETFLOW-MIB::cnfTopFlowsSrcAS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsDstAS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsInputIfIndex.1 = INTEGER: 1
CISCO-NETFLOW-MIB::cnfTopFlowsOutputIfIndex.1 = INTEGER: 0
CISCO-NETFLOW-MIB::cnfTopFlowsFirstSwitched.1 = Timeticks: (12073160) 1 day, 9:32:11.60
CISCO-NETFLOW-MIB::cnfTopFlowsLastSwitched.1 = Timeticks: (12073160) 1 day, 9:32:11.60
CISCO-NETFLOW-MIB::cnfTopFlowsTOS.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsProtocol.1 = Gauge32: 17
CISCO-NETFLOW-MIB::cnfTopFlowsTCPFlags.1 = Gauge32: 16
CISCO-NETFLOW-MIB::cnfTopFlowsSamplerID.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsClassID.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsFlags.1 = Gauge32: 0
CISCO-NETFLOW-MIB::cnfTopFlowsBytes.1 = Gauge32: 75
CISCO-NETFLOW-MIB::cnfTopFlowsPackets.1 = Gauge32: 1
```

Tip You must convert the source and destination IP addresses from hexadecimal to dotted decimal format used in the display output before you can correlate them to source and destination hosts on your network. For example, in the display output above: 0A 04 09 02 = 10.4.9.2 and 0A 04 09 AF = 10.4.9.175.

Configuration Examples for NetFlow Top Talkers

Configuring NetFlow Top Talkers Using SNMP Commands Example

The following output from the network management workstation shows the command and the response for enabling NetFlow on interface GigabitEthernet6/2 (ifindex number 60):

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfCINetflowEnable.60 integer 1
CISCO-NETFLOW-MIB::cnfCINetflowEnable.60 = INTEGER: interfaceDirIngress(1)
```

The following output from the network management workstation shows the command and the response for specifying 5 as the maximum number of top talkers that will be retrieved by a NetFlow top talkers query:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsTopN.0 unsigned 5
CISCO-NETFLOW-MIB::cnfTopFlowsTopN.0 = Gauge32: 5
```

The following output from the network management workstation shows the command and the response for specifying the sort criteria for the top talkers:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsSortBy.0 integer 2
CISCO-NETFLOW-MIB::cnfTopFlowsSortBy.0 = INTEGER: byPackets(2)
```

The following output from the network management workstation shows the command and the response for specifying the amount of time that the list of top talkers is retained:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsCacheTimeout.0 unsigned
2000
CISCO-NETFLOW-MIB::cnfTopFlowsCacheTimeout.0 = Gauge32: 2000 milliseconds
```

Configuring NetFlow Top Talkers Match Criteria Using SNMP Commands Example

The following output from the network management workstation shows the **snmpset** command and the response for specifying the following NetFlow Top Talkers match criteria:

- Source IP address-172.16.23.0
- Source IP address mask-255.255.255.0 (/24)
- IP address type-IPv4

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchSrcAddress.0 decimal
 172.16.23.0 cnfTopFlowsMatchSrcAddressMask.0 unsigned 24 cnfTopFlowsMatchSrcAddressType.0
 integer 1
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddress.0 = Hex-STRING: AC 10 17 00
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddressMask.0 = Gauge32: 24
CISCO-NETFLOW-MIB::cnfTopFlowsMatchSrcAddressType.0 = INTEGER: ipv4(1)
```

The following output from the network management workstation shows the **snmpset** command and the response for specifying the class-map *my-class-map* as aNetFlow Top Talkers match criterion:

```
workstation% snmpset -c private -m all -v2c 10.4.9.62 cnfTopFlowsMatchClass.0 s my-class-map
CISCO-NETFLOW-MIB::cnfTopFlowsMatchClass.0 = STRING: my-class-map.
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis

Related Topic	Document Title
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
CISCO-NETFLOW-MIB	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL (requires CCO login account): http://www.cisco.com/go/mibs

RFCs

RFCs	Title
No new or modified RFCs are supported by this feature, and support for existing RFCs has not been modified by this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands

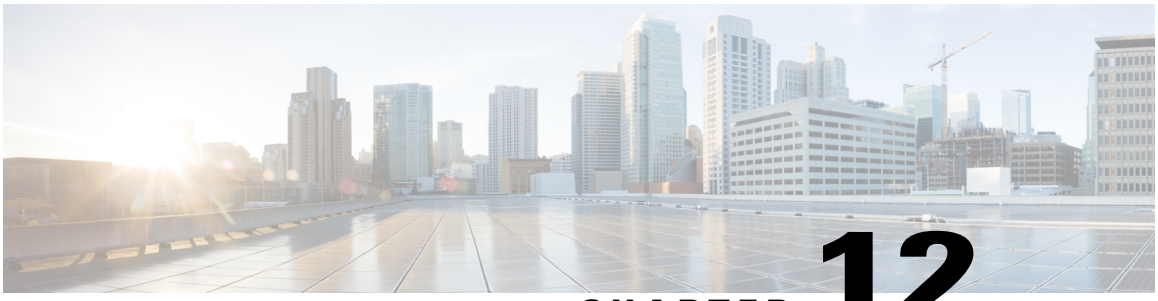
The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train 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 . An account on Cisco.com is not required.

Table 40: Feature Information for Configuring NetFlow Top Talkers using the Cisco IOS CLI or SNMP Commands

Feature Name	Releases	Feature Configuration Information
NetFlow MIB	12.3(7)T, 12.2(25)S 12.2(27)SBC	The NetFlow MIB feature provides MIB objects to allow users to monitor NetFlow cache information, the current NetFlow configuration, and statistics. The following command was introduced by this feature: **ip flow-cache timeout**.

Feature Name	Releases	Feature Configuration Information
NetFlow MIB and Top Talkers	12.3(11)T, 12.2(25)S 12.2(27)SBC 12.2(33)SXH	The NetFlow MIB feature that was originally released in Cisco IOS Release12.3(7)T was modified in Cisco IOS Release 12.3(11)T to support the new NetFlow Top Talkers feature. The modifications to the NetFlow MIB and the new Top Talkers feature were released under the feature name NetFlow MIB and Top Talkers. The NetFlow MIB and Top Talkers feature uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications (top talkers) in the network. The NetFlow MIB component of the NetFlow MIB and Top Talkers feature enables you to configure top talkers and view the top talker statistics using SNMP. The following commands were introduced by this feature: **cache-timeout**, **ip flow-top-talkers**, **match**, **show ip flow top-talkers**, **sort-by**, and **top**.



CHAPTER 12

NetFlow Layer 2 and Security Monitoring Exports

The NetFlow Layer 2 and Security Monitoring Exports feature improves your ability to detect and analyze network threats such as denial of service (DoS) attacks by increasing the number of fields from which NetFlow can capture relevant data.

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 network and security monitoring, network planning, traffic analysis, and IP accounting.

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 NetFlow Layer 2 and Security Monitoring Exports

- Before you configure NetFlow Layer 2 and Security Monitoring Exports, you should understand NetFlow accounting and know how to configure your router to capture IP traffic accounting statistics using NetFlow. See the "Cisco IOS NetFlow Overview" and "Configuring NetFlow and NetFlow Data Export" modules for more details.
- NetFlow and Cisco Express Forwarding (formerly known as CEF), distributed Cisco Express Forwarding (formerly known as dCEF), or fast switching must be configured on your system.
- If you want to export the data captured with the NetFlow Layer 2 and Security Monitoring feature, you must configure NetFlow to use the NetFlow Version 9 data export format.

Information About NetFlow Layer 2 and Security Monitoring Exports

NetFlow Layer 2 and Security Monitoring

The Layer 2 and Layer 3 fields supported by the NetFlow Layer 2 and Security Monitoring Exports feature increase the amount of information that can be obtained by NetFlow about the traffic in your network. You can use the network traffic information for applications such as traffic engineering and usage-based billing.

Layer 3 fields captured by the NetFlow Layer 2 and Security Monitoring Exports feature improve the capabilities of NetFlow for identifying DoS attacks. Layer 2 IP header fields help identify the path that the DoS attack is taking through the network.

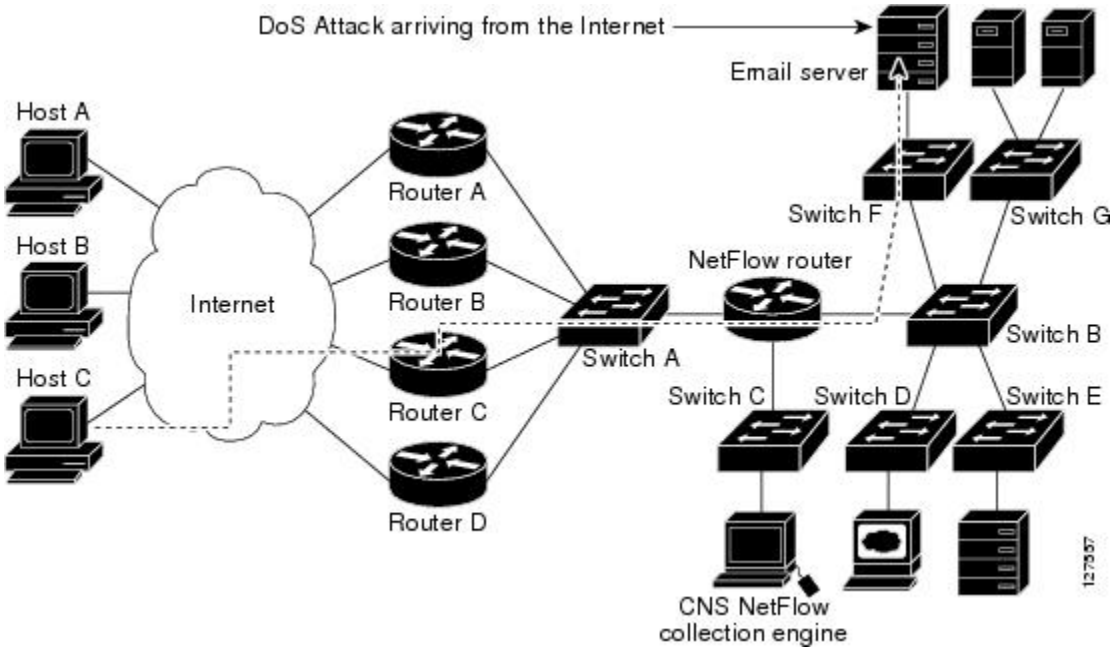
Layer 2 and Layer 3 fields are not key fields. They provide additional information about the traffic in an existing flow. Changes in the values of NetFlow key fields, such as the source IP address, from one packet to the next packet results in the creation of a new flow. For example, if the first packet captured by NetFlow has a source IP address of 10.34.0.2 and the second packet captured has a source IP address of 172.16.213.65, NetFlow will create two separate flows.

Most DoS attacks consist of an attacker sending the same type of IP datagram repeatedly, in an attempt to overwhelm target systems. In such cases, the incoming traffic often has similar characteristics, such as the same values in each datagram for one or more fields that the NetFlow Layer 2 and Security Monitoring Exports feature can capture.

The originator of DoS attacks cannot be easily identified because the IP source address of the device sending the traffic is usually forged. However, you can easily trace the traffic back through the network to the router on which it is arriving by using the NetFlow Layer 2 and Security Monitoring Exports feature to capture the MAC address and VLAN-ID fields. If the router on which traffic is arriving supports NetFlow, you can

configure the NetFlow Layer 2 and Security Monitoring Exports feature on it to identify the interface on which the traffic is arriving. The figure below shows an example of an attack in progress.

Figure 26: DoS Attack Arriving over the Internet



Note You can analyze the data captured by NetFlow directly from the router by using the **show ip cache verbose flow** command or by the Cisco Network Services (CNS) NetFlow Collector Engine.

Once you have concluded that a DoS attack is taking place by analyzing the Layer 3 fields in the NetFlow flows, you can analyze the Layer 2 fields in the flows to discover the path that the DoS attack is taking through the network.

An analysis of the data captured by the NetFlow Layer 2 and Security Monitoring Exports feature, for the scenario shown in the above figure, indicates that the DoS attack is arriving on Router C, because the upstream MAC address is from the interface that connects Router C to Switch A. It is also evident that there are no routers between the target host (the e-mail server) and the NetFlow router, because the destination MAC address of the DoS traffic that the NetFlow router is forwarding to the e-mail server is the MAC address of the e-mail server.

You can learn the MAC address that Host C is using to send traffic to Router C by configuring the NetFlow Layer 2 and Security Monitoring Exports feature on Router C. The source MAC address will be from Host C. The destination MAC address will be for the interface on the NetFlow router.

Once you know the MAC address that Host C is using and the interface on Router C on which Host C's DoS attack is arriving, you can mitigate the attack by reconfiguring Router C to block Host C's traffic. If Host C is on a dedicated interface, you can disable the interface. If Host C is using an interface that carries traffic from other users, you must configure your firewall to block Host C's traffic, but still allow the traffic from the other users to flow through Router C.

Layer 2 Information Capture Using NetFlow Layer 2 and Security Monitoring Exports

The NetFlow Layer 2 and Security Monitoring Exports feature can capture the values of the MAC address and VLAN ID fields from flows. The two supported VLAN types are 802.1q and the Cisco Inter-Switch Link (ISL) protocol.

Layer 2 MAC Address Fields

The Layer 2 fields for which the NetFlow Layer 2 and Security Monitoring Exports feature captures the values are as follows:

- The source MAC address field from frames that are received by the NetFlow router.
- The destination MAC address field from frames that are transmitted by the NetFlow router.
- The VLAN ID field from frames that are received by the NetFlow router.
- The VLAN ID field from frames that are transmitted by the NetFlow router.

Figure 2 shows the Ethernet Type II and Ethernet 802.3 frame formats. The destination address field and the source address field in the frame formats are the MAC address values that are captured by NetFlow.

Figure 27: Ethernet Type II and 802.3 Frame Formats

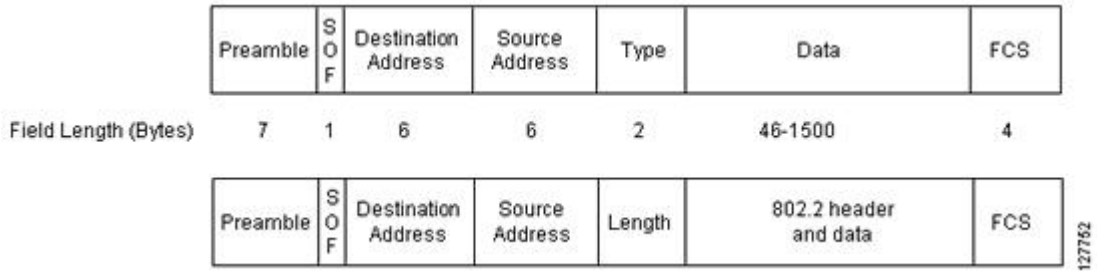


Table 1 explains the fields for the Ethernet frame formats.

Table 41: Ethernet Type II and 802.3 Frame Fields

Field	Description
Preamble	The entry in the Preamble field is an alternating pattern of 0s and 1s that communicates to receiving stations about an incoming frame. It also provides a means for the receiving stations to synchronize their clocks with the incoming bit stream.
SOF (Start of frame)	The SOF field holds an alternating pattern of 0s and 1s, ending with two consecutive 1s, indicating that the next bit is the first bit of the first byte of the destination MAC address.

Field	Description
Destination Address	The 48-bit destination address identifies which station on the LAN should receive the frame. The first two bits of the destination MAC address are reserved for the following special functions: • The first bit in the destination address field indicates whether the address is an individual address (0) or a group address (1). • The second bit indicates whether the destination address is globally administered (0) or locally administered (1). The remaining 46 bits form a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network.
Source Address	The 48-bit source address identifies which station transmitted the frame. The source address is always an individual address, and the leftmost bit in the Source Address field is always 0.
Type or Length	Type—In an Ethernet Type II frame, a part of the frame is used for the Type field. The Type field is used to identify the next layer protocol in the frame. Length—In an 802.3 Ethernet frame, a part of the frame is used for the Length field. The Length field is used to indicate the length of the Ethernet frame. The value can be from 46 to 1500 bytes.
Data or 802.2 header and data	Ethernet Type II—46 to 1500 bytes of data or 802.3/802.2—8 bytes of header and 38 to 1492 bytes of data.
FCS (Frame Check Sequence)	This field contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending station and is recalculated by the receiving station, to check for damaged frames. The FCS is generated for the destination address, source address, Type, and Data fields of the frame. The FCS does not include the data portion of the frame.

Layer 2 VLAN ID Fields

NetFlow can capture the value in the VLAN ID field for 802.1q tagged VLANs and Cisco ISL encapsulated VLANs. This section describes the two types of VLANs, 802.1q and ISL.

Note ISL and 802.1q are commonly called VLAN encapsulation protocols.

Understanding 802.1q VLANs

Devices that use 802.1q insert a four-byte tag into the original frame before it is transmitted. Figure 3 shows the format of an 802.1q tagged Ethernet frame.

Figure 28: 802.1q Tagged Ethernet Type II or 802.3 Frame

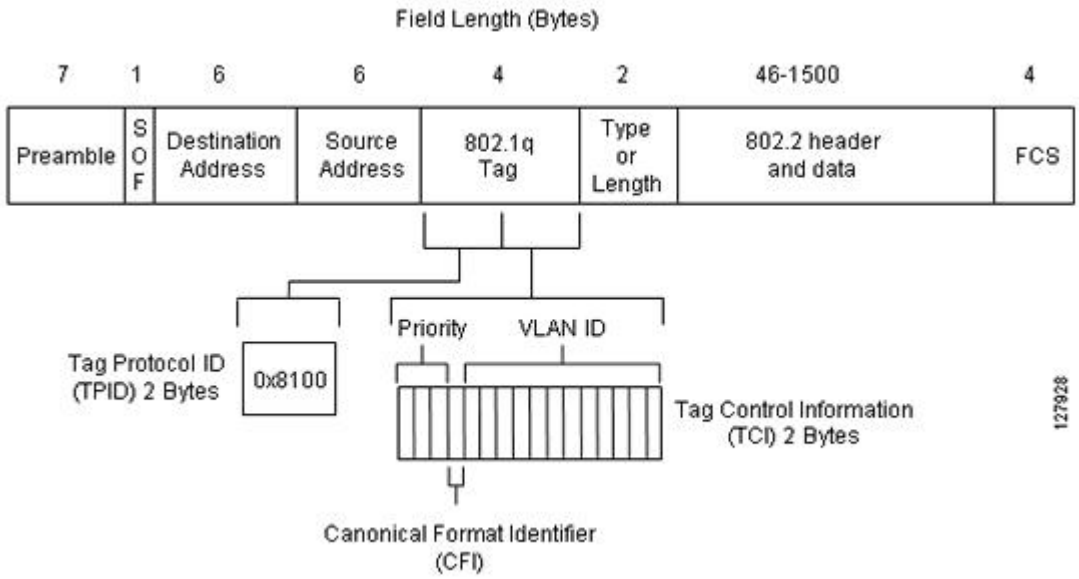


Table 2 describes the fields for 802.1q VLANs.

Table 42: 802.1q VLAN Encapsulation Fields

Field	Description
Destination Address	The 48-bit destination address identifies which stations on the LAN should receive the frame. The first two bits of the destination MAC address are reserved for the following special functions: • The first bit in the destination address field indicates whether the address is an individual address (0) or a group address (1). • The second bit indicates whether the destination address is globally administered (0) or locally administered (1). The remaining 46 bits form a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network.
Source Address	The 48-bit source address identifies which station transmitted the frame. The source address is always an individual address, and the leftmost bit in the Source Address field is always 0.

Field	Description
Type or Length	Type—In an Ethernet Type II frame, a part of the frame is used for the Type field. The Type field is used to identify the next layer protocol in the frame. Length—In an 802.3 Ethernet frame, a part of the frame is used for the Length field. The Length field is used to indicate the length of the Ethernet frame. The value can be from 46 to 1500 bytes.
Data or 802.2 header and data	Ethernet Type II—46 to 1500 bytes of data or 802.3/802.2—8 bytes of header and 38 to 1492 bytes of data.
FCS (Frame Check Sequence)	This field contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending station and is recalculated by the receiving station, to check for damaged frames. The FCS is generated for the destination address, source address, Type, and Data fields of the frame. The FCS does not include the data portion of the frame.
Tag Protocol ID (TPID)	This 16-bit field is set to a value of 0x8100 to identify the frame as an IEEE 802.1q tagged frame.
Priority	This 3-bit field refers to the 802.1p priority. It is also known as user priority. It indicates the frame priority level used for prioritizing traffic and can represent levels 0–7.
Tag Control Information	This 2-byte Tag Control Information field consists of the following two subfields: • Canonical Format Indentifier (CFI)—If the value of this 1-bit field is 1, the MAC address is in noncanonical format. If the value of this field is 0, the MAC address is in canonical format. • VLAN ID—This 12-bit field uniquely identifies the VLAN to which the frame belongs. It can have a value from 0 to 4095.

Cisco ISL VLANs

ISL is a Cisco-proprietary protocol for encapsulating frames on a VLAN trunk. Devices that use ISL add an ISL header to the frame. This process is known as VLAN encapsulation. 802.1Q is the IEEE standard for tagging frames on a VLAN trunk. Figure 4 shows the format of a Cisco ISL-encapsulated Ethernet frame.

Figure 29: Cisco ISL Tagged Ethernet Frame

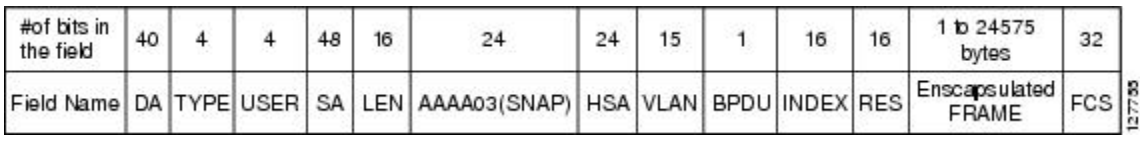


Table 3 describes the fields for 802.1q VLANs.

Table 43: ISL VLAN Encapsulation

Field	Description
DA (destination address)	This 40-bit field is a multicast address and is set at 0*n*01-00-0c-00-00 or 0*n*03-00-0c-00-00. The receiving host determines that the frame is encapsulated in ISL by reading the 40-bit DA field and matching it with one of the two ISL multicast addresses.
TYPE	This 4-bit field indicates the type of frame that is encapsulated and to indicate alternative encapsulations. TYPE codes: • 0000—Ethernet • 0001—Token Ring • 0010—FDDI • 0011—ATM
USER	This 4-bit field is used to extend the meaning of the Frame TYPE field. The default USER field value is 0000. For Ethernet frames, the USER field bits 0 and 1 indicate the priority of the packet as it passes through the switch. Whenever traffic can be handled more quickly, the packets with this bit set should take advantage of the quicker path. However, such paths are not required. USER codes: • *xx*00—Normal priority • *xx*01—Priority 1 • *xx*10—Priority 2 • *xx*11—Highest priority
SA	This 48-bit field is the source address field of the ISL packet. It should be set to the 802.3 MAC address of the switch port transmitting the frame. The receiving device can ignore the SA field of the frame.

Field	Description
LEN	This 16-bit value field stores the actual packet size of the original packet. The LEN field represents the length of the packet in bytes, excluding the DA, TYPE, USER, SA, LEN, and FCS fields. The total length of the excluded fields is 18 bytes, so the LEN field represents the total length minus 18 bytes.
AAAA03(SNAP)	The AAAA03 Subnetwork Access Protocol (SNAP) field is a 24-bit constant value of 0*x*AAAA03.
HSA	This 24-bit field represents the upper three bytes (the manufacturer's ID portion) of the SA field. It must contain the value 0*x*00-00-0C.
VLAN	This 15-bit field is the virtual LAN ID of the packet. This value is used to mark frames on different VLANs.
BPDU	The bit in the bridge protocol data unit (BPDU) field is set for all BPDU packets that are encapsulated by the ISL frame. The BPDUs are used by the spanning tree algorithm to learn information about the topology of the network. This bit is also set for Cisco Discovery Protocol and VLAN Trunk Protocol (VTP) frames that are encapsulated.
INDEX	This 16-bit field indicates the port index of the source of the packet as it exits the switch. It is used for diagnostic purposes only, and may be set to any value by other devices. It is ignored in received packets.
RES	This 16-bit field is used when Token Ring or FDDI packets are encapsulated with an ISL frame.
Encapsulated FRAME	This field contains the encapsulated Layer 2 frame.
FCS	The FCS field consists of 4 bytes. It includes a 32-bit CRC value, which is created by the sending station and is recalculated by the receiving station, to check for damaged frames. The FCS covers the DA, SA, Length/Type, and Data fields. When an ISL header is attached to a Layer 2 frame, a new FCS is calculated over the entire ISL packet and added to the end of the frame. **Note** The addition of the new FCS does not alter the original FCS that is contained within the encapsulated frame.

Layer 3 Information Capture Using NetFlow Layer 2 and Security Monitoring Exports

The five fields that the NetFlow Layer 2 and Security Monitoring Exports feature captures from Layer 3 IP traffic in a flow are the following:

- Internet Control Message Protocol (ICMP) type and code
- ID field
- Fragment offset
- Packet length field
- Time-to-live field

Figure 5 shows the fields in an IP packet header.

Figure 30: IP Packet Header Fields

Table 4 describes the header fields in Figure 5.

Table 44: IP Packet Header Fields

Field	Description
Version	The version of the IP protocol. If this field is set to 4, it is an IPv4 datagram. If this field is set to 6, it is an IPv6 datagram. **Note** IPv4 and IPv6 headers have different structures.
IHL (Internet Header Length)	Internet Header Length is the length of the Internet header in 32-bit word format and thus points to the beginning of the data. **Note** The minimum value for the correct header length is 5.
ToS	Type of service (ToS) provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when a networking device transmits a datagram through a particular network.
Total Length	Total length is the length of the datagram, measured in octets, including Internet header and data.

Field	Description
Identification (ID)	The value in the ID field is entered by the sender. All the fragments of an IP datagram have the same value in the ID field. Subsequent IP datagrams from the same sender will have different values in the ID field. Frequently, a host receives fragmented IP datagrams from several senders concurrently. Also, frequently a host receives multiple IP datagrams from the same sender concurrently. The value in the ID field is used by the destination host to ensure that the fragments of an IP datagram are assigned to the same packet buffer during the IP datagram reassembly process. The unique value in the ID field is used to prevent the receiving host from mixing together IP datagram fragments of different IP datagrams from the same sender during the IP datagram reassembly process.
Flags	A sequence of three bits is used to set and track IP datagram fragmentation parameters. The bits are: • 001—The IP datagram can be fragmented. More fragments of the current IP datagram are in transit. • 000—The IP datagram can be fragmented. This is the last fragment of the current IP datagram. • 010—The IP datagram cannot be fragmented. This is the entire IP datagram.
Fragment Offset	This field indicates where in the datagram this fragment belongs.
TTL (Time-to-Live)	This field indicates the maximum time the datagram is allowed to remain in the Internet system. If this field contains the value 0, then the datagram must be destroyed. This field is modified in Internet header processing. The TTL is measured in units of seconds, but because every module that processes a datagram must decrease the TTL by at least 1 even if it processes the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram can exist. The intention is to discard undeliverable datagrams and bound the maximum datagram lifetime.
Protocol	Indicates the type of transport packet included in the data portion of the IP datagram. Common values are: • 1—ICMP • 6—TCP • 17—UDP
Header checksum	A checksum on the header only. Because some header fields, such as the TTL field, change every time an IP datagram is forwarded, this value is recomputed and verified at each point that the Internet header is processed.

Field	Description
Source IP Address	IP address of the sending station.
Destination IP Address	IP address of the destination station.
Options and Padding	The options and padding may appear in datagrams. If they do appear, they must be implemented by all IP modules (host and gateways). Options and padding are always implemented in any particular datagram; transmissions are not.

Figure 6 shows the fields in an ICMP datagram.

Figure 31: ICMP Datagram

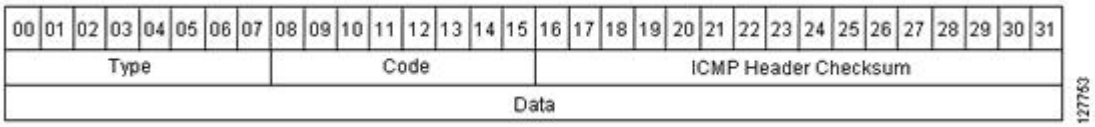


Table 5 interprets the packet format in the figure seen above. ICMP datagrams are carried in the data area of an IP datagram, after the IP header.

Table 45: ICMP Packet Format

Type	Name	Codes
0	Echo reply	0—None.
1	Unassigned	—
2	Unassigned	—

Type	Name	Codes
3	Destination unreachable	0—Network unreachable. 1—Host unreachable. 2—Protocol unreachable. 3—Port unreachable. 4—Fragmentation needed and don't fragment (DF) bit set. 5—Source route failed. 6—Destination network unknown. 7—Destination host unknown. 8—Source host isolated. 9—Communication with the destination network is administratively prohibited. 10—Communication with the destination host is administratively prohibited. 11—Destination network unreachable for ToS. 12—Destination host unreachable for ToS.
4	Source quench	0—None.
5	Redirect	0—None. 0—Redirect datagram for the network. 1—Redirect datagram for the host. 2—Redirect datagram for the ToS and network. 3—Redirect datagram for the ToS and host.
6	Alternate host address	0—Alternate address for the host.
7	Unassigned	—
8	Echo	0—None.
9	Router advertisement	0—None.
10	Router selection	0—None.
11	Time exceeded	0—Time to live exceeded in transit.
12	Parameter problem	0—Pointer indicates the error. 1—Missing a required option. 2—Inappropriate length.

Type	Name	Codes
13	Timestamp	0—None.
14	Timestamp reply	0—None.
15	Information request	0—None.
16	Information reply	0—None.
17	Address mask request	0—None.
18	Address mask reply	0—None.
19	Reserved (for security)	—
20–29	Reserved (for robustness experiment)	—
30	Trace route	—
31	Datagram conversion error	—
32	Mobile host redirect	—
33	IPv6 where-are-you	—
34	IPv6 I-am-here	—
35	Mobile registration request	—
36	Mobile registration reply	—
37–255	Reserved	—

NBAR Data Export

Network based application recognition (NBAR) is a classification engine that recognizes and classifies a wide variety of protocols and applications, including web-based and other difficult-to-classify applications and protocols that use dynamic TCP/UDP port assignments.

When NBAR recognizes and classifies a protocol or application, the network can be configured to apply the appropriate application mapping with that protocol.

For a Catalyst 6500 series switch equipped with a Supervisor 32/programmable intelligent services accelerator (PISA), the NBAR flow can be exported along with NetFlow export records.

The application-aware NetFlow feature integrates NBAR with NetFlow to provide the ability to export application information collected by NBAR using NetFlow. The application IDs created for the NetFlow

Version 9 attribute export application names along with the standard attributes such as IP address and TCP/UDP port information. The NetFlow collector collects these flows based on the source IP address and ID. The source ID refers to the unique identification for flows exported from a particular device.

The NBAR data exported to the NetFlow collector contains application mapping information. Using the NetFlow Data export options, the table containing the application IDs mapped to their application names is exported to the NetFlow collector. The mapping table is sent using the **ip flow-export template options nbar** command. By default, the mapping information is refreshed every 30 minutes. You can configure the refresh interval by using the **ip flow-export template options timeout-rate** command.

NetFlow export uses several aging mechanisms to manage the NetFlow cache. However, the NBAR data export intervals do not use NetFlow aging parameters.

Benefits of NBAR NetFlow Integration

NBAR enables network administrators to track a variety of protocols and the amount of traffic generated by each protocol. NBAR also allows network administrators to organize traffic into classes. These classes can then be used to provide different levels of service for network traffic, thereby allowing better network management by providing the appropriate level of network resources for network traffic.

How to Configure NetFlow Layer 2 and Security Monitoring Exports

Configuring NetFlow Layer 2 and Security Monitoring Exports

Before You Begin

Cisco Express Forwarding (formerly known as CEF), distributed Cisco Express Forwarding (formerly known as dCEF), or fast switching for IP must be configured on your system before you configure the NetFlow Layer 2 and Security Monitoring Exports feature.

The task in the "Verifying NetFlow Layer 2 and Security Monitoring Exports" section uses the **show ip cache verbose flow** command to display the values of the fields; the NetFlow Layer 2 and Security Monitoring Exports feature is configured to capture the values of these fields. In order to display the values of the fields, your router must forward the IP traffic that meets the criteria for these fields. For example, if you configure the **ip flow-capture ip-id** command, your router must be forwarding IP datagrams to capture the IP ID values from the IP datagrams in the flow.

Depending on the release that your router supports, you can capture the values of the Layer 3 IP fragment offset field from the IP headers in your IP traffic using the **ip flow-capture fragment-offset** command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-capture fragment-offset**
4. **ip flow-capture icmp**
5. **ip flow-capture ip-id**
6. **ip flow-capture mac-addresses**
7. **ip flow-capture packet-length**
8. **ip flow-capture ttl**
9. **ip flow-capture vlan-id**
10. **interface** *type* [*number* | *slot* / *port*]
11. Enter one of the following commands:
    - **ip flow ingress**
    - **ip flow egress**
12. **exit**

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	**ip flow-capture fragment-offset** **Example:** `Device(config)# ip flow-capture fragment-offset`	(Optional) Enables the software to capture the value of the IP fragment offset field from the first fragmented IP datagram in a flow.
Step 4	**ip flow-capture icmp** **Example:** `Device(config)# ip flow-capture icmp`	(Optional) Enables the software to capture the value of the ICMP type and code fields from ICMP datagrams in a flow.

	Command or Action	Purpose
Step 5	**ip flow-capture ip-id** **Example:** `Device(config)# ip flow-capture ip-id`	(Optional) Enables the software to capture the value of the IP ID field from the first IP datagram in a flow.
Step 6	**ip flow-capture mac-addresses** **Example:** `Device(config)# ip flow-capture mac-addresses`	(Optional) Enables the software to capture the values of the source and destination MAC addresses from the traffic in a flow.
Step 7	**ip flow-capture packet-length** **Example:** `Device(config)# ip flow-capture packet-length`	(Optional) Enables the software to capture the minimum and maximum values of the packet length field from IP datagrams in a flow.
Step 8	**ip flow-capture ttl** **Example:** `Device(config)# ip flow-capture ttl`	(Optional) Enables the software to capture the minimum and maximum values of the time-to-live (TTL) field from IP datagrams in a flow.
Step 9	**ip flow-capture vlan-id** **Example:** `Device(config)# ip flow-capture vlan-id`	(Optional) Enables the software to capture the 802.1q or ISL VLAN-ID field from VLAN encapsulated frames in a flow that is received or transmitted on trunk ports.
Step 10	**interface** *type* [*number* | *slot* / *port*] **Example:** `Device(config)# interface ethernet 0/0`	Enters interface configuration mode for the type of interface specified in the command.

Step 11	Enter one of the following commands:
	• **ip flow ingress**
	• **ip flow egress**
	Example:
	`Device(config-if)# ip flow ingress`
	or
	`Device(config-if)# ip flow egress`
		Enables ingress NetFlow data collection on the interface.
		or
		Enables egress NetFlow data collection on the interface.

	Command or Action	Purpose
Step 12	**exit** **Example:** `Device(config-if)# exit`	Exits interface configuration mode.

Verifying NetFlow Layer 2 and Security Monitoring Exports

Perform this task to verify the configuration of NetFlow Layer 2 and Security Monitoring Exports.

Restrictions

The Verifying NetFlow Layer 2 and Security Monitoring Exports task uses the **show ip cache verbose flow** command. The following restrictions apply to using the **show ip cache verbose flow** command.

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running distributed Cisco Express Forwarding (formerly known as dCEF), NetFlow cache information is maintained on each line card or Versatile Interface Processor (VIP). If you want to use the **show ip cache verbose flow** command to display this information on a distributed platform, you must enter the command at a line card prompt.

Cisco 7500 Series Platform

To display detailed NetFlow cache information on a Cisco 7500 series router that is running distributed Cisco Express Forwarding (formerly known as dCEF), enter the following sequence of commands:

```
Device# if-con

slot-number
LC-
slot-number
# show ip cache verbose flow
```

Depending on your release, you can retrieve detailed NetFlow cache information. Enter the following command to display detailed NetFlow cache information:

```
Device# execute-on
slot-number
show ip cache verbose flow
```

Cisco 12000 Series Platform

To display detailed NetFlow cache information on a Cisco 12000 series router, enter the following sequence of commands:

```
Device# attach
slot-number
LC-
```

```
slot-number
# show ip cache verbose flow
```

Depending on your release, you can retrieve detailed NetFlow cache information. Enter the following command to display detailed NetFlow cache information:

```
Device# execute-on slot-number show ip cache verbose flow
```

The following sample output shows values from the Layer 2 and Layer 3 fields in the flows captured by the NetFlow Layer 2 and Security Monitoring Exports feature.

```
Device# show ip cache verbose flow

IP packet size distribution (25229 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .206 .793 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  6 active, 4090 inactive, 17 added
  505 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 25736 bytes
  12 active, 1012 inactive, 39 added, 17 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-Telnet           1      0.0       362   940      2.7      60.2       0.0
TCP-FTP              1      0.0       362   840      2.7      60.2       0.0
TCP-FTPD             1      0.0       362   840      2.7      60.1       0.1
TCP-SMTP             1      0.0       361  1040      2.7      60.0       0.1
UDP-other            5      0.0         1    66      0.0       1.0      10.6
ICMP                 2      0.0      8829  1378    135.8      60.7       0.0
Total:              11      0.0      1737  1343    147.0      33.4       4.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.251.138.218  Et1/0.1        172.16.10.2     06 80  00      65
0015 /0  0                     0015 /0  0     10.0.0.0                840    10.8
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                           Max plen:       840
Min TTL:        59                           Max TTL:         59
IP id:           0
```

Configuring NBAR Support for NetFlow Exports

Perform this task to export NBAR data to the Cisco NetFlow Collector Software.

Before You Begin

You must enable NetFlow Version 9 and NBAR before you configure NBAR data export.

You must add and configure the following fields to the Cisco NetFlow Collector Software to identify the flow exported by the NBAR data export feature:

- app_id field as an integer with Numeric ID of 95.
- app_name field as a UTF-8 String with Numeric ID of 96.
- sub_app_id field as an integer with Numeric ID of 97.
- biflowDirection field as an integer with Numeric ID of 239.

Note The biflowDirection field provides information about the host that initiates the session. The size of this field is one byte. RFC 5103 provides details for using this field.

Note NBAR support can be configured only with the NetFlow Version 9 format. If you try to configure NBAR data export with other versions, the following error message appears:

```
1d00h: %FLOW : Export version 9 not enabled
```

NBAR data export does not use NetFlow aging parameters.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export version 9**
4. **ip flow-capture nbar**
5. **ip flow-export template options nbar**
6. **exit**
7. **show ip flow export nbar**
8. **clear ip flow stats nbar**

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	**ip flow-export version 9** **Example:** `Router(config)# ip flow-capture version 9`	Enables the Version 9 format to export NetFlow cache entries.

	Command or Action	Purpose
Step 4	**ip flow-capture nbar** **Example:** `Router(config)# ip flow-capture nbar`	Enables you to capture the NBAR data in NetFlow export records.
Step 5	**ip flow-export template options nbar** **Example:** `Router(config)# ip flow-export template options nbar`	Exports application mapping information to the Cisco NetFlow Collector Software.
Step 6	**exit** **Example:** `Router(config)# exit`	Exits global configuration mode.
Step 7	**show ip flow export nbar** **Example:** `Router# show ip flow export nbar`	(Optional) Displays NBAR export records.
Step 8	**clear ip flow stats nbar** **Example:** `Router# clear ip flow stats nbar`	(Optional) Clears NetFlow accounting statistics for NBAR.

Configuration Examples for NetFlow Layer 2 and Security Monitoring Exports

Example: Configuring NetFlow Layer 2 and Security Monitoring Exports

The following example shows how to configure the NetFlow Layer 2 and Security Monitoring Exports feature:

```
Router> enable
Router# configure terminal
Router(config)# ip flow-capture fragment-offset
Router(config)# ip flow-capture icmp
Router(config)# ip flow-capture ip-id
Router(config)# ip flow-capture mac-addresses
Router(config)# ip flow-capture packet-length
Router(config)# ip flow-capture ttl
Router(config)# ip flow-capture vlan-id
```

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip flow ingress
or
Router(config-if)# ip flow egress
Router(config-if)# exit
```

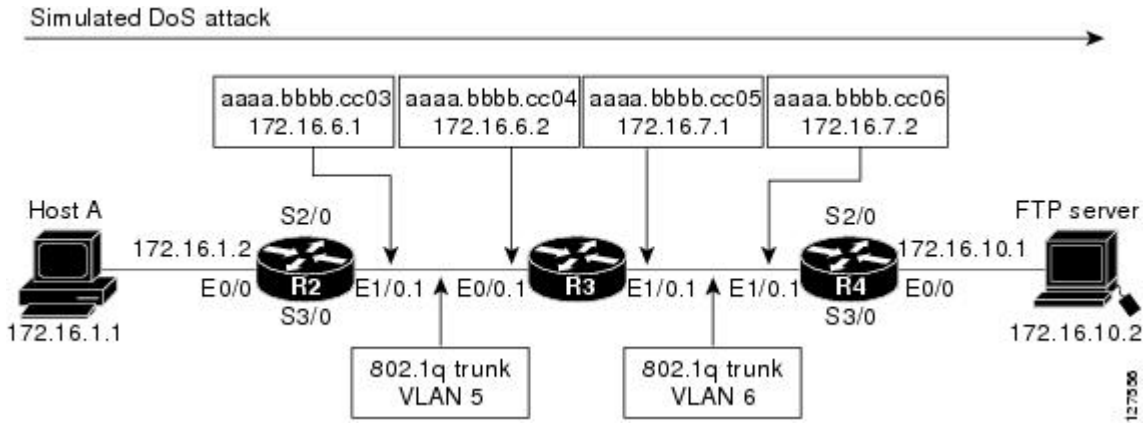
Example: Analyzing a Simulated FTP Attack

The following example shows how to use the NetFlow Layer 2 and Security Monitoring Exports feature to find out whether your network is being attacked by a host that is sending fake FTP traffic in an attempt to overwhelm the FTP server. This attack might cause end users to see a degradation in the ability of the FTP server to accept new connections or to service existing connections.

Figure 7 shows a network in which Host A is sending fake FTP packets to the FTP server.

This example also shows you how to use the Layer 2 data, captured by the NetFlow Layer 2 and Security Monitoring Exports feature, to learn where the traffic is originating and what path it is taking through the network.

Figure 32: Test Network



Tip Track the MAC addresses and IP addresses of the devices in your network. You can use them to analyze attacks and resolve problems.

Note This example does not include the **ip flow-capture icmp** command, which captures the value of the ICMP type and code fields.

R2

```
!
hostname R2
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc02
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc03
 no ip address
```

```
!
interface Ethernet1/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.1 255.255.255.0
!
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R3

```
!
hostname R3
!
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture ip-id
ip flow-capture mac-addresses
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc04
 no ip address
!
interface Ethernet0/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.2 255.255.255.0
 ip accounting output-packets
 ip flow ingress
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc05
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.1 255.255.255.0
 ip accounting output-packets
 ip flow egress
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R4

```
!
hostname R4
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc07
 ip address 172.16.10.1 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc06
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.2 255.255.255.0
!
router rip
 version 2
```

```
 network 172.16.0.0
 no auto-summary
!
```

The **show ip cache verbose flow** command displays the NetFlow flows that have been captured from the FTP traffic that Host A is sending.

The fields that have values captured by the **ip flow-capture** command are shown in Table 6. The fields and values are used to analyze the traffic for this example. The other fields captured by the **show ip cache verbose flow** command are explained in subsequent tables (Table 7 to Table 9).

```
R3# show ip cache verbose flow

IP packet size distribution (3596 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .003 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .995 .000 .000 .000 .000 .000 .000 .000
```

The preceding output shows the percentage distribution of packets by size. In this display, 99.5 percent of the packets fall in the 1024-byte size range, and 0.3 percent fall in the 64-byte range.

The rest of the output of the **show ip cache verbose flow** command is as follows:

```
IP Flow Switching Cache, 278544 bytes
  5 active, 4091 inactive, 25 added
  719 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 25736 bytes
  10 active, 1014 inactive, 64 added, 25 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP              5      0.0       429   840      6.6      58.1       1.8
Total:               5      0.0       129   835      6.6      17.6       7.9
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.132.221.111  Et1/0.1        172.16.10.2     06 80  00     198
0015 /0  0                     0015 /0  0     0.0.0.0                840    41.2
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                            Max plen:       840
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        10.251.138.218  Et1/0.1        172.16.10.2     06 80  00     198
0015 /0  0                     0015 /0  0     0.0.0.0                840    41.2
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                            Max plen:       840
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        10.10.12.1      Et1/0.1        172.16.10.2     06 80  00     203
0015 /0  0                     0015 /0  0     0.0.0.0                840    42.2
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                            Max plen:       840
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        10.231.185.254  Et1/0.1        172.16.10.2     06 80  00     203
0015 /0  0                     0015 /0  0     0.0.0.0                840    42.2
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                            Max plen:       840
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        10.71.200.138   Et1/0.1        172.16.10.2     06 80  00     203
0015 /0  0                     0015 /0  0     0.0.0.0                840    42.2
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      840                            Max plen:       840
Min TTL:        59                            Max TTL:         59
IP id:           0
R3#
```

Table 6 describes the significant fields shown in the NetFlow cache section of the output.

Table 46: Field Descriptions in the NetFlow Cache Section of the Output

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but that were not assigned to a specific flow at the time this command was entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code caused entries to expire (used by Cisco Customer Support Engineers (CSEs) for diagnostic purposes).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
last clearing of statistics	The period of time that has passed since the **clear ip flow stats** command was last executed. The standard time output format of hours, minutes, and seconds (hh:mm:ss) is used for a period of time less than 24 hours. This time output format changes to hours and days after the time exceeds 24 hours.

Table 7 describes the significant fields shown in the activity by the protocol section of the output.

Table 47: Field Descriptions in the Activity by Protocol Section of the Output

Field	Description
Protocol	IP protocol and the well-known port number. (Refer to http://www.iana.org, Protocol Assignment Number Services, for the latest RFC values.) **Note** Only a small subset of all protocols is displayed.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol per second, which is equal to the total flows divided by the number of seconds for this summary period.

Field	Description
Packets/Flow	Average number of packets for the flows for this protocol, which is equal to the total packets for this protocol divided by the number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes for the packets for this protocol, which is equal to the total bytes for this protocol divided by the total number of packets for this protocol for this summary period.
Packets/Sec	Average number of packets for this protocol per second, which is equal to the total packets for this protocol divided by the total number of seconds for this summary period.
Active(Sec)/Flow	Number of seconds between the first and the last packet of an expired flow divided by the number of total flows for this protocol, for this summary period.
Idle(Sec)/Flow	Number of seconds observed from the last packet in each nonexpired flow for this protocol until the time at which the **show ip cache verbose flow** command was entered divided by the total number of flows for this protocol, for this summary period.

Table 8 describes the significant fields in the NetFlow record section of the output.

Table 48: Field Descriptions in the NetFlow Record Section of the Output

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source port number (displayed in hexadecimal format), IP address mask, and autonomous system number. This is always set to 0 in Multiprotocol Label Switching (MPLS) flows.
SrcIPaddress	The source IP address of the traffic in the five flows. The traffic is using five different IP source addresses. They are: • 10.132.221.111 • 10.251.138.218 • 10.10.12.1 • 10.231.185.254 • 10.71.200.138

Field	Description
DstIf	Interface from which the packet was sent. **Note** If an asterisk (*) immediately follows the DstIf field, the flow being shown is an egress flow.
Port Msk AS	Source port number (displayed in hexadecimal format), IP address mask, and autonomous system number. The value of this field is always set to 0 in MPLS flows.
DstIPaddress	The destination IP address of the traffic. **Note** 172.17.10.2 is the IP address of the FTP server.
NextHop	The Border Gateway Protocol (BGP) next-hop address. This is always set to 0 in MPLS flows.
Pr	IP protocol “well-known” port number, displayed in hexadecimal format. (Refer to http://www.iana.org, Protocol Assignment Number Services, for the latest RFC values.)
ToS	Type of service, displayed in hexadecimal format.
B/Pk	Average number of bytes observed in the packets seen for this flow.
Flgs	TCP flag, shown in hexadecimal format. This value is the result of bitwise OR of the TCP flags from all packets in the flow.
Pkts	Number of packets in this flow.
Active	Time the flow has been active.

Table 9 describes the fields and values for the NetFlow Traffic Classification and Identification fields for the NetFlow record lines section of the output.

Table 49: NetFlow Traffic Classification and Identification Fields in the NetFlow Record lines section of the Output

Field	Description
MAC	The source and destination MAC addresses from the traffic, read from left to right in the output. • The traffic is received from MAC address aaaa.bbbb.cc03. **Note** This MAC address is interface 1/0.1 on router R2. • The traffic is transmitted to MAC address aaaa.bbbb.cc06. **Note** This MAC address is interface 1/0.1 on router R4.
VLAN id	The source and destination VLAN IDs, read from left to right in the output. • The traffic is received from VLAN 5. • The traffic is transmitted to VLAN 6.
Min plen	The minimum packet length for packets captured in the five flows. The current value is 840.
Max plen	The maximum packet length for packets captured in the five flows. The current value is 840.
Min TTL	The minimum time to live (TTL) for packets captured in the five flows. The current value is 59.
Max TTL	The maximum TTL for packets captured in the five flows. The current value is 59.
IP ID	The IP identifier field for the traffic in the five flows. The current value is 0.

The fact that the Layer 3 TTL, identifier, and packet length fields in the five flows have the same values indicates that this traffic is a DoS attack. If this data had been captured from real traffic, the values would normally be different. The fact that all five of these flows have a TTL value of 59 indicates that this traffic is

originating from points that are at the same distance from R3. Real user traffic would normally be arriving from different distances; therefore, the TTL values would be different.

If this traffic is identified as a DoS attack (based on the data captured in the Layer 3 fields), you can use the Layer 2 information in the flows to identify the path the traffic is taking through the network. In this example, the traffic is being sent to R3 on VLAN 5, by R2. You can demonstrate that R2 is transmitting the traffic over interface 1/0.1 because the source MAC address (aaaa.bbbb.cc03) belongs to 1/0.1 on R2. You can identify that R3 is transmitting the traffic using VLAN 6 on interface 1/0.1 to interface 1/0.1 on R4 because the destination MAC address (aaaa.bbbb.cc06) belongs to interface 1/0.1 on R4.

You can use this information to mitigate this attack. One possible way to mitigate this attack is to configure an extended IP access list that blocks FTP traffic from any host with a source address that is on the 10.0.0.0 network. Another possible solution is to configure a default route for the 10.0.0.0 network that points to the null interface on the router.

Caution Each of these solutions blocks traffic from legitimate hosts on the 10.0.0.0 network. Therefore these solutions should be used only while you identify the point of origin of the attack and decide how to stop it.

Example: Analyzing a Simulated ICMP Ping Attack

The following example shows how to use the NetFlow Layer 2 and Security Monitoring Exports feature to learn that your network is being attacked by ICMP traffic. It uses the network shown in Figure 7. Host A is sending very large ICMP ping packets to the FTP server.

R2

```
!
hostname R2
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc02
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc03
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.1 255.255.255.0
!
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R3

```
!
hostname R3
!
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture icmp
ip flow-capture ip-id
```

```
ip flow-capture mac-addresses
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc04
 no ip address
!
interface Ethernet0/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.2 255.255.255.0
 ip accounting output-packets
 ip flow ingress
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc05
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.1 255.255.255.0
 ip accounting output-packets
 ip flow egress
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R4

```
!
hostname R4
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc07
 ip address 172.16.10.1 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc06
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.2 255.255.255.0
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

The **show ip cache verbose flow** command displays the NetFlow flows that have been captured from the ICMP traffic that Host A is sending.

The fields that have their values captured by the **ip flow-capture** command are explained in Table 10. The fields and values are used to analyze the traffic for this example. The other fields captured by the **show ip cache verbose flow** command are explained in the subsequent tables (Table 11 to Table 13).

```
R3# show ip cache verbose flow

IP packet size distribution (5344 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .000 .166 .832 .000 .000 .000 .000 .000 .000
```

The preceding output shows the percentage distribution of packets by size. In this display, 16.6 percent of the packets fall in the 1024-byte size range and 83.2 percent fall in the 1536-byte range.

The rest of the output of the **show ip cache verbose flow** command is as follows:

```
IP Flow Switching Cache, 278544 bytes
  3 active, 4093 inactive, 7 added
  91 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 10 seconds
IP Sub Flow Cache, 25736 bytes
  7 active, 1017 inactive, 17 added, 7 added to flow
  0 alloc failures, 0 force free
  1 chunk, 0 chunks added
  last clearing of statistics 00:01:13
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                 2      0.0      1500  1378     42.8      11.4      10.9
Total:               2      0.0       600  1378     42.9      11.5      10.8
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.106.1.1      Et1/0.1        172.16.10.2     01 00  10     391
0000 /0  0                     0800 /0  0     0.0.0.0              1500     8.6
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      1500                           Max plen:       1500
Min TTL:         59                           Max TTL:          59
ICMP type:       8                            ICMP code:         0
IP id:       13499
Et0/0.1        10.106.1.1      Et1/0.1        172.16.10.2     01 00  00    1950
0000 /0  0                     0000 /0  0     0.0.0.0              1354     8.6
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      772                            Max plen:       1500
Min TTL:         59                           Max TTL:          59
ICMP type:       0                            ICMP code:         0
IP id:       13499                            FO:            185
R3#
```

For field descriptions of the NetFlow Cache output, see Table 10.

Table 50: Field Descriptions in the NetFlow Cache Section of the Output

Field	Description
bytes	Number of bytes of memory used by the NetFlow cache.
active	Number of active flows in the NetFlow cache at the time this command was entered.
inactive	Number of flow buffers that are allocated in the NetFlow cache but that were not assigned to a specific flow at the time this command was entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code caused entries to expire (used by Cisco Customer Support Engineers (CSEs) for diagnostic purposes).
flow alloc failures	Number of times the NetFlow code tried to but was not able to allocate flows.

Field	Description
last clearing of statistics	The period of time that has passed since the **clear ip flow stats** command was last executed. The standard time output format of hours, minutes, and seconds (hh:mm:ss) is used for a period of time less than 24 hours. The time output format changes to hours and days after the time exceeds 24 hours.

For field descriptions of the Activity by Protocol lines section of the output, see Table 11.

Table 51: Field Descriptions in the Activity by Protocol lines section of the Output

Field	Description
Protocol	IP protocol and the well-known port number. (Refer to http://www.iana.org, Protocol Assignment Number Services, for the latest RFC values.) **Note** Only a small subset of all protocols is displayed.
Total Flows	Number of flows for this protocol since the last time statistics were cleared.
Flows/Sec	Average number of flows for this protocol per second, which is equal to the total flows divided by the number of seconds for this summary period.
Packets/Flow	Average number of packets for the flows for this protocol, which is equal to the total packets for this protocol divided by the number of flows for this protocol for this summary period.
Bytes/Pkt	Average number of bytes for the packets for this protocol, which is equal to the total bytes for this protocol divided by the total number of packets for this protocol for this summary period.
Packets/Sec	Average number of packets for this protocol per second, which is equal to the total packets for this protocol divided by the total number of seconds for this summary period.
Active(Sec)/Flow	Number of seconds between the first and the last packet of an expired flow divided by the number of total flows for this protocol, for this summary period.

Field	Description
Idle(Sec)/Flow	Number of seconds observed from the last packet in each nonexpired flow for this protocol until the time at which the **show ip cache verbose flow** command was entered, divided by the total number of flows for this protocol, for this summary period.

For field descriptions of the NetFlow Record lines section of the output, see Table 12.

Table 52: Field Descriptions in the NetFlow Record lines section of the Output

Field	Description
SrcIf	Interface on which the packet was received.
Port Msk AS	Source port number (displayed in hexadecimal format), IP address mask, and autonomous system number. The value of this field is always set to 0 in MPLS flows.
SrcIPaddress	IP address of the device that transmitted the packet. The sending host is using 10.106.1.1 as the source IP address.
DstIf	Interface from which the packet was sent. **Note** If an asterisk (*) immediately follows the DstIf field, the flow being shown is an egress flow.
Port Msk AS	Destination port number (displayed in hexadecimal format), IP address mask, and autonomous system. This is always set to 0 in MPLS flows.
DstIPaddress	IP address of the destination device.
NextHop	The BGP next-hop address. This is always set to 0 in MPLS flows.
Pr	IP protocol “well-known” port number, displayed in hexadecimal format. (Refer to http://www.iana.org, Protocol Assignment Number Services, for the latest RFC values.)
ToS	Type of service, displayed in hexadecimal format.
B/Pk	Average number of bytes observed for the packets seen for this flow.

Field	Description
Flgs	TCP flag, shown in hexadecimal format. This value is the result of bitwise OR of the TCP flags from all packets in the flow.
Pkts	Number of packets in this flow.
Active	Time the flow has been active.

For field descriptions of the NetFlow Traffic Classification and Identification fields, see Table 13.

Table 53: NetFlow Traffic Classification and Identification

Field	Description
MAC	The source and destination MAC addresses from the traffic, read from left to right in the output. • The traffic is received from MAC address aaaa.bbbb.cc03. **Note** This MAC address is interface 1/0.1 on router R2. • The traffic is transmitted to MAC address aaaa.bbbb.cc06. **Note** This MAC address is interface 1/0.1 on router R4.
VLAN id	The source and destination VLAN IDs, read from left to right in the output. • The traffic is received from VLAN 5. • The traffic is transmitted to VLAN 6.
Min plen	The minimum packet length for the packets captured in the two flows. The current value for the first flow is 1500. The current value for the second flow is 772.
Max plen	The maximum packet length for the packets captured in the two flows. The current value for the first flow is 1500. The current value for the second flow is 1500.

Field	Description
Min TTL	The minimum time to live (TTL) for the packets captured in the two flows. The current value is 59.
Max TTL	The maximum TTL for the packets captured in the two flows. The current value is 59.
IP	The IP identifier field for the traffic in the flows. The current value is 13499 for the two flows.
ICMP type	The Internet Control Message Protocol (ICMP) type field from the ICMP datagram captured in the first flow. The value is 8.
ICMP code	The ICMP code field from the ICMP datagram captured in the second flow. The value is 0.
FO	This is the value of the fragment offset field from the first fragmented datagram in the second flow. The value is 185.

Two ICMP flows are shown in the output. They are from the same ICMP datagram because they have the same IP ID field value of 13499. When two ICMP flows have the same IP ID value, the ICMP datagram being analyzed has been fragmented. The first flow has the ICMP type field set to 8, which indicates that this is an ICMP echo request (ping) datagram. The value of 185 in the fragment offset (FO) field in the second flow shows where this fragment will be placed in the memory buffer of the FTP server as the server reassembles the ICMP datagram. The value of 185 applies only to the first fragment of this datagram. The subsequent values will be greater because they include the previous fragments.

The value of 0 in the ICMP type field of the second flow does not mean that this flow is an ICMP echo reply as Table 13 shows. In this case, the ICMP type field value is set to 0 because the ICMP headers for fragments of ICMP datagrams do not have the type and code fields. The default value of 0 is inserted instead.

Note If this data were captured from a real ICMP attack, it would probably have more than one flow.

Although you cannot learn the original size of the ICMP datagram from the information shown by the **show ip cache verbose flow** command, the fact that the datagram was large enough to be fragmented in transit is a good indication that this is not a normal ICMP datagram. Notice the values in the minimum packet length and maximum packet length fields for both flows. The values for both fields are set to 1500 for the first flow. The value for the minimum packet length is set to 772 and the value for the maximum packet length is set to 1500 for the second flow.

If this traffic is identified as a DoS attack based on the data captured in the Layer 3 fields, you can use the Layer 2 information in the flows to identify the path that the traffic is taking through the network. In this example, the traffic is being sent to R3 on VLAN 5, by R2. Here, R2 is transmitting the traffic over interface 1/0.1 because the source MAC address (aaaa.bbb.cc03) belongs to 1/0.1 on R2. It is evident that R3 is transmitting the traffic using VLAN 6 on interface 1/0.1 to interface 1/0.1 on R4, because the destination MAC address (aaaa.bbbb.cc06) belongs to interface 1/0.1 on R4.

You can use this information to mitigate the attack. One possible way to mitigate this attack is by configuring an extended IP access list that blocks ICMP traffic from any host with a source address that is on the 10.0.0.0 network. Another possible solution is to configure a default route for the 10.0.0.0 network that points to the null interface on the router.

Caution Each of these solutions blocks traffic from legitimate hosts on the 10.0.0.0 network. Therefore, these solutions should be used only while you identify the point of origin of the attack and decide how to stop it.

Example: Configuring NBAR Support for NetFlow Exports

The following example shows how to configure NBAR support for NetFlow exports:

```
Device(config)# ip flow-export version 9
Device(config)# ip flow-capture nbar
Device(config)# ip flow-export template options nbar
Device(config)# exit
```

The following is sample output from the **show ip flow export nbar** command:

```
Device# show ip flow export nbar

Nbar netflow is enabled
10 nbar flows exported
0 nbar flows failed to export due to lack of internal buffers
```

The following example shows how to clear NBAR data from NetFlow accounting statistics:

```
Device# clear ip flow stats nbar
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS master command list, all releases	Cisco IOS Master Command List, All Releases
NetFlow commands	Cisco IOS NetFlow Command Reference
Overview of NetFlow	*Cisco IOS NetFlow Overview*
Overview of NBAR	*Classifying Network Traffic Using NBAR*

Related Topic	Document Title
Configuring NBAR	*Configuring NBAR Using the MQC*
Configuring NBAR using protocol-discovery	*Enabling Protocol Discovery*
Capturing and exporting network traffic data	*Configuring NetFlow and NetFlow Data Export*
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards and RFCs

Standards/RFCs	Title
RFC 5103	Bidirectional Flow Export Using IP Flow Information Export (IPFIX)

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for NetFlow Layer 2 and Security Monitoring Exports

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 . An account on Cisco.com is not required.

Table 54: Feature Information for NetFlow Layer 2 and Security Monitoring Exports

Feature Name	Releases	Feature Information
Application-Aware NetFlow	12.2(18)ZYA2	The Application-Aware NetFlow feature enables capturing of application information collected by PISA NBAR and exports using NetFlow Version 9. The following commands were modified by this feature: **clear ip flow stats**, **ip flow-capture**, **ip flow-export template options**, and **show ip flow export**.
NetFlow Layer 2 and Security Monitoring Exports	12.2(33)SRA 12.3(14)T	The NetFlow Layer 2 and Security Monitoring Exports feature enables the capture of values from fields in Layer 2 and Layer 3 of IP traffic for accounting and security analysis. The following commands were modified by this feature: **ip flow-capture**, **ip flow-export**, and **show ip cache verbose flow**.
Support for capturing the value from the fragment offset field of IP headers added to NetFlow Layer 2 and Security Monitoring Exports[9]	12.4(2)T	The **fragment-offset** keyword for the **ip flow-capture** command enables capturing the value of the IP fragment offset field from the first fragmented IP datagram in a flow.

9 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

Glossary

export packet—A type of packet built by a device (for example, a router) with NetFlow services enabled. The packet contains NetFlow statistics. The packet is addressed to another device (for example, the NetFlow Collection Engine). The other device processes the packet (parses, aggregates, and stores information about IP flows).

flow—A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, type of service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

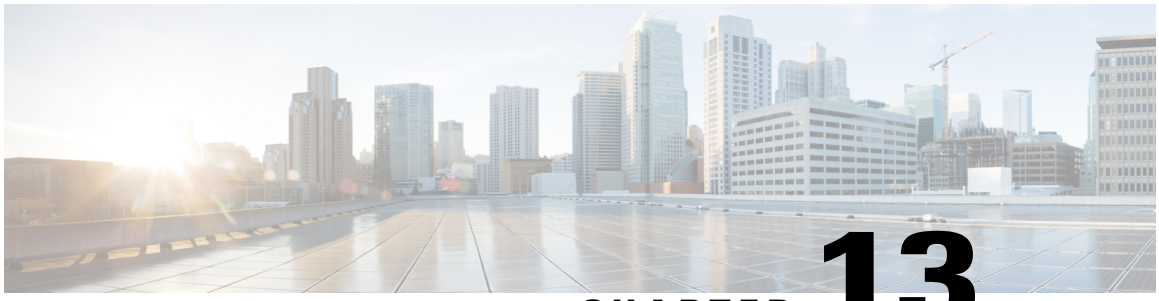
NBAR—A classification engine in the Cisco IOS software that recognizes a wide variety of applications, including web-based and client/server applications.

NetFlow—Cisco IOS accounting feature that maintains per-flow information.

NetFlow Aggregation—A NetFlow feature that lets you summarize NetFlow export data on a Cisco IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)**—**A Cisco application that is used with NetFlow on specific Cisco devices. The NetFlow Collection Engine collects packets from the device that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9—NetFlow export format Version 9. A flexible and extensible means of carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configurations.



CHAPTER 13

NetFlow Reliable Export With SCTP

NetFlow is a Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology. This document describes the NetFlow application and the new NetFlow Reliable Export With Stream Control Transmission Protocol (SCTP) feature.

The NetFlow Reliable Export with SCTP feature adds the ability for NetFlow to use the reliable and congestion-aware SCTP when exporting statistics to a network management system that supports the NetFlow data export formats, such as a system running CNS NetFlow Collection Engine (NFC).

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 NetFlow Reliable Export With SCTP

NetFlow and Cisco Express Forwarding (CEF), distributed CEF (dCEF), or fast switching must be configured on your system.

Restrictions for NetFlow Reliable Export With SCTP

The NetFlow SCTP collector must support SCTP.

Information About NetFlow Reliable Export With SCTP

NetFlow Data Capture

NetFlow identifies packet flows for both ingress and egress IP packets. It does not involve any connection-setup protocol. NetFlow is completely transparent to the existing network, including end stations and application software and network devices like LAN switches. Also, NetFlow capture and export are performed independently on each internetworking device; NetFlow need not be operational on each router in the network.

NetFlow is supported on IP and IP encapsulated traffic over most interface types and Layer 2 encapsulations.

You can display and clear NetFlow statistics. NetFlow statistics consist of IP packet size distribution, IP flow switching cache information, and flow information.

NetFlow Benefits

NetFlow can capture a rich set of traffic statistics. These traffic statistics include user, protocol, port, and type of service (ToS) information that can be used for a wide variety of purposes, including network traffic analysis and capacity planning, security, enterprise accounting and departmental chargebacks, Internet Service Provider (ISP) billing, data warehousing, and data mining for marketing purposes.

Network Application and User Monitoring

NetFlow data enables you to view detailed, time and application based usage of a network. This information allows you to plan and allocate network and application resources, and provides for extensive near real-time network monitoring capabilities. It can be used to display traffic patterns and application-based views. NetFlow provides proactive problem detection and efficient troubleshooting, and it facilitates rapid problem resolution. You can use NetFlow information to efficiently allocate network resources and to detect and resolve potential security and policy violations.

Network Analysis and Planning

You can use NetFlow to capture data for extended periods of time, which enables you to track network utilization and anticipate network growth and plan upgrades. NetFlow service data can be used to optimize network planning, which includes peering, backbone upgrades, and routing policy planning. It also enables you 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) behavior,

and enables the analysis of new network applications. NetFlow offers valuable information that you can use to reduce the cost of operating the network.

Denial of Service and Security Analysis

You can use NetFlow data to identify and classify in real time denial of service (DoS) attacks, viruses, and worms. Changes in network behavior indicate anomalies that are clearly reflected in NetFlow data. The data is also a valuable forensic tool that you can use to understand and replay the history of security incidents.

Accounting and Billing

NetFlow data provides fine-grained metering for highly flexible and detailed resource utilization accounting. For example, flow data includes details such as IP addresses, packet and byte counts, timestamps, and information about type of service (ToS) and application ports. Service providers might utilize the information for billing based on time-of-day, bandwidth usage, application usage, or QoS. Enterprise customers might utilize the information for departmental charge-back or cost allocation for resource utilization.

Traffic Engineering

NetFlow provides autonomous system (AS) traffic engineering details. You can use NetFlow-captured traffic data to understand source-to-destination traffic trends. This data can be used for load-balancing traffic across alternate paths or for forwarding traffic along a preferred route. NetFlow can measure the amount of traffic crossing peering or transit points. You can use the data to help you decide if a peering arrangement with other service providers is fair and equitable.

NetFlow Data Storage and Data Mining

NetFlow data can be stored for later retrieval and analysis in support of marketing and customer service programs. For example, the data can be mined to find out which applications and services are being used by internal and external users and target the users for improved service and advertising. In addition, NetFlow data gives market researchers access to the who, what, where, and how long information relevant to enterprises and service providers.

NetFlow Cisco IOS Packaging Information

Cisco 7200/7500/7400/MGX/AS5850

Although NetFlow functionality is included in all software images for these platforms, you must purchase a separate NetFlow feature license. NetFlow licenses are sold on a per-node basis.

Other Routers

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn . You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Elements of a NetFlow Network Flow

A NetFlow network flow is defined as a unidirectional stream of packets between a given source and destination. The source and destination are each defined by a network-layer IP address and transport-layer source and destination port numbers. Specifically, a flow is defined by the combination of the following seven key fields:

- Source IP address
- Destination IP address
- Source port number
- Destination port number
- Layer 3 protocol type
- Type of service
- Input logical interface

These seven key fields define a unique flow. If a packet has one key field different from another packet, it is considered to belong to another flow. A flow might also contain other accounting fields (such as the AS number in the NetFlow export Version 5 flow format). The fields that a given flow contains depend on the export record version that you configure. Flows are stored in the NetFlow cache.

NetFlow Main Cache Operation

The key components of NetFlow are the NetFlow cache that stores IP flow information and the NetFlow export or transport mechanism that sends NetFlow data to a network management collector, such as the NetFlow Collection Engine. NetFlow operates by creating a NetFlow cache entry (a flow record) for each active flow. NetFlow maintains a flow record within the cache for each active flow. Each flow record in the NetFlow cache contains values for the fields that are being monitored that can later be exported to a collection device, such as the NetFlow Collection Engine.

NetFlow Data Capture

NetFlow captures data from ingress (incoming) and egress (outgoing) packets. NetFlow gathers data for the following ingress IP packets:

- IP-to-IP packets
- IP-to-Multiprotocol Label Switching (MPLS) packets

NetFlow captures data for all egress (outgoing) packets through use of the following features:

- Egress NetFlow Accounting--NetFlow gathers data for all egress packets for IP traffic only.
- NetFlow MPLS Egress--NetFlow gathers data for all egress MPLS-to-IP packets.

NetFlow Export Formats

NetFlow exports data in User Datagram Protocol (UDP) datagrams in one of five formats: Version 9, Version 8, Version 7, Version 5, or Version 1. Version 9 export format, the latest version, is the most flexible and extensible format. Version 1 was the initial NetFlow export format; Version 8 only supports export from aggregation caches, and Version 7 is supported only on certain platforms. (Versions 2 through 4 and Version 6 were either not released or are not supported.)

- Version 9--A flexible and extensible format, which provides the versatility needed for support of new fields and record types. This format accommodates new NetFlow-supported technologies such as MPLS, and Border Gateway Protocol (BGP) next hop. The distinguishing feature of the NetFlow Version 9 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. Internet Protocol Information Export (IPFIX) was based on the Version 9 export format.
- Version 8--A format added to support data export from aggregation caches. Version 8 allows export datagrams to contain a subset of the usual Version 5 export data, if that data is valid for a particular aggregation cache scheme.
- Version 7--A version supported on a Catalyst 6000 series switch with a multilayer switch feature card (MSFC) running CatOS Release 5.5(7) and later. On a Catalyst 6000 series switch with an MSFC, you can export using either the Version 7 or the Version 8 format.
- Version 5--A version that adds BGP AS information and flow sequence numbers.
- Version 1--The initially released export format, rarely used today. Do not use the Version 1 export format unless the legacy collection system you are using requires it. Use either the Version 9 export format or the Version 5 export format for data export from the main cache.

NetFlow Reliable Export With SCTP

Prior to the introduction of the NetFlow Reliable Export With SCTP feature in Cisco IOS Release 12.4(4)T exporting NetFlow information was unreliable because NetFlow encapsulated the exported traffic in UDP packets for transmission to the NFC. Using an unreliable transport protocol such as UDP for sending information across a network has two major disadvantages:

- Lack of congestion awareness--The exporter sends packets as fast as it can generate them, without any regard to the bandwidth available on the network. If the link is fully congested when the NetFlow router attempts to send, the packet might simply be dropped, either before it is put on the exporter's output queue or before it gets to the next hop's input queue.
- Lack of reliability--With export over UDP, the collector has no method of signaling to the exporter that it didn't receive an exported packet. Most versions of NetFlow export packet contain a sequence number, so the collector often knows when it has lost a packet. But given that the exporter discards the export packet as soon as it has been sent and that the NetFlow router lacks a mechanism to request a retransmission of the packet, exporting over UDP can be considered to be unreliable

The NetFlow Reliable Export With SCTP feature uses the SCTP to overcome the two major disadvantages of using UDP as the transport layer protocol:

- SCTP has a congestion control mechanism to ensure that the router does not send data to the collector faster than it can receive it.
- SCTP transmits messages in a reliable manner. SCTP messages are buffered on the router until they have been acknowledged by the collector. Messages that are not acknowledged by the collector are retransmitted by the router.

SCTP is a reliable message-oriented transport layer protocol, which allows data to be transmitted between two end-points in a reliable, partially reliable, or unreliable manner. An SCTP session consists of an association between two end-points, which may contain one or more logical channels called streams. SCTP's stream based transmission model facilitates the export of a mix of different data types, such as NetFlow templates and NetFlow data, over the same connection. The maximum number of inbound and outbound streams supported by an end-point is negotiated during the SCTP association initialization process.

When you configure the NetFlow Version 9 Export and NetFlow Reliable Export features, NetFlow creates a minimum of two streams--stream 0 for templates and options, and one or more streams for carrying data, as required. The following commands are not applicable when you configure the NetFlow Version 9 Export and NetFlow Reliable Export features together because NetFlow Reliable Export export connections use SCTP reliable stream 0 for NetFlow Version 9 Export, and these commands apply only to NetFlow export connections that use UDP:

- **ip flow-export template refresh-rate**
- **ip flow-export template timeout-rate**
- **ip flow-export template options refresh-rate**
- **ip flow-export template options timeout-rate**

When more than one cache (main cache and one or more aggregation caches) is exporting data, each cache creates its own streams with their own configured reliability levels. For example, you can configure the main cache to use SCTP in full reliability mode and the NetFlow prefix aggregation cache to use partial reliability mode to send messages to the same collector using the same SCTP port.

Note When you are using SCTP as the transport protocol for exporting NetFlow traffic, the traffic is usually referred to as messages instead of datagrams because SCTP is a message-oriented protocol. When you are using UDP as the transport protocol for exporting NetFlow traffic, the traffic is usually referred to as datagrams because UDP is a datagram-oriented protocol.

Security

SCTP contains several built-in features to counter many common security threats such as the syn-flood type of DoS attack.

SCTP uses the following techniques to resist flooding attacks:

- A four-way start-up handshake is used to ensure that anyone opening an association is a genuine caller, rather the someone performing a 'syn-flood' type of DoS attack.
- Cookies are used to defer commitment of resources at the responding SCTP node until the handshake is completed.
- Verification Tags are used to prevent insertion of extraneous packets into the flow of an established association.

Reliability Options

SCTP allows data to be transmitted between two end-points (a router running NetFlow SCTP export and a collector that is receiving and acknowledging the SCTP messages) in a reliable manner. In addition to the default behavior of full reliability, SCTP can be configured for partially-reliable or unreliable transmission for applications that do not require full reliability.

When SCTP is operating in full reliability mode, it uses a selective-acknowledgment scheme to guarantee the ordered delivery of messages. The SCTP protocol stack buffers messages until their receipt has been acknowledged by the receiving end-point. (collector). SCTP has a congestion control mechanism that can be used to limit how much memory is consumed by SCTP for buffering packets.

If a stream is specified as unreliable, then the packet is simply sent once and not buffered on the exporter. If the packet is lost enroute to the receiver, the exporter cannot retransmit it.

When a stream is specified as partially-reliable a limit is placed on how much memory should be dedicated to storing un-acknowledged packets. The limit on how much memory should be dedicated to storing unacknowledged packets is configurable by means of the **buffer-limit** *limit* command. If the limit on how much memory should be dedicated to storing unacknowledged packets is exceeded and the router attempts to buffer another packet, the oldest unacknowledged packet is discarded. When SCTP discards the oldest unacknowledged packet, a message called a forward-tsn (transmit sequence number) is sent to the collector to indicate that this packet will not be received. This prevents NetFlow from consuming all the free memory on a router when a situation has arisen which requires many packets to be buffered, for example when SCTP is experiencing long response times from an SCTP peer connection.

When SCTP is operating in partially reliable mode, the limit on how much memory should be dedicated to storing un-acknowledged packets should initially be set as high as possible. The limit can be reduced if other processes on the router begin to run out of memory. Deciding on the best value for the limit involves a trade-off between avoiding starving other processes of the memory that they require to operate and dropping SCTP messages that have not been acknowledged by the collector.

Unreliable SCTP can be used when the collector that you are using doesn’t support UDP as a transport protocol for receiving NetFlow export datagrams and you do not want to allocate the resources on your router required to provide reliable, or partially reliable, SCTP connections.

Congestion Avoidance

SCTP uses congestion avoidance algorithms that are similar to those for TCP. An SCTP end-point advertises the size of its receive window (rWnd) to ensure that a sender cannot flood it with more messages than it can store in its input queues.

Each SCTP sender also maintains a congestion window (cWnd), which determines the number of unacknowledged packets that can be outstanding at a given time. SCTP uses the same 'slow-start' algorithm as TCP, in which it starts with a small cWnd and gradually increases it until it reaches its optimum size.

Whenever a packet isn't acknowledged within the given timeout period, the value of cWnd is halved. This method of congestion avoidance is known as added increase / multiplicative decrease and has been shown to be the most effective congestion avoidance algorithm in most circumstances.

SCTP also employs the fast-retransmit algorithm whereby it retransmits a message if it receives acknowledgments from four messages which were sent after the message in question. This is preferable to waiting for the timeout period to elapse and triggering a retransmit of the message.

Options for Backup Collectors

You can configure a backup collector for SCTP. It is used as a message destination in the event that the primary collector becomes unavailable. When connectivity with the primary collector has been lost, and a backup

collector is configured, SCTP begins using the backup collector. The default period of time that SCTP waits until it starts using the backup collector is 25 milliseconds (msec). You can configure a different value for interval with the **fail-over** *time* command.

The router sends periodic SCTP heartbeat messages to the SCTP collectors that you have configured. The router uses the SCTP heartbeat message acknowledgements from the collectors to monitor the status of each collector. This allows an application, such as NetFlow, to be quickly informed when connectivity to a collector is lost.

You can configure SCTP backup in fail-over or redundant mode. When the router is configured with SCTP backup in fail-over mode, the router waits to activate the association with the backup collector until the router has not received acknowledgements for the SCTP heartbeat messages from the primary collector for the time specified by the **fail-over** *time* command (or the default of 25 msec if this parameter has not been modified).

Note SCTP retransmits messages that have not been acknowledged three times. The router will initiate fail-over after three retransmissions of the same message are not acknowledged by the primary collector.

When the router is configured with SCTP backup in redundant mode, the router activates the association with the backup collector immediately, and if NetFlow v9 export is configured the router sends the (options) templates in advance. The router will not start sending other SCTP messages to a backup collector in redundant mode until the router has not received acknowledgments for the SCTP heartbeat messages from the primary collector for the time specified by the **fail-over** *time* command. Fail-over mode is the preferred method when the backup collector is on the end of an expensive lower-bandwidth link such as ISDN.

During the time that SCTP is using the backup collector, SCTP continues to try to restore the association with the primary collector. This goes on until connectivity is restored or the primary SCTP collector is removed from the configuration.

When connectivity to the primary collector is available again, the router waits for a period of time before reverting to using it as the primary destination. You configure the value of the period of time that SCTP waits until reverting to the primary collector with the **restore-time** *time* command. The default period of time that SCTP waits until it reverts to the primary collector is 25 sec.

Under either fail-over mode any records which have been queued between losing connectivity with the primary destination and establishing the association with the backup collector might be lost. A count is maintained of how many records were lost. It can be viewed with the **show ip flow export sctp verbose** command.

To avoid a flapping SCTP association with a collector (the SCTP association goes up and down in quick succession), the time period configured with the **restore-time** *time* command should be greater than the period of a typical connectivity problem. For example, your router is configured to use IP fast convergence for its routing table and you have a LAN interface that is going up and down repeatedly (flapping). That causes the IP route to the primary collector to be added and removed from the routing table repeatedly (route flapping) every 2000 msec (2 sec). you need to configure the restore time for a value greater than 2000 msecs.

The backup connection uses stream 0 for sending templates, options templates, and option data record. The data stream(s) inherit the reliability settings of the primary connection.

Export to Multiple Collectors

You can configure your networking device to export NetFlow data to a maximum of two export destinations (collectors) per cache (main and aggregation caches), using any combination of UDP and SCTP. A destination is identified by a unique combination of hostname or IP address and port number or port type. The table below shows examples of permitted multiple NetFlow export destinations for each cache.

Table 55: Examples of Permitted Multiple NetFlow Export Destinations for Each Cache

First Export Destination	Second Export Destination
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *10.25.89.32 285 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *172.16.89.32 100 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *172.16.89.32 285 udp*
ip flow-export *10.25.89.32 100 udp*	**ip flow-export** *10.25.89.32 100 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *10.25.89.32 285 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *172.16.89.32 100 sctp*
ip flow-export *10.25.89.32 100 sctp*	**ip flow-export** *172.16.89.32 285 sctp*

The most common use of the multiple-destination feature is to send the NetFlow cache entries to two different destinations for redundancy. Therefore, in most cases the second destination IP address is not the same as the first IP address. The port numbers can be the same when you are configuring two unique destination IP addresses. If you want to configure both instances of the command to use the same destination IP address, you must use unique port numbers. You receive a warning message when you configure the two instances of the command with the same IP address. The warning message is, "%Warning: Second destination address is the same as previous address <ip-address>".

SCTP Support For Export Formats

SCTP based reliable transport is available for all NetFlow export formats: Versions 1, 5, 8 and 9.

How to Configure NetFlow Reliable Export with SCTP

You can configure two primary SCTP export destinations (collectors) and two backup SCTP export destinations for each NetFlow cache (main cache and aggregation caches). The backup SCTP export destinations inherit the reliability characteristics of the primary SCTP export destination. For example, if you configure partial reliability with a buffer limit of 2000 packets for the primary SCTP export destination, the backup SCTP destination also uses partial reliability and a buffer limit of 2000 packets.

You can use several permutations when you configure NetFlow Reliable Export With SCTP. The most basic configuration requires only one SCTP export destination. The other tasks below explain how to configure some of the more common permutations of NetFlow Reliable Export With SCTP.

Configuring NetFlow SCTP Export for One Export Destination

This is the most basic NetFlow SCTP export configuration. This NetFlow SCTP export configuration uses full reliability.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **end**
5. **show ip flow export sctp** verbose

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 5 **show ip flow export sctp** verbose
Displays the status and statistics for NetFlow SCTP export. Reliability is set to the default of full.

Example:

```
Router# show ip flow export sctp verbose
```

```
IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
4 flows exported in 4 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Configuring NetFlow SCTP Export for One Export Destination with Partial Reliability

This NetFlow SCTP export configuration uses partial reliability.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **reliability partial buffer-limit** *limit*
5. **end**
6. **show ip flow export sctp** verbose

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **reliability partial buffer-limit** *limit*
Configures partial reliability for this SCTP export destination and sets the packet buffer limit to 3000.

Example:

```
Router(config-flow-export-sctp)# reliability partial buffer-limit 3000
```

Step 5 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 6 **show ip flow export sctp** verbose
Displays the status and statistics for NetFlow SCTP export. Reliability is now set to partial.

Example:

```
Router# show ip flow export sctp verbose

Pv4 main cache exporting to 172.16.12.200, port 100, partial
status: connected
backup mode: redundant
11 flows exported in 11 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Configuring NetFlow SCTP Export for One Export Destination with No Reliability

Reliability is disabled in this NetFlow SCTP export configuration.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **reliability none**
5. **end**
6. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **reliability none**
Configures partial reliability for this SCTP export destination and sets the packet buffer limit to none.

Example:

```
Router(config-flow-export-sctp)# reliability none
```

Step 5 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 6 **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow SCTP export. Reliability is now set to none.

Example:

```
Router# show ip flow export sctp verbose

Pv4 main cache exporting to 172.16.12.200, port 100, none
status: connected
backup mode: redundant
15 flows exported in 15 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Configuring NetFlow SCTP Export for One Export Destination and One Backup Export Destination

This NetFlow SCTP export configuration uses full reliability, a backup SCTP export destination, and redundant mode backup.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **backup destination** [*ip-address* | *hostname*] *sctp-port*
5. **end**
6. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **backup destination** [*ip-address* | *hostname*] *sctp-port*
Configures an SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.247.198 200
```

Step 5 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 6 **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow SCTP export. Backup mode is redundant. The association with the SCTP backup export destination is active (connected). The SCTP backup export destination is not being used because the primary export destination is still active (connected).

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
35 flows exported in 35 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for One Export Destination and One Backup Exp Dest With Fail-Over Mode Backup

Perform this task to configure NetFlow SCTP export for one export and one backup destination with fail-over mode backup.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

This NetFlow SCTP export configuration uses full reliability, a backup SCTP export destination, and fail-over mode backup.

Note The backup fail-over and restore times are modified here so that you can see an example of how to configure these commands. The values used in this example might not be suitable for your network. If you want to override the default values for the fail-over and restore times you need to analyze the performance of your network and the collector that you are using to determine values that are appropriate for your network.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **backup destination** [*ip-address* | *hostname*] *sctp-port*
5. **backup mode fail-over**
6. **backup fail-over** *fail-over-time*
7. **backup restore-time** *restore-time*
8. **end**
9. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **backup destination** [*ip-address* | *hostname*] *sctp-port*
Configures an SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.247.198 200
```

Step 5 **backup mode fail-over**
Configures the router to fail-over mode for the backup export destination.

Example:

```
Router(config-flow-export-sctp)# backup mode fail-over
```

Step 6 **backup fail-over** *fail-over-time*
The length of time that the router will wait until failing over to the backup SCTP export destination has been increased to 3500 msec.

Example:

```
Router(config-flow-export-sctp)# backup fail-over 3500
```

Step 7 **backup restore-time** *restore-time*
The length of time that the router will wait until reverting to the primary SCTP export destination has been increased to 1500 msecs.

Example:

```
Router (config)# backup restore-time 1500
```

Step 8 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 9 **show ip flow export sctp verbose**

Displays the status and statistics for NetFlow SCTP export. Backup mode is fail-over. The association with the SCTP backup export destination is not active (not connected) because NetFlow SCTP export waits to activate the association with the backup destination until the primary export destination is no longer available.

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: fail-over
114 flows exported in 93 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 3500 milli-seconds
restore time:   1500 seconds
backup: 192.168.247.198, port 200
   status: not connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for Two Export Destinations and Two Backup Export Destinations

This configuration is the most basic SCTP export configuration that uses multiple export destinations. You can configure a maximum of two export destinations for every NetFlow cache.

Each SCTP export destination has its own area in the configuration file for the options that you can configure for it such as fail-over mode, fail-over timers and reliability. Therefore you must make certain that the last SCTP export destination that you entered in the router's configuration is the SCTP export destination that you want to modify.

For example, if you enter these commands in this order:

- **ip flow-export destination** *172.16.12.200 100* **sctp**
- **ip flow-export destination** *172.16.45.57 100* **sctp**
- **backup destination** *192.168.100.2 200*

The **backup destination** *192.168.100.2 200* is assigned to the **ip flow-export destination** *172.16.45.57 100* **sctp**command.

To change the SCTP export destination that you are modifying, reenter the command line for the SCTP export destination that you want to modify.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **backup destination** [*ip-address* | *hostname*] *sctp-port*
5. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
6. **backup destination** [*ip-address* | *hostname*] *sctp-port*
7. **end**
8. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **backup destination** [*ip-address* | *hostname*] *sctp-port*
Configures an SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.247.198 200
```

Step 5 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures a second export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.45.57 100 sctp
```

Step 6 **backup destination** [*ip-address* | *hostname*] *sctp-port*

Configures a second SCTP backup destination using SCTP on port 200.

Example:

```
Router(config-flow-export-sctp)# backup destination 192.168.100.2 200
```

Step 7 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 8 **show ip flow export sctp verbose**
Displays the status and statistics for the two primary and backup NetFlow SCTP export destinations. Reliability is set to the default of full.

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
219 flows exported in 176 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 3500 milli-seconds
restore time:   10 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
IPv4 main cache exporting to 172.16.45.57, port 100, full
status: connected
backup mode: redundant
66 flows exported in 47 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 1
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for One Fully Reliable and One Partially Reliable Export Destination

This SCTP export configuration uses two SCTP export destinations. One of the export destinations uses full reliability and the other export destination uses partial reliability.

Before You Begin

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
4. **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
5. **reliability partial buffer-limit** *limit*
6. **end**
7. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.12.200 100 sctp
```

Step 4 **ip flow-export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures a second export destination using SCTP on port 100.

Example:

```
Router (config)# ip flow-export destination 172.16.45.57 100 sctp
```

Step 5 **reliability partial buffer-limit** *limit*
Configures partial reliability for this SCTP export destination and sets the packet buffer limit to 3000.

Example:

```
Router(config-flow-export-sctp)# reliability partial buffer-limit 3000
```

Step 6 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 7 **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow export with SCTP. Reliability is set to full for SCTP export destination 172.16.12.200 and to partial SCTP export destination 172.16.45.57.

Example:

```
Router# show ip flow export sctp verbose

IPv4 main cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
229 flows exported in 186 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 3500 milli-seconds
restore time:   10 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
IPv4 main cache exporting to 172.16.45.57, port 100, partial
status: connected
backup mode: redundant
76 flows exported in 57 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 1
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Configuring NetFlow SCTP Export for the NetFlow Source-Prefix Aggregation Cache

This SCTP export example shows how to configure NetFlow SCTP export for the NetFlow source prefix aggregation cache. You can configure a maximum of two export destinations for every NetFlow cache.

When you enter NetFlow aggregation cache configuration mode in the router the current router prompt changes to reflect this mode.

For example, if the current router prompt is, Router(config)# and you enter the **ip flow-aggregation cache prefix** command, the router prompt is changed to the NetFlow aggregation cache configuration prompt of Router(config-flow-cache)#.

You need to pay close attention when you are configuring NetFlow SCTP export options for NetFlow aggregation caches because the NetFlow aggregation cache configuration prompt is changed to the NetFlow SCTP export prompt when you enter a NetFlow SCTP export command in NetFlow aggregation cache configuration mode, even though you are still working in NetFlow aggregation cache configuration mode.

For example, if your current prompt is the NetFlow aggregation cache configuration prompt, Router(config-flow-cache)#, and you enter the **export destination** *172.16.12.200 100* **sctp** command, the router prompt will change to the NetFlow SCTP export configuration mode prompt, Router(config-flow-export-sctp)#. The NetFlow SCTP export commands that you configure are assigned to the NetFlow aggregation cache that you are modify with NetFlow SCTP export options.

Use the configuration in the Configuration Examples for NetFlow Reliable Export With SCTP, on page 313 to practice using the different configuration modes

Prerequisites

You must have NetFlow enabled on at least one interface in your router before you can export NetFlow data.

You must have a NetFlow collector in your network that supports NetFlow SCTP export.

SCTP Export for NetFlow Aggregation Caches

All of the NetFlow SCTP options that are available for the main NetFlow cache are also available in NetFlow Aggregation cache mode.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-aggregation cache aggregation-cache-type**
4. **enable**
5. **export destination** [*ip-address* | *hostname*] *port* **sctp**
6. **end**
7. **show ip flow export sctp verbose**

DETAILED STEPS

Step 1 **enable**
Enters privileged EXEC mode.

Example:

```
Router> enable
```

Step 2 **configure terminal**
Enters global configuration mode.

Example:

```
Router# configure terminal
```

Step 3 **ip flow-aggregation cache aggregation-cache-type**
Enters NetFlow aggregation cache mode for the cache type.

Example:

```
Router (config)# ip flow-aggregation cache source-prefix
```

Step 4 **enable**
Activates the NetFlow aggregation cache.

Example:

```
Router(config-flow-cache)# enable
```

Step 5 **export destination** [*ip-address* | *hostname*] *port* **sctp**
Configures an export destination using SCTP for the aggregation cache.

Example:

```
Router (config-flow-cache)# export destination 172.16.12.200 100 sctp
```

Step 6 **end**
Returns to privileged EXEC mode.

Example:

```
Router(config-flow-export-sctp)# end
```

Step 7 **show ip flow export sctp verbose**
Displays the status and statistics for NetFlow export with SCTP.

Example:

```
Router# show ip flow export sctp verbose

source-prefix cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
0 flows exported in 0 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
```

Verifying NetFlow Reliable Export With SCTP

The **show ip flow export sctp** [**verbose**]command provides information on the status and statistics of the options that you have configured for the NetFlow Reliable Export With SCTP feature.

Cisco IOS also provides commands for monitoring and troubleshooting the status and statistics for all of the SCTP features (including NetFlow Reliable Export With SCTP) that you have configured on the networking device. Refer to the Stream Control Transmission Protocol (SCTP) , Release 2 configuration guide http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122newft/122t/122t8/ft_sctp2.htm for more information on interpreting the output from these commands, and the other commands that are available for monitoring and troubleshooting SCTP.

SUMMARY STEPS

1. **show ip sctp association list**
2. **show ip sctp association parameters** *association-id*
3. **show ip sctp errors**
4. **show ip sctp instances**
5. show ip sctp statistics

DETAILED STEPS

Step 1 **show ip sctp association list**
Shows the list of SCTP associations.

Example:

```
Router# show ip sctp association list
** SCTP Association List **
AssocID: 0,  Instance ID: 0
Current state: ESTABLISHED
Local port: 51882, Addrs: 172.16.6.2
Remote port: 100, Addrs: 172.16.12.200
AssocID: 1,  Instance ID: 1
Current state: ESTABLISHED
Local port: 59004, Addrs: 172.16.6.2
Remote port: 200, Addrs: 192.168.247.198
```

Step 2 **show ip sctp association parameters** *association-id*
Displays the current parameters for the association ID.

Example:

```
Router# show ip sctp association parameters 0
** SCTP Association Parameters **
AssocID: 0  Context: 1  InstanceID: 0
Assoc state: ESTABLISHED  Uptime: 00:19:44.504
Local port: 51882
Peers Adaption layer indication is NOT set
Local addresses: 172.16.6.2
Remote port: 100
Primary dest addr: 172.16.12.200
Effective primary dest addr: 172.16.12.200
Destination addresses:
```

```
172.16.12.200:   State:  ACTIVE(CONFIRMED)
  Heartbeats:  Enabled   Timeout: 500 ms
  RTO/RTT/SRTT: 5000/0/3 ms   TOS: 0  MTU: 1500
  cwnd: 3000  ssthresh: 9000  outstand: 0
  Num retrans: 0  Max retrans: 2  Num times failed: 0
Local vertag: DAF7029F  Remote vertag: A3923131
Num inbound streams: 20  outbound streams: 20
Max assoc retrans: 2  Max init retrans: 2
CumSack timeout: 200 ms  Bundle timeout: 100 ms
Min RTO: 5000 ms  Max RTO: 5000 ms
Max Init RTO (T1): 1000 ms
LocalRwnd: 9000  Low: 9000   RemoteRwnd: 9000  Low: 8936
Congest levels: 0  current level: 0  high mark: 1
```

Step 3 **show ip sctp errors**
Shows any SCTP errors that have occurred.

Example:

```
Router# show ip sctp errors
** SCTP Error Statistics **
No SCTP errors logged.
```

Step 4 **show ip sctp instances**
Shows the details and status for the SCTP instances.

Example:

```
Router# show ip sctp instances
** SCTP Instances **
Instance ID: 0  Local port: 51882  State: available
Local addrs: 172.16.6.2
Default streams inbound: 20  outbound: 20
Adaption layer indication is not set
  Current associations:  (max allowed: 6)
  AssocID: 0  State: ESTABLISHED  Remote port: 100
    Dest addrs: 172.16.12.200
Instance ID: 1  Local port: 59004  State: available
Local addrs: 172.16.6.2
Default streams inbound: 20  outbound: 20
Adaption layer indication is not set
  Current associations:  (max allowed: 6)
  AssocID: 1  State: ESTABLISHED  Remote port: 200
    Dest addrs: 192.168.247.198
```

Step 5 show ip sctp statistics
Shows the SCTP overall statistics:

Example:

```
Router# show ip sctp statistics
** SCTP Overall Statistics **
Control Chunks
  Sent: 615  Rcvd: 699
Data Chunks Sent
  Total: 57  Retransmitted: 0
  Ordered: 57  Unordered: 0
  Total Bytes: 3648
Data Chunks Rcvd
  Total: 0  Discarded: 0
  Ordered: 0  Unordered: 0
  Total Bytes: 0
  Out of Seq TSN: 0
SCTP Dgrams
```

```
  Sent: 671  Rcvd: 699
ULP Dgrams
  Sent: 57  Ready: 0  Rcvd: 0
Additional Stats
  Assocs Currently Estab: 2
  Active Estab: 2  Passive Estab: 0
  Aborts: 0  Shutdowns: 0
  T1 Expired: 1  T2 Expired: 0
```

Configuration Examples for NetFlow Reliable Export With SCTP

The following example includes these NetFlow accounting and NetFlow SCTP export features:

- NetFlow ingress and egress accounting
- Multiple SCTP export destinations for the Main NetFlow cache with backup destinations
- Multiple SCTP export destinations for the NetFlow protocol-port aggregation cache using partial reliability and fail-over mode backup destinations
- Multiple SCTP export destinations for the NetFlow bgp-nexthop-tos aggregation cache with reliability disabled and redundant mode backup destinations

```
Router# show running-config
.
.
.
interface Ethernet0/0.1
 ip address 172.16.6.2 255.255.255.0
 ip flow ingress
!
!
interface Ethernet1/0.1
 ip address 172.16.7.1 255.255.255.0
 ip flow egress
!
ip flow-export destination 172.16.45.57 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.100.2 200
!
ip flow-export destination 172.16.12.200 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.247.198 200
!
ip flow-aggregation cache protocol-port
 export destination 172.16.12.200 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.247.198 200
 backup mode fail-over
 export destination 172.16.45.57 100 sctp
 reliability partial buffer-limit 3000
 backup destination 192.168.100.2 200
 backup mode fail-over
 enabled
!
ip flow-aggregation cache bgp-nexthop-tos
 export version 9
 export destination 172.16.12.200 100 sctp
 backup destination 192.168.247.198 200
 export destination 172.16.45.57 100 sctp
 backup destination 192.168.100.2 200
```

```
 enabled
!
```

The display output of the **show ip flow export sctp verbose** command shows the status and statistics for this configuration example:

```
Router# show ip flow export sctp verbose
IPv4 main cache exporting to 172.16.45.57, port 100, partial
status: connected
backup mode: redundant
104 flows exported in 84 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 2
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
IPv4 main cache exporting to 172.16.12.200, port 100, partial
status: connected
backup mode: redundant
104 flows exported in 84 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 1
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
protocol-port cache exporting to 172.16.12.200, port 100, partial
status: connected
backup mode: fail-over
19 flows exported in 18 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
protocol-port cache exporting to 172.16.45.57, port 100, partial
status: connected
backup mode: fail-over
15 flows exported in 15 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
bgp-nexthop-tos cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
20 flows exported in 10 sctp messages.
0 packets dropped due to lack of SCTP resources
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.247.198, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
bgp-nexthop-tos cache exporting to 172.16.45.57, port 100, full
status: connected
backup mode: redundant
20 flows exported in 10 sctp messages.
0 packets dropped due to lack of SCTP resources
```

```
fail-over time: 25 milli-seconds
restore time:   25 seconds
backup: 192.168.100.2, port 200
   status: connected
   fail-overs: 0
   0 flows exported in 0 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	Cisco IOS NetFlow Overview
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	Getting Started with Configuring NetFlow and NetFlow Data Export
Tasks for configuring NetFlow to capture and export network traffic data	Configuring NetFlow and NetFlow Data Export
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring Random Sampled NetFlow	Using NetFlow Filtering or Sampling to Select the Network Traffic to Track
Tasks for configuring NetFlow aggregation caches	Configuring NetFlow Aggregation Caches
Tasks for configuring NetFlow BGP next hop support	Configuring NetFlow BGP Next Hop Support for Accounting and Analysis
Tasks for configuring NetFlow multicast support	Configuring NetFlow Multicast Accounting
Tasks for detecting and analyzing network threats with NetFlow	Detecting and Analyzing Network Threats With NetFlow
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	NetFlow Layer 2 and Security Monitoring Exports
Tasks for configuring the SNMP NetFlow MIB	Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data

Related Topic	Document Title
Tasks for configuring the NetFlow MIB and Top Talkers feature	Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	Cisco CNS NetFlow Collection Engine Documentation

Standards

Standards	Title
No new or modified standards are supported by this feature, and support for existing standards has not been modified by this feature.	--

MIBs

MIBs	MIBs Link
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
RFC 3954	Cisco Systems NetFlow Services Export Version 9
RFC2690	Stream Control Transmission Protocol
RFC 3578	Stream Control Transmission Protocol-Partial Reliability Extension

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for NetFlow Reliable Transport Using SCTP

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 . An account on Cisco.com is not required.

Table 56: Feature Information for NetFlow Reliable Transport Using SCTP

Feature Name	Releases	Feature Configuration Information
NetFlow Reliable Export With SCTP	12.4(4)T	The NetFlow Reliable Export With SCTP feature provides a more robust and flexible method for exporting NetFlow data to collectors than UDP, which was the only transport option prior to the introduction of this feature. NetFlow Reliable Export With SCTP has the following benefits: • Backup destinations--You can configure backup destinations for every SCTP export destination. The backup destinations can use redundant mode (always connected) and fail-over mode (connect as required). Fail-over mode is more suitable for backup destinations that are reachable over expensive dial-up links such as ISDN. • Reliability--NetFlow SCTP provides a very reliable level of transport that has error correction and flow control. You can modify the level of reliability for each SCTP export destination depending on the importance of the data that you are exporting. The following commands were introduced or modified by this feature: **ip flow export**, **show ip flow export**, and **export**.

Glossary

CEF --Cisco Express Forwarding. A Layer 3 IP switching technology that optimizes network performance and scalability for networks with large and dynamic traffic patterns.

BGP --Border Gateway Protocol. Interdomain routing protocol that replaces Exterior Border Gateway Protocol (EBGP). A BGP system exchanges reachability information with other BGP systems. BGP is defined by RFC 1163.

BGP next hop --IP address of the next hop to be used to reach a certain destination.

data record --Provides information about an IP flow that exists on the device that produced an export packet. Each group of data records (meaning each data flowset), refers to a previously transmitted template ID, which can be used to parse the data within the records.

dCEF --distributed Cisco Express Forwarding. A type of CEF switching in which line cards (such as Versatile Interface Processor (VIP) line cards) maintain identical copies of the forwarding information base (FIB) and adjacency tables. The line cards perform the express forwarding between port adapters; this relieves the Route Switch Processor of involvement in the switching operation.

export packet --A type of packet built by a device (for example, a router) with NetFlow services enabled. The packet is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information on IP flows).

fast switching --A Cisco feature in which a route cache is used to expedite packet switching through a router.

flow --A unidirectional stream of packets between a given source and destination, each of which is defined by a network-layer IP address and transport-layer source and destination port numbers.

flowset --A collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two different types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

NetFlow --A Cisco IOS application that provides statistics on packets flowing through the router. It is emerging as a primary network accounting and security technology.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--A Cisco application that is used with NetFlow on Cisco routers and Catalyst 5000 series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means of carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

options data record --A special type of data record used in the NetFlow process. It is based on an options template and has a reserved template ID that provides information about the NetFlow process itself.

options template --A type of template record used to communicate the format of data related to the NetFlow process.

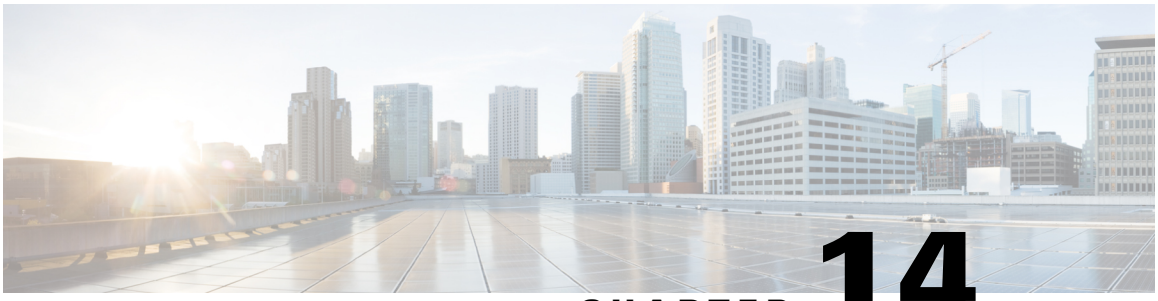
packet header --First part of an export packet. It provides basic information about the packet (such as the NetFlow version, number of records contained in the packet, and sequence numbering) so that lost packets can be detected.

SCTP --Stream Control Transmission Protocol. The Stream Control Transmission Protocol (SCTP) is a transport layer protocol defined in 2000 by the IETF Signaling Transport (SIGTRAN) working group. The protocol is defined in RFC 2960, and an introductory text is provided by RFC 3286.

template flowset --A collection of template records that are grouped in an export packet.

template ID --A unique number that distinguishes a template record produced by an export device from other template records produced by the same export device. A NetFlow Collection Engine application can receive export packets from several devices. You should be aware that uniqueness is not guaranteed across export devices. The NetFlow Collection Engine should cache the address of the export device that produced the template ID in order to enforce uniqueness.

template record --Defines the format of subsequent data records that might be received in current or future export packets. A template record within an export packet does not necessarily indicate the format of data records within that same packet. A NetFlow Collection Engine application must cache any template records received and then parse any data records it encounters by locating the appropriate template record in the cache.



CHAPTER 14

Detecting and Analyzing Network Threats With NetFlow

This document contains information about and instructions for detecting and analyzing network threats such as denial of service attacks (DoS) through the use of the following NetFlow features:

- NetFlow Layer 2 and Security Monitoring Exports--This feature improves your ability to detect and analyze network threats such as denial of service attacks (DoS) by adding 9 fields that NetFlow can capture the values from.A few examples are:
  - IP Time-to-Live field
  - Packet length field
  - ICMP type and code fields
- NetFlow Dynamic Top Talkers CLI--This feature gives you an overview of the highest volume traffic in your network by aggregating flows on a common field. For example, you can aggregate all of the flows for a destination network by aggregating them on the destination prefix. There are over 20 fields from flows that you can aggregate the highest volume traffic on. A few examples are:
  - Source or destination IP address
  - Source or destination prefix
  - Source or destination port
  - ICMP type and code
- NetFlow Top Talkers--This feature gives you a more detailed view of the traffic in your network than the NetFlow Dynamic Top Talkers CLI feature because it looks at individual flows. You use the NetFlow Dynamic Top Talkers CLI feature to quickly identify high volume traffic of interest. You use the NetFlow Top Talkers feature to obtain more detailed information on each of the flows in the high volume traffic.
- NetFlow Input Filters--This feature tracks a specific subset of NetFlow traffic for the purpose of class-based traffic analysis and monitoring. This feature is used in conjunction with the Top Talkers feature to help you focus your analysis on the traffic that might be a network threat such as a DoS attack.

- Random Sampled NetFlow--This feature is typically used for statistical sampling of network traffic for traffic engineering or capacity planning purposes. It is used in the context of monitoring and analyzing network threats because it can be used to reduce the impact on the router using NetFlow to monitor traffic that might be a network threat, such as a DoS attack.

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 Detecting and Analyzing Network Threats With NetFlow

Before you can use NetFlow for detecting and analyzing network threats you need to understand NetFlow and how to configure your router to capture IP traffic status and statistics using NetFlow. See the Cisco IOS NetFlow Overview and Configuring NetFlow and NetFlow Data Export modules for more details.

NetFlow and Cisco Express Forwarding (CEF) or distributed CEF (dCEF) must be configured on your system before you enable NetFlow.

Information About Detecting and Analyzing Network Threats With NetFlow

NetFlow Layer 2 and Security Monitoring

The Layer 2 and Layer 3 fields supported by the NetFlow Layer 2 and Security Monitoring Exports feature increase the amount of information that can be obtained by NetFlow about the traffic in your network. You can use the network traffic information for applications such as traffic engineering and usage-based billing.

Layer 3 fields captured by the NetFlow Layer 2 and Security Monitoring Exports feature improve the capabilities of NetFlow for identifying DoS attacks. Layer 2 IP header fields help identify the path that the DoS attack is taking through the network.

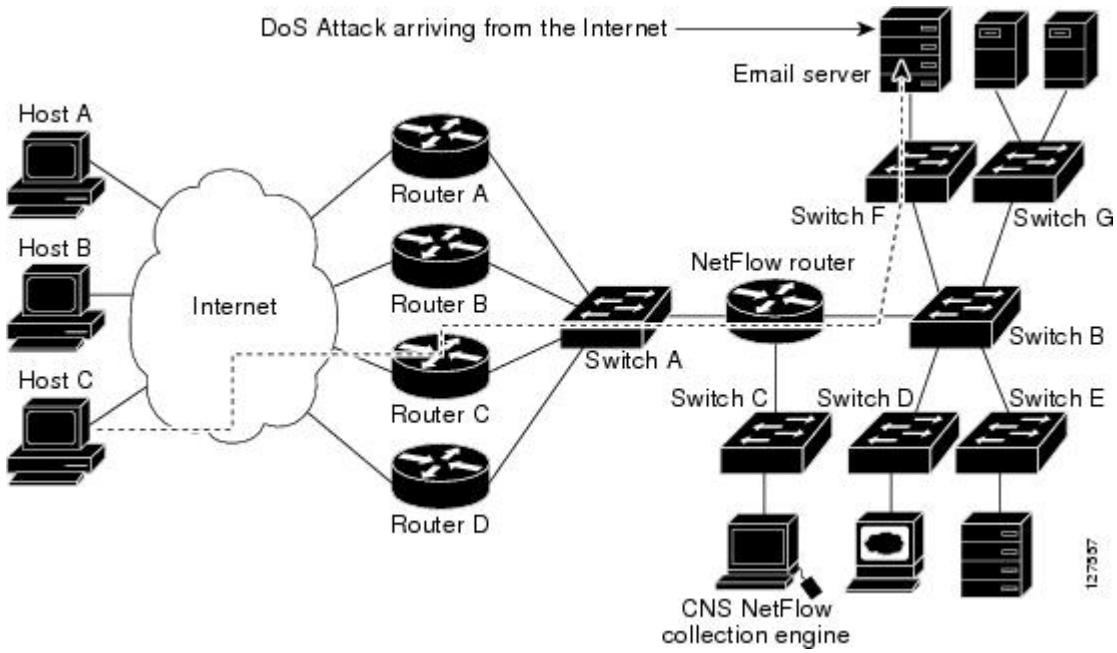
Layer 2 and Layer 3 fields are not key fields. They provide additional information about the traffic in an existing flow. Changes in the values of NetFlow key fields, such as the source IP address, from one packet to the next packet results in the creation of a new flow. For example, if the first packet captured by NetFlow has a source IP address of 10.34.0.2 and the second packet captured has a source IP address of 172.16.213.65, NetFlow will create two separate flows.

Most DoS attacks consist of an attacker sending the same type of IP datagram repeatedly, in an attempt to overwhelm target systems. In such cases, the incoming traffic often has similar characteristics, such as the same values in each datagram for one or more fields that the NetFlow Layer 2 and Security Monitoring Exports feature can capture.

The originator of DoS attacks cannot be easily identified because the IP source address of the device sending the traffic is usually forged. However, you can easily trace the traffic back through the network to the router on which it is arriving by using the NetFlow Layer 2 and Security Monitoring Exports feature to capture the MAC address and VLAN-ID fields. If the router on which traffic is arriving supports NetFlow, you can

configure the NetFlow Layer 2 and Security Monitoring Exports feature on it to identify the interface on which the traffic is arriving. The figure below shows an example of an attack in progress.

Figure 33: DoS Attack Arriving over the Internet



Note You can analyze the data captured by NetFlow directly from the router by using the **show ip cache verbose flow** command or by the Cisco Network Services (CNS) NetFlow Collector Engine.

Once you have concluded that a DoS attack is taking place by analyzing the Layer 3 fields in the NetFlow flows, you can analyze the Layer 2 fields in the flows to discover the path that the DoS attack is taking through the network.

An analysis of the data captured by the NetFlow Layer 2 and Security Monitoring Exports feature, for the scenario shown in the above figure, indicates that the DoS attack is arriving on Router C, because the upstream MAC address is from the interface that connects Router C to Switch A. It is also evident that there are no routers between the target host (the e-mail server) and the NetFlow router, because the destination MAC address of the DoS traffic that the NetFlow router is forwarding to the e-mail server is the MAC address of the e-mail server.

You can learn the MAC address that Host C is using to send traffic to Router C by configuring the NetFlow Layer 2 and Security Monitoring Exports feature on Router C. The source MAC address will be from Host C. The destination MAC address will be for the interface on the NetFlow router.

Once you know the MAC address that Host C is using and the interface on Router C on which Host C's DoS attack is arriving, you can mitigate the attack by reconfiguring Router C to block Host C's traffic. If Host C is on a dedicated interface, you can disable the interface. If Host C is using an interface that carries traffic from other users, you must configure your firewall to block Host C's traffic, but still allow the traffic from the other users to flow through Router C.

Layer 3 Information Capture Using NetFlow Layer 2 and Security Monitoring Exports

The five fields that the NetFlow Layer 2 and Security Monitoring Exports feature captures from Layer 3 IP traffic in a flow are the following:

- Internet Control Message Protocol (ICMP) type and code
- ID field
- Fragment offset
- Packet length field
- Time-to-live field

Figure 5 shows the fields in an IP packet header.

Figure 34: IP Packet Header Fields

Table 4 describes the header fields in Figure 5.

Table 57: IP Packet Header Fields

Field	Description
Version	The version of the IP protocol. If this field is set to 4, it is an IPv4 datagram. If this field is set to 6, it is an IPv6 datagram. **Note** IPv4 and IPv6 headers have different structures.
IHL (Internet Header Length)	Internet Header Length is the length of the Internet header in 32-bit word format and thus points to the beginning of the data. **Note** The minimum value for the correct header length is 5.
ToS	Type of service (ToS) provides an indication of the abstract parameters of the quality of service desired. These parameters are to be used to guide the selection of the actual service parameters when a networking device transmits a datagram through a particular network.
Total Length	Total length is the length of the datagram, measured in octets, including Internet header and data.

Field	Description
Identification (ID)	The value in the ID field is entered by the sender. All the fragments of an IP datagram have the same value in the ID field. Subsequent IP datagrams from the same sender will have different values in the ID field. Frequently, a host receives fragmented IP datagrams from several senders concurrently. Also, frequently a host receives multiple IP datagrams from the same sender concurrently. The value in the ID field is used by the destination host to ensure that the fragments of an IP datagram are assigned to the same packet buffer during the IP datagram reassembly process. The unique value in the ID field is used to prevent the receiving host from mixing together IP datagram fragments of different IP datagrams from the same sender during the IP datagram reassembly process.
Flags	A sequence of three bits is used to set and track IP datagram fragmentation parameters. The bits are: • 001—The IP datagram can be fragmented. More fragments of the current IP datagram are in transit. • 000—The IP datagram can be fragmented. This is the last fragment of the current IP datagram. • 010—The IP datagram cannot be fragmented. This is the entire IP datagram.
Fragment Offset	This field indicates where in the datagram this fragment belongs.
TTL (Time-to-Live)	This field indicates the maximum time the datagram is allowed to remain in the Internet system. If this field contains the value 0, then the datagram must be destroyed. This field is modified in Internet header processing. The TTL is measured in units of seconds, but because every module that processes a datagram must decrease the TTL by at least 1 even if it processes the datagram in less than a second, the TTL must be thought of only as an upper bound on the time a datagram can exist. The intention is to discard undeliverable datagrams and bound the maximum datagram lifetime.
Protocol	Indicates the type of transport packet included in the data portion of the IP datagram. Common values are: • 1—ICMP • 6—TCP • 17—UDP
Header checksum	A checksum on the header only. Because some header fields, such as the TTL field, change every time an IP datagram is forwarded, this value is recomputed and verified at each point that the Internet header is processed.

Field	Description
Source IP Address	IP address of the sending station.
Destination IP Address	IP address of the destination station.
Options and Padding	The options and padding may appear in datagrams. If they do appear, they must be implemented by all IP modules (host and gateways). Options and padding are always implemented in any particular datagram; transmissions are not.

Figure 6 shows the fields in an ICMP datagram.

Figure 35: ICMP Datagram

Table 5 interprets the packet format in the figure seen above. ICMP datagrams are carried in the data area of an IP datagram, after the IP header.

Table 58: ICMP Packet Format

Type	Name	Codes
0	Echo reply	0—None.
1	Unassigned	—
2	Unassigned	—

Type	Name	Codes
3	Destination unreachable	0—Network unreachable. 1—Host unreachable. 2—Protocol unreachable. 3—Port unreachable. 4—Fragmentation needed and don't fragment (DF) bit set. 5—Source route failed. 6—Destination network unknown. 7—Destination host unknown. 8—Source host isolated. 9—Communication with the destination network is administratively prohibited. 10—Communication with the destination host is administratively prohibited. 11—Destination network unreachable for ToS. 12—Destination host unreachable for ToS.
4	Source quench	0—None.
5	Redirect	0—None. 0—Redirect datagram for the network. 1—Redirect datagram for the host. 2—Redirect datagram for the ToS and network. 3—Redirect datagram for the ToS and host.
6	Alternate host address	0—Alternate address for the host.
7	Unassigned	—
8	Echo	0—None.
9	Router advertisement	0—None.
10	Router selection	0—None.
11	Time exceeded	0—Time to live exceeded in transit.
12	Parameter problem	0—Pointer indicates the error. 1—Missing a required option. 2—Inappropriate length.

Type	Name	Codes
13	Timestamp	0—None.
14	Timestamp reply	0—None.
15	Information request	0—None.
16	Information reply	0—None.
17	Address mask request	0—None.
18	Address mask reply	0—None.
19	Reserved (for security)	—
20–29	Reserved (for robustness experiment)	—
30	Trace route	—
31	Datagram conversion error	—
32	Mobile host redirect	—
33	IPv6 where-are-you	—
34	IPv6 I-am-here	—
35	Mobile registration request	—
36	Mobile registration reply	—
37–255	Reserved	—

Layer 2 Information Capture Using NetFlow Layer 2 and Security Monitoring Exports

The NetFlow Layer 2 and Security Monitoring Exports feature can capture the values of the MAC address and VLAN ID fields from flows. The two supported VLAN types are 802.1q and the Cisco Inter-Switch Link (ISL) protocol.

Layer 2 MAC Address Fields

The Layer 2 fields for which the NetFlow Layer 2 and Security Monitoring Exports feature captures the values are as follows:

- The source MAC address field from frames that are received by the NetFlow router.
- The destination MAC address field from frames that are transmitted by the NetFlow router.

- The VLAN ID field from frames that are received by the NetFlow router.
- The VLAN ID field from frames that are transmitted by the NetFlow router.

Figure 2 shows the Ethernet Type II and Ethernet 802.3 frame formats. The destination address field and the source address field in the frame formats are the MAC address values that are captured by NetFlow.

Figure 36: Ethernet Type II and 802.3 Frame Formats

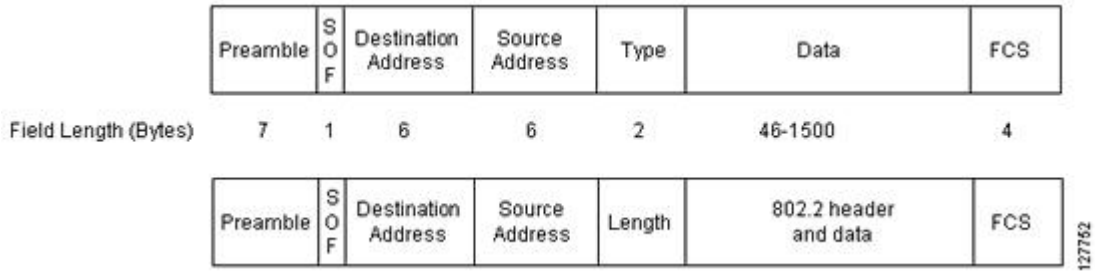


Table 1 explains the fields for the Ethernet frame formats.

Table 59: Ethernet Type II and 802.3 Frame Fields

Field	Description
Preamble	The entry in the Preamble field is an alternating pattern of 0s and 1s that communicates to receiving stations about an incoming frame. It also provides a means for the receiving stations to synchronize their clocks with the incoming bit stream.
SOF (Start of frame)	The SOF field holds an alternating pattern of 0s and 1s, ending with two consecutive 1s, indicating that the next bit is the first bit of the first byte of the destination MAC address.
Destination Address	The 48-bit destination address identifies which station on the LAN should receive the frame. The first two bits of the destination MAC address are reserved for the following special functions: • The first bit in the destination address field indicates whether the address is an individual address (0) or a group address (1). • The second bit indicates whether the destination address is globally administered (0) or locally administered (1). The remaining 46 bits form a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network.
Source Address	The 48-bit source address identifies which station transmitted the frame. The source address is always an individual address, and the leftmost bit in the Source Address field is always 0.

Field	Description
Type or Length	Type—In an Ethernet Type II frame, a part of the frame is used for the Type field. The Type field is used to identify the next layer protocol in the frame. Length—In an 802.3 Ethernet frame, a part of the frame is used for the Length field. The Length field is used to indicate the length of the Ethernet frame. The value can be from 46 to 1500 bytes.
Data or 802.2 header and data	Ethernet Type II—46 to 1500 bytes of data or 802.3/802.2—8 bytes of header and 38 to 1492 bytes of data.
FCS (Frame Check Sequence)	This field contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending station and is recalculated by the receiving station, to check for damaged frames. The FCS is generated for the destination address, source address, Type, and Data fields of the frame. The FCS does not include the data portion of the frame.

Layer 2 VLAN ID Fields

NetFlow can capture the value in the VLAN ID field for 802.1q tagged VLANs and Cisco ISL encapsulated VLANs. This section describes the two types of VLANs, 802.1q and ISL.

Note ISL and 802.1q are commonly called VLAN encapsulation protocols.

Understanding 802.1q VLANs

Devices that use 802.1q insert a four-byte tag into the original frame before it is transmitted. Figure 3 shows the format of an 802.1q tagged Ethernet frame.

Figure 37: 802.1q Tagged Ethernet Type II or 802.3 Frame

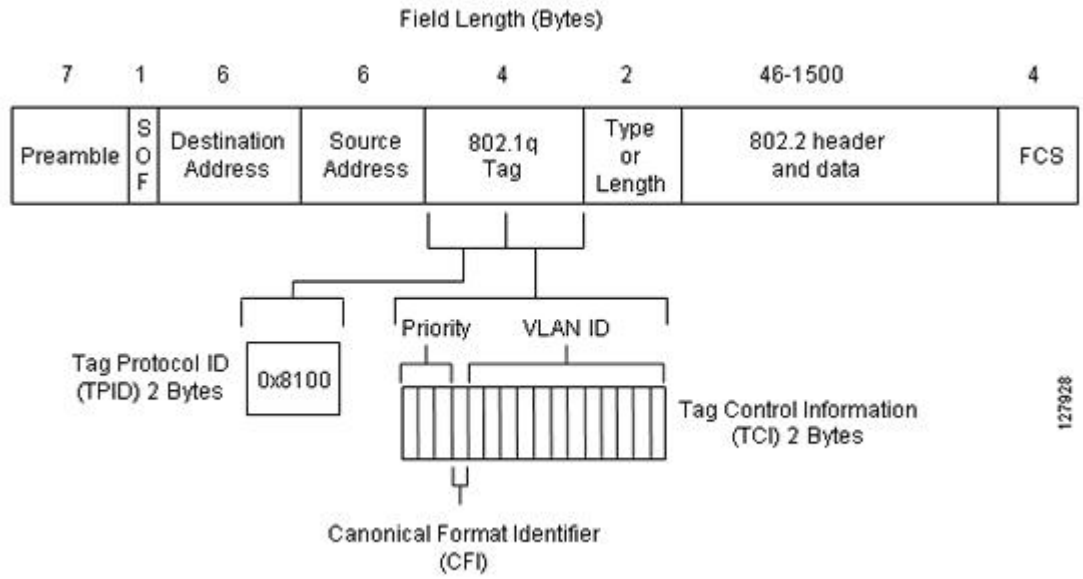


Table 2 describes the fields for 802.1q VLANs.

Table 60: 802.1q VLAN Encapsulation Fields

Field	Description
Destination Address	The 48-bit destination address identifies which stations on the LAN should receive the frame. The first two bits of the destination MAC address are reserved for the following special functions: • The first bit in the destination address field indicates whether the address is an individual address (0) or a group address (1). • The second bit indicates whether the destination address is globally administered (0) or locally administered (1). The remaining 46 bits form a uniquely assigned value that identifies a single station, a defined group of stations, or all stations on the network.
Source Address	The 48-bit source address identifies which station transmitted the frame. The source address is always an individual address, and the leftmost bit in the Source Address field is always 0.

Field	Description
Type or Length	Type—In an Ethernet Type II frame, a part of the frame is used for the Type field. The Type field is used to identify the next layer protocol in the frame. Length—In an 802.3 Ethernet frame, a part of the frame is used for the Length field. The Length field is used to indicate the length of the Ethernet frame. The value can be from 46 to 1500 bytes.
Data or 802.2 header and data	Ethernet Type II—46 to 1500 bytes of data or 802.3/802.2—8 bytes of header and 38 to 1492 bytes of data.
FCS (Frame Check Sequence)	This field contains a 32-bit cyclic redundancy check (CRC) value, which is created by the sending station and is recalculated by the receiving station, to check for damaged frames. The FCS is generated for the destination address, source address, Type, and Data fields of the frame. The FCS does not include the data portion of the frame.
Tag Protocol ID (TPID)	This 16-bit field is set to a value of 0x8100 to identify the frame as an IEEE 802.1q tagged frame.
Priority	This 3-bit field refers to the 802.1p priority. It is also known as user priority. It indicates the frame priority level used for prioritizing traffic and can represent levels 0–7.
Tag Control Information	This 2-byte Tag Control Information field consists of the following two subfields: • Canonical Format Indentifier (CFI)—If the value of this 1-bit field is 1, the MAC address is in noncanonical format. If the value of this field is 0, the MAC address is in canonical format. • VLAN ID—This 12-bit field uniquely identifies the VLAN to which the frame belongs. It can have a value from 0 to 4095.

Cisco ISL VLANs

ISL is a Cisco-proprietary protocol for encapsulating frames on a VLAN trunk. Devices that use ISL add an ISL header to the frame. This process is known as VLAN encapsulation. 802.1Q is the IEEE standard for tagging frames on a VLAN trunk. Figure 4 shows the format of a Cisco ISL-encapsulated Ethernet frame.

Figure 38: Cisco ISL Tagged Ethernet Frame

#of bits in the field	40	4	4	48	16	24	24	15	1	16	16	1 to 24575 bytes	32
Field Name	DA	TYPE	USER	SA	LEN	AAAA03(SNAP)	HSA	VLAN	BPDU	INDEX	RES	Enscapsulated FRAME	FCS

127755

Table 3 describes the fields for 802.1q VLANs.

Table 61: ISL VLAN Encapsulation

Field	Description
DA (destination address)	This 40-bit field is a multicast address and is set at 0*n*01-00-0c-00-00 or 0*n*03-00-0c-00-00. The receiving host determines that the frame is encapsulated in ISL by reading the 40-bit DA field and matching it with one of the two ISL multicast addresses.
TYPE	This 4-bit field indicates the type of frame that is encapsulated and to indicate alternative encapsulations. TYPE codes: • 0000—Ethernet • 0001—Token Ring • 0010—FDDI • 0011—ATM
USER	This 4-bit field is used to extend the meaning of the Frame TYPE field. The default USER field value is 0000. For Ethernet frames, the USER field bits 0 and 1 indicate the priority of the packet as it passes through the switch. Whenever traffic can be handled more quickly, the packets with this bit set should take advantage of the quicker path. However, such paths are not required. USER codes: • *xx*00—Normal priority • *xx*01—Priority 1 • *xx*10—Priority 2 • *xx*11—Highest priority
SA	This 48-bit field is the source address field of the ISL packet. It should be set to the 802.3 MAC address of the switch port transmitting the frame. The receiving device can ignore the SA field of the frame.

Field	Description
LEN	This 16-bit value field stores the actual packet size of the original packet. The LEN field represents the length of the packet in bytes, excluding the DA, TYPE, USER, SA, LEN, and FCS fields. The total length of the excluded fields is 18 bytes, so the LEN field represents the total length minus 18 bytes.
AAAA03(SNAP)	The AAAA03 Subnetwork Access Protocol (SNAP) field is a 24-bit constant value of 0*x*AAAA03.
HSA	This 24-bit field represents the upper three bytes (the manufacturer's ID portion) of the SA field. It must contain the value 0*x*00-00-0C.
VLAN	This 15-bit field is the virtual LAN ID of the packet. This value is used to mark frames on different VLANs.
BPDU	The bit in the bridge protocol data unit (BPDU) field is set for all BPDU packets that are encapsulated by the ISL frame. The BPDUs are used by the spanning tree algorithm to learn information about the topology of the network. This bit is also set for Cisco Discovery Protocol and VLAN Trunk Protocol (VTP) frames that are encapsulated.
INDEX	This 16-bit field indicates the port index of the source of the packet as it exits the switch. It is used for diagnostic purposes only, and may be set to any value by other devices. It is ignored in received packets.
RES	This 16-bit field is used when Token Ring or FDDI packets are encapsulated with an ISL frame.
Encapsulated FRAME	This field contains the encapsulated Layer 2 frame.
FCS	The FCS field consists of 4 bytes. It includes a 32-bit CRC value, which is created by the sending station and is recalculated by the receiving station, to check for damaged frames. The FCS covers the DA, SA, Length/Type, and Data fields. When an ISL header is attached to a Layer 2 frame, a new FCS is calculated over the entire ISL packet and added to the end of the frame. **Note** The addition of the new FCS does not alter the original FCS that is contained within the encapsulated frame.

NetFlow Top Talkers

The usual implementation of NetFlow exports NetFlow data to a collector. The NetFlow Top Talkers features can be used for security monitoring or accounting purposes for top talkers, and matching and identifying key traffic in your network. These features are also useful for a network location where a traditional NetFlow export operation is not possible. The NetFlow Top Talkers features do not require a collector to obtain information regarding flows. Instead, the NetFlow data is displayed on the router when the NetFlow Dynamic Top Talkers CLI **show ip flow top** command, or the NetFlow Top Talkers **show ip flow top-talkers**is used.

Comparison of the NetFlow Dynamic Top Talkers CLI and NetFlow Top Talkers Features

There are two very similar NetFlow features that can be used for monitoring the highest volume traffic in your network. The feature names are:

NetFlow Dynamic Top Talkers CLI

This feature was introduced in 12.4(4)T. The NetFlow Dynamic Top Talkers CLI feature is used to obtain an overview of the highest volume traffic (top talkers) in your network. It provides an overview of the traffic by aggregating the flows in the cache based on the aggregation field that you select when you use the NetFlow Dynamic Top Talkers CLI feature.

The NetFlow Dynamic Top Talkers CLI feature does not require modifications to the configuration of the router. The **show ip flow top** command is the only command that you need to use for the NetFlow Dynamic Top Talkers CLI feature. You can invoke any of the NetFlow Dynamic Top Talkers CLI options directly from the **show ip flow top** command whenever you need them.

Note The information that you want to use the NetFlow Dynamic Top Talkers CLI feature to analyze must be available in the cache. For example, if you want to be able to identify the MAC address in the flows, you must configure the **ip flow-capture mac-addresses** command in order to capture the values from the MAC address fields in the traffic first.

The NetFlow Dynamic Top Talkers CLI feature aggregates flows and allows them to be sorted so that they can be viewed. The flows can be aggregated on fields in the cache such as source or destination IP address, ICMP type and code values, and so forth. For a full list of the fields that you can aggregate the flows on, refer to the **show ip flow top**command in the Cisco IOS NetFlow command reference documentation.

The aggregated top talker flows can be sorted by any of the following criteria:

- The aggregated field in the display data
- The number of bytes in the display data
- The number of flows in the display data
- The by number of packets in the display data
- In ascending or descending order (to find the least used Top talker)

In addition to sorting top talkers, you can further organize your output by specifying criteria that the top talkers must match, such as source or destination IP address or port. The **match** keyword is used to specify this

criterion. For a full list of the matching criterion that you can select, refer to the **show ip flow top**command in the Cisco IOS NetFlow command reference documentation.

The NetFlow Dynamic Top Talkers CLI feature can help you quickly identify traffic that is associated with security threats such as DoS attacks because it does not require configuration modifications. You can change the NetFlow Dynamic Top Talkers CLI options for identifying and analyzing network threats in the aggregated flows on-the-fly as you learn more about the traffic that is of interest. For example, after you have identified that there is a lot of ICMP traffic in your network by using the **show ip flow top 10 aggregate icmp** command you can learn what IP networks the traffic is being sent to by using the **show ip flow top 10 aggregate icmp match destination-prefix 172.0.0.0/8** command.

Note A high volume of ICMP traffic might indicate that an ICMP-based DoS attack is in progress.

The **show ip flow top** command:

- Does not require additional NetFlow configuration commands to display top talkers. Therefore you do not need to supply the configuration mode password to the administrators who use the he **show ip flow top** command to monitor network traffic. The only prerequisite for using the **show ip flow top** command is that you have configured NetFlow on at least one interface on the router.
- Aggregates flows automatically based on the aggregation method that you select, and independently of any netflow aggregation cache(s).
- Allows you to change the parameters of the command, such as the number of flows to display, the display order, and match criterion, on-the-fly every time that you use the command without having to change the router's configuration.
- Allows you to sort the display output in ascending or descending order based on:
  - The aggregated field
  - The number of bytes
  - The number of flows,
  - The number of packets

show ip flow top and show ip cache verbose flow

Many of the values shown in the display output of the **show ip cache verbose flow** command are in hexadecimal. If you want to match these values using the **show ip flow top** command with the **match** keyword, you must enter the field value that you want to match in hexadecimal. For example, to match on the destination port of 00DC in the following except from the **show ip cache verbose flow** command, you would use the **match destination-port** *0x00DC* keywords and argument for the **show ip flow top** command.

```
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop             B/Pk  Active
Et0/0.1        10.10.11.4      Et1/0.1        172.16.10.8     06 00  00     209
00DC /0  0                     00DC
 /0  0     0.0.0.0               40   281.4
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       40                            Max plen:        40
Min TTL:        59                            Max TTL:         59
IP id:           0
```

Match Criteria with the show ip flow top command

You can limit the top talkers that are displayed by the **show ip flow top** command by using the **match** keyword and arguments. For example, you can display the IP destination address top talkers that have a prefix of 224.0.0.0 using the **show ip flow top 10 aggregate destination-address match destination-prefix** *224.0.0.0/3* command.

For a full list of the matching criterion that you can select, refer to the **show ip flow top**command in the *Cisco IOS NetFlow Command Reference* . If you do not configure match criteria all of the flows are considered as candidates for aggregation as top talkers based on the volume of traffic they represent.

The Order That Aggregation Occurs in

With the exception of the **flows** keyword, all matches are performed prior to aggregation, and only matching flows are aggregated. For example, the **show ip flow top***5***aggregate destination-address match destination-prefix** *172.16.0.0/16* command analyzes all of the available flows looking for any flows that have destination addresses that match the **destination-prefix** value of *172.16.0.0/16*. If it finds any matches it aggregates them, and then displays the number of aggregated **destination-address** flows that is equal to the number of top talkers that were requested in the command-in this case five.

The **flows** keyword matches the number of aggregated flows post-aggregation. For example, the **show ip flow top** *2* **aggregate destination-address match** *6* command aggregates all of the flows on the values in their destination IP address field, and then displays the top talkers that have 6 aggregated flows.

Number of Flows Matched

If you do not specify match criteria and there is traffic in the flows that includes the field that you used to aggregate the flows on, all of the flows will match. For example, if your router has 20 flows with IP traffic and you enter the **show ip flow top 10 aggregate destination-address** command the display will indicate that 20 of 20 flows matched, and the 10 top talkers will be displayed.

If you use the match keyword to limit the flows that are aggregated to the flows with a destination prefix of 224.0.0.0/3, and only one flow matches this criterion the output will indicate that one out of six flows matched. For example, if your router has 6 flows with IP traffic, but only one of them has a destination prefix of 224.0.0.0/3, and you enter the **show ip flow top 10 aggregate destination-address match destination-prefix** *224.0.0.0/3* command, the display will indicate that 1 of 6 flows matched.

If the total number of top talkers is less than the number of top talkers that were requested in the command, the total number of top talkers is displayed. For example, if you enter a value of five for the number of top talkers to display and there are only three top talkers that match the criteria that you used, the display will only include three top talkers.

When a match criterion is included with the **show ip flow top** command, the display output will indicate "N of M flows matched" where N <= M, N = matched flows, and M = total flows seen. The numbers of flows seen could potentially be more than the total number of flows in the cache if some of the analyzed flows were removed from the cache and new flows were created ahead of the current point, as the top talkers feature sweeps through the cache. Therefore, M is NOT the total number of flows in the cache, but rather, the number of observed flows.

If you attempt to display the top talkers by aggregating them on a field that is not in the cache you will see the "% aggregation-field" is not available for this cache" message. For example, if you use the **show ip flow top** *5* **aggregate** *s* **ource-vlan** command, and you have not enabled the capture of VLAN IDs from the flows, you will see the "% VLAN id is not available for this cache" message.

NetFlow Top Talkers

This feature was introduced in 12.3(11)T. NetFlow Top Talkers is used to obtain information about individual flows in the cache. It does not aggregate the flows like the NetFlow Dynamic Top Talkers CLI feature.

The NetFlow Top Talkers feature compares all of the flows and displays information about each of the flows that have the heaviest traffic volumes (top talkers). The **show ip flow top-talkers**command requires you to pre-configure the router using the NetFlow Top Talkers configuration commands:

- **ip flow-top-talkers** --Enters the NetFlow Top Talkers configuration mode.
- **sort-by** --Selects the sort order for the flows in the display output.
  - **bytes**--Sort the flows based on the numbers of bytes in each flow.
  - **packets**--Sort the flows based on the numbers of packets in each flow.
- **top** --Specifies the number of top talkers to monitor.
- **match** (optional)--Specifies additional criteria, such as IP addresses, port numbers, and so forth, that must be matched in the flow to qualify as a candidate for top talker status.

For a full list of the matching criterion that you can select, refer to the **ip flow top-talkers**command in the *Cisco IOS NetFlow Command Reference* . If you do not configure match criteria all of the flows are considered as candidates as top talkers based on the volume of traffic they represent.

- **show ip flow top talkers** [**verbose**]--Displays the flows.

For more information on the NetFlow Top Talkers feature, refer to Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands.

Filtering and Sampling of NetFlow Traffic

NetFlow provides highly granular per-flow traffic statistics in a Cisco router. A flow is a unidirectional stream of packets that arrive at the router on the same subinterface, have the same source and destination IP addresses, Layer 4 protocol, TCP/UDP source and destination ports, and the same ToS (type of service) byte in the IP headers. The router accumulates NetFlow statistics in a NetFlow cache and can export them to an external device (such as the Cisco Networking Services (CNS) NetFlow Collection Engine) for further processing.

Full NetFlow accounts for all traffic entering the subinterface on which it is enabled. But in some cases, you might gather NetFlow data on only a subset of this traffic. The Random Sampled NetFlow feature and the NetFlow Input Filters feature each provide ways to limit incoming traffic to only traffic of interest for NetFlow processing. Random Sampled NetFlow provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets. The NetFlow Input Filters feature provides the capability to gather NetFlow data on only a specific user-defined subset of traffic.

Note Random Sampled NetFlow is more statistically accurate than Sampled NetFlow. NetFlow's ability to sample packets was first provided by a feature named Sampled NetFlow. The methodology that the Sampled NetFlow feature uses is *deterministic* sampling, which selects every nth packet for NetFlow processing on a per-interface basis. For example, if you set the sampling rate to 1 out of 100 packets, then Sampled NetFlow samples the 1st, 101st, 201st, 301st, and so on packets. Sampled NetFlow does not allow random sampling and thus can make statistics inaccurate when traffic arrives in fixed patterns.

Note The Random Sampled NetFlow algorithms are applied after input filtering.

The table below compares the NetFlow Input Filters feature and the NetFlow Random Sampled feature.

Table 62: Comparison of the NetFlow Input Filters Feature and the Random Sampled NetFlow Feature

Comparison Category	NetFlow Input Filters Feature	Random Sampled NetFlow Feature
Brief description	This feature enables you to gather NetFlow data on only a specific subset of traffic. You do this by creating filters to select flows for NetFlow processing. For example, you can select flows from a specific group of hosts. This feature also lets you select various sampling rates for selected flows.	This feature provides NetFlow data for a subset of traffic in a Cisco router by processing only one randomly selected packet out of n sequential packets (n is a user-configurable parameter). Packets are sampled as they arrive (before any NetFlow cache entries are made for those packets).
Main uses	You can use this feature for class-based traffic analysis and monitoring on-network or off-network traffic. This feature is also useful if you have too much traffic and you want to limit the traffic that is analyzed.	You can use this feature for traffic engineering, capacity planning, and applications where full NetFlow is not needed for an accurate view of network traffic. This feature is also useful if you have too much traffic and you want to limit the traffic that is analyzed.
Export format support	This feature is supported in the Version 5 and Version 9 NetFlow export formats.	This feature is supported in the Version 5 and Version 9 NetFlow export formats.
Cisco IOS release support	12.3(4)T.	12.3(2)T, 12.2(18)S, and 12.0(26)S.

Comparison Category	NetFlow Input Filters Feature	Random Sampled NetFlow Feature
Subinterface support	You can configure NetFlow Input Filters per subinterface as well as per physical interface. You can select more than one filter per subinterface and have all of the filters run simultaneously.	You can configure the Random Sampled NetFlow feature per subinterface as well as per physical interface. You can not run Full NetFlow and Random Sampled NetFlow concurrently on the same subinterface. You must disable full NetFlow on the subinterface before Random Sampled NetFlow will take effect. Traffic is collected only on the subinterfaces on which Random Sampled NetFlow is configured. As with full NetFlow, enabling Random Sampled NetFlow on a physical interface does not enable Random Sampled NetFlow on subinterfaces automatically--you must explicitly configure it on the subinterfaces.
Memory impact	This feature requires no additional memory. It allows you to use a smaller NetFlow cache than full NetFlow, because it significantly reduces the number of flows. This feature requires an insignificant amount of memory for each configured NetFlow filter.	This feature can create a smaller NetFlow cache than full NetFlow if by reducing the number of packets being analyzed the numbers of flows in the cache is also reduced. This feature requires an insignificant amount of memory for each configured NetFlow sampler.
Performance impact	Accounting of classified traffic saves router resources by reducing the number of flows being processed and exported. The amount of bandwidth saved depends on the usage and the class-map criteria. However, performance might degrade depending on the number and complexity of class maps configured in a policy.	Statistical traffic sampling substantially reduces consumption of router resources (especially CPU resources) while providing valuable NetFlow data. This feature substantially reduces the impact of NetFlow data export on interface traffic. For example, a sampling rate of 1 out of 100 packets reduces the export of NetFlow data by about 99% percent.

NetFlow Input Filters Flow Classification

For the NetFlow Input Filters feature, classification of packets can be based on any of the following: IP source and destination addresses, Layer 4 protocol and port numbers, incoming interface, MAC address, IP Precedence, DSCP value, Layer 2 information (such as Frame-Relay DE bits or Ethernet 802.1p bits), and Network-Based Application Recognition (NBAR) information. The packets are classified (filtered) on the above criteria, and flow accounting is applied to them on subinterfaces.

The filtering mechanism uses the Modular QoS Command-Line Interface (MQC) to classify flows. You can create multiple filters with matching samplers on a per-subinterface basis. For example, you can subdivide subinterface traffic into multiple classes based on type of service (ToS) values or destination prefixes (or

both). For each class, you can also configure sampling at a different rate, using higher rates for higher-priority classes of traffic and lower rates for lower-priority ones.

MQC has many policies (actions) such as bandwidth rate and queuing management. These policies are applied only if a packet matches a criterion in a class map that is applied to the subinterface. A class map contains a set of match clauses and instructions on how to evaluate the clauses and acts as a filter for the policies, which are applied only if a packet's content satisfies the match clause. The NetFlow Input Filters feature adds NetFlow accounting to the MQC infrastructure, which means that flow accounting is done on a packet only if it satisfies the match clauses.

Two types of filter are available:

- ACL-based flow-mask filters
- Fields of filter (source IP address, destination IP address, source application port, destination application port, port protocol, ToS bits, and TCP flags)

For more information on Modular QoS Command-Line Interface (MQC) refer to the *Cisco IOS Quality of Service Solutions Configuration Guide* .

Random Sampled NetFlow Sampling Mode

Sampling mode makes use of an algorithm that selects a subset of traffic for NetFlow processing. In the random sampling mode that the Random Sampled NetFlow feature uses, incoming packets are randomly selected on average one out of each n sequential packets is selected for NetFlow processing. For example, if you set the sampling rate to 1 out of 100 packets, then NetFlow might sample the 5th packet and then the 120th, 230th, 302nd, and so on. This sample configuration provides NetFlow data on 1 percent of total traffic. The n value is a parameter that you can configure from 1 to 65535 packets.

Random Sampled NetFlow The NetFlow Sampler Map

Random Sampled NetFlow is useful if you have too much traffic and you want to limit the traffic that is analyzed. A NetFlow sampler map is created with the **flow-sampler-map** *sampler-map-name* command. The sampling mode for the sampler map is configured with the **mode random one-out-of** *sampling-rate* command. The range of values for the *sampling-rate* argument is 1 to 65535. Each NetFlow sampler map can be applied to one or many subinterfaces as well as physical interfaces. The sampler map is applied to an interface or subinterface with the **flow-sampler** *sampler-map-name* command. You can define up to eight NetFlow sampler maps.

How to Configure and Use NetFlow to Detect and Analyze Network Threats

Using NetFlow to detect and analyze network threats requires a combination of configuration commands and show commands. You start by configuring the NetFlow Layer 2 and Security Monitoring Exports feature to capture values of the additional non-key fields from the flows so that they can be displayed in the cache by the NetFlow show commands. Capturing the values in the additional non-key fields is required so that you can identify the path the traffic is taking through the network and other characteristics of the traffic such as TTL values and packet length values.

After you configure the NetFlow Layer 2 and Security Monitoring Exports feature, you use the NetFlow Dynamic Top Talkers CLI command to obtain an overview of the traffic flows the router is forwarding. The overview displays information such as the protocol distribution in the flows, the source ip addresses that are sending the flows, and the networks the flows are being sent to.

After you identify the type of flows that you want to focus, on such as ICMP traffic, and other characteristics such as source IP addresses and destination network prefixes, you use the NetFlow Top Talkers feature to obtain more focused and detailed information on the individual flows. The NetFlow Top Talkers feature is configured with match criteria that focuses it on the types of traffic that you have identified. If your router is keeping track of several flows and you are only interested in analyzing a subset of them you, can configure NetFlow Input Filters to limit the flows that NetFlow is tracking.

Prerequisites

CEF or dCEF must be configured globally, and on the interface that you want to run NetFlow on, before you configure NetFlow Layer 2 and Security Monitoring Exports.

You must have NetFlow enabled on at least one interface in the router before you configure NetFlow Layer 2 and Security Monitoring Exports.

If you want to capture the values of the Layer 3 IP fragment offset field from the IP headers in your IP traffic using the **ip flow-capture fragment-offset** command, your router must be running Cisco IOS 12.4(2)T or later.

This section contains the following procedures:

Configuring NetFlow Layer 2 and Security Monitoring Exports

Perform the following task to configure the NetFlow Layer 2 and Security Monitoring Exports feature.

Before You Begin

To export the data captured with the NetFlow Layer 2 and Security Monitoring feature, you must configure NetFlow to use the NetFlow Version 9 data export format.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-capture fragment-offset**
4. **ip flow-capture icmp**
5. **ip flow-capture ip-id**
6. **ip flow-capture mac-addresses**
7. ip flow-capture packet-length
8. **ip flow-capture ttl**
9. **ip flow-capture vlan-id**
10. **interface type** *interface-type interface-number*]
11. **ip flow ingress**
12. end

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	**ip flow-capture fragment-offset** **Example:** `Router(config)# ip flow-capture fragment-offset`	Enables capturing the value of the IP fragment offset field from the first fragmented IP datagram in a flow.
Step 4	**ip flow-capture icmp** **Example:** `Router(config)# ip flow-capture icmp`	Enables you to capture the value of the ICMP type and code fields from the first ICMP datagram in a flow.
Step 5	**ip flow-capture ip-id** **Example:** `Router(config)# ip flow-capture ip-id`	Enables you to capture the value of the IP-ID field from the first IP datagram in a flow.
Step 6	**ip flow-capture mac-addresses** **Example:** `Router(config)# ip flow-capture mac-addresses`	Enables you to capture the values of the source and destination MAC addresses from the first Layer 2 frame in a flow.
Step 7	ip flow-capture packet-length **Example:** `Router(config)# ip flow-capture packet-length`	Enables you to capture the minimum and maximum values of the packet length field from IP datagrams in a flow.
Step 8	**ip flow-capture ttl** **Example:** `Router(config)# ip flow-capture ttl`	Enables you to capture the minimum and maximum values of the Time-to-Live (TTL) field from IP datagrams in a flow.

	Command or Action	Purpose
Step 9	**ip flow-capture vlan-id** **Example:** `Router(config)# ip flow-capture vlan-id`	Enables you to capture the 802.1q or ISL VLAN-ID field from first VLAN encapsulated Layer 2 frame in a flow that is received or transmitted on a trunk port.
Step 10	**interface type** *interface-type interface-number*] **Example:** `Router(config)# interface ethernet 0/0`	Enters interface configuration mode for the type of interface specified in the command.

Step 11	**ip flow ingress**
	Example:
	`and/or`
	Example:
	`ip flow egress`
	Example:
	`Router(config-if)# ip flow ingress`
	Example:
	`and/or`
	Example:
	`Router(config-if)# ip flow egress`
		Enables ingress NetFlow data collection on the interface.
		and/or
		Enables egress NetFlow data collection on the interface.

Step 12	end **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Verifying NetFlow Layer 2 and Security Monitoring Exports

This task verifies that NetFlow Layer 2 and Security Monitoring Exports is configured correctly. The **show ip cache verbose flow**command gives a detailed view of the status and statistics for flows in the NetFlow main cache. The values for the NetFlow non-key fields that you have configured with the NetFlow Layer 2 and Security Monitoring Exports feature are included for each flow.

To see the values of the fields that you have configured the NetFlow Layer 2 and Security Monitoring Exports feature to capture, your router must be forwarding IP traffic that meets the criteria for these fields. For example, if you configure the **ip flow-capture vlan-id** command, your router must be forwarding IP datagrams over interfaces that are configured as VLAN trunks to capture the VLAN-ID values from the layer-two frames carrying the IP datagrams in the flow.

Restrictions

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running dCEF, NetFlow cache information is maintained on each line card or Versatile Interface Processor. If you want to use the **show ip cache verbose flow** command to display this information on a distributed platform, you must enter the command at a line card prompt.

Cisco 7500 Series Platform

To display detailed NetFlow cache information on a Cisco 7500 series router that is running distributed dCEF, enter the following sequence of commands:

```
Router# if-con

slot-number
LC-
slot-number
# show ip cache verbose
 flow
```

For Cisco IOS Releases 12.3(4)T, 12.3(6), and 12.2(20)S and later, enter the following command to display detailed NetFlow cache information:

```
Router# execute-on
slot-number
show ip cache verbose
 flow
```

Cisco 12000 Series Platform

To display detailed NetFlow cache information on a Cisco 12000 Series Internet Router, enter the following sequence of commands:

```
Router# attach

slot-number
LC-
slot-number
# show ip cache verbose
 flow
```

For Cisco IOS Releases 12.3(4)T, 12.3(6), and 12.2(20)S and later, enter the following command to display detailed NetFlow cache information:

Router# **execute-on** *slot-number* **show ip cache verbose flow**

To verify the configuration of NetFlow Layer 2 and Security Monitoring Exports use the following step.

SUMMARY STEPS

1. **show ip cache verbose flow**

DETAILED STEPS

show ip cache verbose flow

This example shows that NetFlow Layer 2 and Security Monitoring Exports is working properly because the values have been captured from the non-key Layer 3 and Layer 2 fields in the flows. The values captured in the flows are shown in **bold** text.

Example:

```
Router# show ip cache verbose flow
IP packet size distribution (33978 total packets):
1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
.856 .143 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
.000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
14 active, 4082 inactive, 59 added
12452 ager polls, 0 flow alloc failures
Active flows timeout in 10 minutes
Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
28 active, 996 inactive, 148 added, 59 added to flow
0 alloc failures, 0 force free
1 chunk, 1 chunk added
last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-SMTP             2      0.0      1730    40      3.6     600.7       0.2
UDP-other           31      0.0         1    54      0.0       3.6      16.8
ICMP                12      0.0      1728    28     22.0     600.1       0.1
Total:              45      0.0       538    29     25.7     189.2      11.6
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
.
.
.
Et0/0.1        10.71.200.138   Et1/0.1        172.16.10.2     01 00  10     696
0000 /0  0                     0C01 /0  0     0.0.0.0                 28   241.4
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
```

Using NetFlow Dynamic Top Talkers CLI to Display the Protocol Distribution

You can obtain a quick overview of the traffic in your network by viewing the protocol distribution. Use this task to display the top talkers (aggregated flows) for these three IPv4 protocol types:

- 1--ICMP
- 6--TCP
- 17--UDP

SUMMARY STEPS

1. **show ip flow top** *number* **aggregate** *aggregate-field* **sorted-by packets descending**

DETAILED STEPS

show ip flow top *number* **aggregate** *aggregate-field* **sorted-by packets descending**
The following example looks for up to three top talkers, aggregates them on the protocol field, sorts them by packets, and displays the output in descending order:

Example:

```
Router# show ip flow top 3 aggregate protocol sorted-by packets descending

There are 3 top talkers:
IPV4 PROT       bytes        pkts       flows
=========  ==========  ==========  ==========
         1      406196       14507          12
         6       96560        2414           2
        17          52           1           1
15 of 15 flows matched.
```

The table below describes the significant fields shown in the display output.

Table 63: show ip flow top 3 aggregate protocol sorted-by packets descending Field Descriptions

Field	Description
There are 3 top talkers	The number of top talkers is displayed.
IPV4 PROT	This position in the display output is used to show the field that you selected to aggregate the flows on. The **protocol** keyword aggregates IPv4 traffic in the flows based on the IPv4 protocol type. In this example there are three IPv4 protocol types in the flows: • 1--ICMP • 6--TCP • 17--UDP
bytes	Displays the numbers of bytes in the aggregated flows for each top talker.
pkts	Displays the numbers of packets in the aggregated flows for each top talker.
flows	Displays the numbers of aggregated flows for each top talker.
15 of 15 flows matched.	Displays the number of flows that matched the command.

All 15 flows in the router are aggregated into three top talkers. In this example all of the flow traffic is top talker traffic. The majority of the traffic is ICMP traffic (IP protocol type 1). This might indicate an ICMP DoS attack is in progress.

Using NetFlow Dynamic Top Talkers CLI to Display the Source IP Address Top Talkers Sending ICMP Traffic

The display output from the **show ip flow top 10 aggregate protocol sorted-by packets descending** used in Using NetFlow Dynamic Top Talkers CLI to Display the Protocol Distribution, on page 347 section indicates that there is a possible ICMP-based DoS attack in progress. The next step to take is to identify the flows that are sending the ICMP traffic. In this case the flows will be aggregated on the source IP addresses.

SUMMARY STEPS

1. **show ip flow top** *number* **aggregate** *aggregate-field* **sorted-by packets match** *match-field match-value*

DETAILED STEPS

show ip flow top *number* **aggregate** *aggregate-field* **sorted-by packets match** *match-field match-value*
The following command looks for up to 20 top talkers, aggregates them on the source IP address, sorts them by packets, and matches on the protocol icmp:

Example:

```
Router# show ip flow top 20 aggregate source-address sorted-by packets match protocol icmp
There are 6 top talkers:
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
10.132.221.111        90440        3230           1
10.10.12.1            90440        3230           1
10.251.138.218        90440        3230           1
10.71.200.138         90384        3228           1
10.231.185.254        90384        3228           1
10.106.1.1            90356        3227           1
6 of 15 flows matched.
Router
```

The table below describes the significant fields shown in the display.

Table 64: show ip flow top 20 aggregate source-address sorted-by packets match protocol icmp Field Descriptions

Field	Description
There are 6 top talkers	The number of top talkers is displayed. **Note** Only 6 top talkers are displayed, even though you asked for 20, because only 6 of the 15 flows in the cache matched the criteria you specified. The number 20 is an upper limit that will be applied in the event that there are over 20 top talkers.
IPV4 SRC-ADDR	This position in the display output is used to show the field that you selected to aggregate the flows on. The **source-address**keyword aggregates flows based on the source IP address. In this example there are 6 IP source addresses with aggregated flows. Each of the IP addresses has 1 flow, therefore no aggregation was performed: • 10.132.221.111 • 10.10.12.1 • 10.251.138.218 • 10.71.200.138 • 10.231.185.254 • 10.106.1.1
bytes	Displays the numbers of bytes in the aggregated flows for each top talker.
pkts	Displays the numbers of packets in the aggregated flows for each top talker.
flows	Displays the numbers of aggregated flows for each top talker.
6 of 15flows matched.	Displays the number of flows that matched the command.

The ICMP traffic is aggregated into six top talkers (source IP addresses). Each top talker has one flow. No aggregation is performed on this traffic because there is a 1-to-1 correlation of IP source addresses and flows.

Using NetFlow Dynamic Top Talkers CLI to Display the Destination IP Address Top Talkers Receiving ICMP Traffic

The display output from the **show ip flow top 5 aggregate source-address sorted-by packets match protocol icmp** command used in Using NetFlow Dynamic Top Talkers CLI to Display the Source IP Address Top Talkers Sending ICMP Traffic, on page 349 section showed the six top talkers (IP source addresses) that are sending the 12 ICMP traffic flows. The next step to take is to identify the flows that are the target of the ICMP traffic. In this case the flows will be aggregated on the destination IP addresses.

SUMMARY STEPS

1. **show ip flow top** *number* **aggregate** *aggregate-field* **sorted-by packets match** *match-field match-value*

DETAILED STEPS

show ip flow top *number* **aggregate** *aggregate-field* **sorted-by packets match** *match-field match-value*
The following command looks for up to 20 top talkers, aggregates them on the destination IP address, sorts them by packets, and matches on the protocol icmp

Example:

```
Router# show ip flow top 20 aggregate destination-address sorted-by packets match protocol icmp
There is 1 top talker:
IPV4 DST-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
172.16.10.2          407456       14552           6
6 of 14 flows matched.
Router
```

The table below describes the significant fields shown in the display.

Table 65: show ip flow top 20 aggregate destination-address sorted-by packets match protocol icmp Field Descriptions

Field	Description
There is 1 top talker	The number of top talkers is displayed. • The ICMP traffic is aggregated into 6 flows for one destination IP addresses.
IPV4 DST-ADDR	This position in the display output is used to show the field that you selected to aggregate the flows on. The **destination-address**keyword aggregates flows based on the destination IP address. In this example there are 3 IP destination address with aggregated flows. The IP addresses has 8 aggregated flows: • 172.16.10.2

Field	Description
bytes	Displays the numbers of bytes in the aggregated flows for each top talker.
pkts	Displays the numbers of packets in the aggregated flows for each top talker.
flows	Displays the numbers of aggregated flows for each top talker.
6 of 14 flows matched.	Displays the number of flows that matched the command.

The previous task identified six ICMP top talkers based on source IP addresses that each had one flow. This task identified that there is one ICMP top talker based on destination IP addresses that is the target for 6 individual flows. There is a 1-to-1 correlation between the number of ICMP flows in the top talkers aggregated on the source IP address and the number of ICMP flows in the top talkers aggregated on the destination IP address. There is a high probability that an ICMP-based DoS attack on the host with the IP address of 172.16.10.2 is in progress.

Configuring NetFlow Top Talkers to Monitor Network Threats

The previous task (Using NetFlow Dynamic Top Talkers CLI to Display the Destination IP Address Top Talkers Receiving ICMP Traffic) identified a probable ICMP-based DoS attack on the host with the IP address 172.16.10.2. This task uses the NetFlow Top Talkers feature to configure the router to monitor the DoS attack by tracking the individual ICMP flows. After you have configured the NetFlow Top Talkers feature to focus on the DoS attack traffic, you can use the **show ip flow top-talkers verbose** command to identify the path the DoS traffic is taking through the network.

Perform the following task to configure the NetFlow Top Talkers feature.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip flow-top-talkers**
4. **match destination address** *ip-address /prefix-mask*
5. **top** *number*
6. **sort-by** [**bytes** | **packets**
7. **end**

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	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	Enters NetFlow top talkers configuration mode.

Step 4	**match destination address** *ip-address /prefix-mask*
	Example:
	`Router(config-flow-top-talkers)`
	`# match destination address 172.16.10.2/32`
		Specifies the destination IP addresses to match.

Step 5	**top** *number* **Example:** `Router(config-flow-top-talkers)# top 50`	Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query.
Step 6	**sort-by** [**bytes** | **packets** **Example:** `Router(config-flow-top-talkers)# sort-by packets`	Specifies the sort criterion for the top talkers. • The top talkers can be sorted either by the total number of packets of each top talker or the total number of bytes of each top talker.
Step 7	**end** **Example:** `Router(config-flow-top-talkers)# end`	Exits to privileged EXEC mode.

Monitoring and Analyzing the NetFlow Top Talkers Flows

To monitor and analyze the NetFlow Top Talkers flows, use the following step.

SUMMARY STEPS

1. **show ip flow top-talkers verbose**

DETAILED STEPS

show ip flow top-talkers verbose

The following sample shows details for the six traffic flows that are being sent to the host with IP address 172.16.10.2.

Example:

```
Router# show ip flow top-talkers verbose
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs Bytes
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.106.1.1      Et1/0.1        172.16.10.2     01 00  10    9408
0000 /0  0                     0800 /0  0     0.0.0.0                28   116.3
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:       8                            ICMP code:        0
IP id:           0
Et0/0.1        10.132.221.111  Et1/0.1        172.16.10.2     01 00  10    9408
0000 /0  0                     0800 /0  0     0.0.0.0                28   116.4
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:       8                            ICMP code:        0
IP id:           0
Et0/0.1        10.10.12.1      Et1/0.1        172.16.10.2     01 00  10    9408
0000 /0  0                     0C01 /0  0     0.0.0.0                28   116.4
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
Et0/0.1        10.251.138.218  Et1/0.1        172.16.10.2     01 00  10    9408
0000 /0  0                     0C01 /0  0     0.0.0.0                28   116.4
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
Et0/0.1        10.71.200.138   Et1/0.1        172.16.10.2     01 00  10    9408
0000 /0  0                     0C01 /0  0     0.0.0.0                28   116.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
Et0/0.1        10.231.185.254  Et1/0.1        172.16.10.2     01 00  10    9408
0000 /0  0                     0C01 /0  0     0.0.0.0                28   116.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
6 of 50 top talkers shown. 6 of 8 flows matched.
```

Note Only six of the eight flows matched because the rest of the flows are not top talker flows.

Note The top 50 flows were requested, however there are only eight flows in the cache.

This display output contains the information required for determining the path that the DoS attack traffic is taking through the network. This information will be used to react to the DoS attack by adding security measures such as access-lists

to the affected interfaces. The table below describes the significant fields in the display from the **show ip flow top-talkers verbose** command for determining the network path the DoS traffic is taking.

Table 66: Significant Field Descriptions for show ip flow top-talkers verbose

Field	Description
SrcIf	Interface on which the packet was received. • All of the ICMP DoS traffic is being received on Et0/0.1
SrcIPaddress	This is the source IP address of the traffic in the six top talkers. The traffic is using 6 different IP source addresses • 10.132.221.111 • 10.10.12.1 • 10.251.138.218 • 10.71.200.138 • 10.231.185.254 • 10.106.1.1
DstIf	Interface from which the packet was transmitted. • All of the ICMP DoS traffic is being transmitted over Et1/0.1 **Note** If an asterisk (*) immediately follows the DstIf field, the flow being shown is an egress flow.
ICMP Type	The ICMP datagram types • 8--Echo • 12--Parameter Problem
ICMP Code	The ICMP codes • 0--None (not applicable) • 1--Depends on the ICMP Type • A code value of 1 for ICMP type 12 indicates that a required option is missing
DstIPaddress	This is the destination IP address of the traffic. **Note** 172.17.10.2 is the IP address that is being attacked.

Field	Description
MAC	These are the source and destination MAC addresses from the traffic. The source and destination MAC address are read from left to right in the output. • The traffic is being received from MAC address aaa.bbb.cc03. **Note** This MAC address is interface 1/0.1 on router R2. • The traffic is being transmitted to MAC address aaa.bbb.cc06. **Note** This MAC address is interface 1/0.1 on router R4.
VLAN id	These are the source and destination VLAN IDs. The source and destination VLAN IDs are read from left to right in the output. • The traffic is being received from VLAN 5. • The traffic is being transmitted to VLAN 6.

The flows in this example show only the ICMP DoS attack traffic that is destined for the host with IP address 172.16.10.2. These flows were created specifically for documenting this task. In a real network, the host under attack might be communicating with other hosts that are using legitimate applications such as e-mail and web sites. In this case, the Top Talkers match filter on the destination IP address (**match destination address 172.16.10.2/32**) that was configured in the Configuring NetFlow Top Talkers to Monitor Network Threats, on page 352 will not limit the display of the **show ip flow top-talkers** command to the ICMP DoS attack traffic.

Note For more information on the fields in the display output of the **show ip cache verbose flow** command, refer to the *Cisco IOS NetFlow Command Reference* .

If you are using the Top Talkers feature to analyze a network threat and you are not able to use the basic match filters to limit the display of the **show ip flow top-talkers** command to the traffic that you are analyzing, you can use NetFlow filtering and sampling to limit the traffic that shows up in the display of the **show ip flow top-talkers** command. The process for configuring NetFlow filtering and sampling is explained in the Configuring NetFlow Filtering and Sampling, on page 356.

Configuring NetFlow Filtering and Sampling

If you use the **show ip cache flow** command or the **show ip cache verbose flow** command to display the flows in the cache, you will see the ICMP flows that are selected by NetFlow filtering and sampling on interface Ethernet0/0.1, and flows for all NetFlow supported traffic types on any other interfaces that NetFlow is running on. The **show ip flow top-talkers** [**verbose**] command is used to display the flow status and statistics for the traffic type you configured with the match criteria over interfaces to which you applied the service

policy. For example, in this case you configured top talkers to match on ICMP traffic sent from any host that is arriving on Ethernet0/0.1 and destined for 172.16.10.2.

In this task the Top Talkers feature is being used more as a flow filter to separate flows of interest from all of the flows the router is seeing, rather than a filter to display the flows with the highest traffic volumes. Top talkers is used in this manner because in this example all of the ICMP DoS attack flows are of interest, not just the flows with the highest volumes. This is why a large value is assigned to the **top** keyword in the top talkers configuration. Setting the value for the **top** keyword to 50 when the largest number of ICMP DoS attack flows tracked by the router is 12 ensures that all of the ICMP DoS attack flows will be tracked.

If your router sees a significant number of flows involved in a DoS attack, you might want to set the value for the **top** keyword to a number that is less than the total number of flows to limit the number of flows that you see in the display when you use the **show ip flow top-talkers**command. This will ensure that you are seeing the flows that have the highest volume of DoS attack traffic. However, if all of the flows have the same traffic volume, the **show ip flow top-talkers**command will not be able to differentiate between them. It displays the number of flows that you set the value of the **top** keyword to, starting from the first flow in the cache.

Perform the following task to configure NetFlow Filtering and sampling.

Note **Restrictions for NetFlow Input Filters**

On Cisco 7500 platforms, the NetFlow Input Filters feature is supported only in distributed mode.

Restrictions for Random Sampled NetFlow

If full NetFlow is enabled on an interface, it takes precedence over Random Sampled NetFlow (which will thus have no effect). Disable full NetFlow on an interface before enabling Random Sampled NetFlow on that interface.

Enabling Random Sampled NetFlow on a physical interface does not automatically enable Random Sampled NetFlow on subinterfaces; you must explicitly configure it on subinterfaces. Also, disabling Random Sampled NetFlow on a physical interface (or a subinterface) does not enable full NetFlow. This restriction prevents the transition to full NetFlow from overwhelming the physical interface (or subinterface). If you want full NetFlow, you must explicitly enable it.

You must use NetFlow Version 9 if you want to use sampler option templates or view NetFlow sampler IDs.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **flow-sampler-map** *sampler-map-name*
4. **mode random** *one-out-of* **packet-interval**
5. **exit**
6. **class-map** *class-map-name* [**match-all** | **match-any**]
7. **match access-group** *access-group*
8. **exit**
9. **policy-map** *policy-map-name*
10. **class {** *class-name* **| class-default}**
11. **netflow-sampler** *sampler-map-name*
12. **exit**
13. **exit**
14. **interface** *interface-type interface-number* [*.subinterface number*]
15. **no** [**ip route-cache flow** | **ip flow ingress**]
16. **service-policy** {**input** | **output**} *policy-map-name*
17. **exit**
18. **ip flow-top-talkers**
19. **top** *number*
20. **sort-by** *packets*
21. **match class-map** *claas-name*
22. **no match destination address** ip-address /*prefix-mask*
23. **exit**
24. **access-list access-list-number permit icmp** *source destination*
25. **end**

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-sampler-map** *sampler-map-name*	Defines a statistical sampling NetFlow export flow sampler map.

	Command or Action	Purpose
	Example: `Router(config)# flow-sampler-map icmp-dos-fs-map`	• The *sampler-map-name* argument is the name of the flow sampler map to be defined. Entering the **flow-sampler-map** command enables the flow sampler configuration mode.
Step 4	**mode random** *one-out-of* **packet-interval** **Example:** `Router(config-sampler-map)# mode random one-out-of 2`	Specifies a statistical sampling NetFlow export random sampling mode and a packet interval. • The **random** keyword specifies that sampling uses the random sampling mode. • The *one-out-of* **packet-interval** argument-keyword pair specifies the packet interval (one out of every *n*packets) from which to sample. For *n*, you can specify from 1 to 65535 (packets).
Step 5	**exit** **Example:** `Router(config-sampler-map)# exit`	Exits back to global configuration mode.
Step 6	**class-map** *class-map-name* [**match-all** | **match-any**] **Example:** `Router(config)# class-map match-any icmp-dos-class-map`	Creates a class map to be used for matching packets to a specified class. • The *class-map-name* argument is the name of the class for the class map. The name can be a maximum of 40 alphanumeric characters. The class name is used for both the class map and for configuring policy for the class in the policy map. • The **match-all | match-any**keywords determine how packets are evaluated when multiple match criteria exist. Packets must either meet all of the match criteria (**match-all)** or only one of the match criteria (**match-any**) to be considered a member of the class. Entering the **class-map**command enables class-map configuration mode, in which you can enter one of the match commands to configure the match criteria for this class.
Step 7	**match access-group** *access-group* **Example:** `Router(config-cmap)# match access-group 101`	Configures the match criteria for a class map on the basis of the specified access control list (ACL). • The *access-group* argument is a numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
Step 8	**exit** **Example:** `Router(config-cmap)# exit`	Exits back to global configuration mode.

	Command or Action	Purpose
Step 9	**policy-map** *policy-map-name* **Example:** `Router(config)# policy-map icmp-dos-policy-map`	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy. • The *policy-map-name* argument is the name of the policy map. The name can be a maximum of 40 alphanumeric characters. Entering the **policy-map**command enables quality of service (QoS) policy-map configuration mode, in which you can configure or modify the class policies for that policy map
Step 10	**class {** *class-name* **| class-default}** **Example:** `Router(config-pmap)# class icmp-dos-class-map`	Specifies the name of the class whose policy you want to create or change or specifies the default class (commonly known as the class-default class) before you configure its policy. • The *class-name* argument is the name of the class for which you want to configure or modify policy. • The **class-default** keyword specifies the default class so that you can configure or modify its policy. Entering the **class** command enables QoS policy-map class configuration mode.
Step 11	**netflow-sampler** *sampler-map-name* **Example:** `Router(config-pmap-c)# netflow-sampler icmp-dos-fs-map`	Enables a NetFlow input filter sampler. • The *sampler-map-name* argument is the name of the NetFlow sampler map to apply to the class. You can assign only one NetFlow input filter sampler to a class. Assigning another NetFlow input filter sampler to a class overwrites the previous one.
Step 12	**exit** **Example:** `Router(config-pmap-c)# exit`	Exits back to policy-map configuration mode.
Step 13	**exit** **Example:** `Router(config-pmap# exit`	Exits back to global configuration mode.
Step 14	**interface** *interface-type interface-number* [*.subinterface number*] **Example:** `Router(config)# interface Ethernet0/0.1`	Specifies the interface and enters subinterface configuration mode. • The *interface-type* argument is the type of interface to be configured. • The *interface-number*argument is the number of the interface. Refer to the appropriate hardware manual for slot and port information.

	Command or Action	Purpose
Step 15	**no** [**ip route-cache flow** | **ip flow ingress**] **Example:** `Router(config-subif)# no ip flow ingress`	Removes the existing NetFlow command from the interface. **Note** NetFlow sampling and filtering can not start if there is another command on the interface that is enabling NetFlow.
Step 16	**service-policy** {**input** | **output**} *policy-map-name* **Example:** `Router(config-subif)# service-policy input icmp-dos-policy-map`	Attaches a policy map to an input interface or virtual circuit (VC), or an output interface or VC, to be used as the service policy for that interface or VC. • The **input** keyword attaches the specified policy map to the input interface or input VC. • The **output** keyword attaches the specified policy map to the output interface or output VC. • The *policy-map-name* is the name of a service policy map (created through use of the **policy-map** command) to be attached. The name can be a maximum of 40 alphanumeric characters.
Step 17	**exit** **Example:** `Router(config-subif)# exit`	Exits back to global configuration mode.
Step 18	**ip flow-top-talkers** **Example:** `Router(config)# ip flow-top-talkers`	Enters NetFlow top talkers configuration mode.
Step 19	**top** *number* **Example:** `Router(config-flow-top-talkers)# top 50`	Specifies the maximum number of top talkers that will be retrieved by a NetFlow top talkers query.
Step 20	**sort-by** *packets* **Example:** `Router(config-flow-top-talkers)# sort-by packets`	Specifies the sort criterion for the top talkers. • The top talkers can be sorted either by the total number of packets of each top talker or the total number of bytes of each top talker.
Step 21	**match class-map** *claas-name* **Example:** `Router(config-flow-top-talkers)# match class-map icmp-dos-class-map`	Specifies that the match criteria should be obtained from the class-map.

	Command or Action	Purpose
Step 22	**no match destination address** ip-address */prefix-mask* **Example:** `Router(config-flow-top-talkers)# no match destination address 172.16.10.2/32`	(Optional) If you still have a match entry for the destination address you should remove it so that only the class-name match criteria is used.
Step 23	**exit** **Example:** `Router(config-sampler-map)# exit`	Exits back to global configuration mode.
Step 24	**access-list access-list-number permit icmp** *source destination* **Example:** `Router(config)# access-list 101 permit icmp any host 172.16.10.2`	Creates an extended access list that is used to track any host that is sending ICMP traffic to 172.16.10.2.
Step 25	**end** **Example:** `Router(config)# end`	Exits to privileged EXEC mode.

Verify NetFlow Filtering and Sampling

To verify that filtering and sampling is working properly, use the following step.

SUMMARY STEPS

1. **show flow-sampler**

DETAILED STEPS

show flow-sampler
Any non-zero value in the display output below indicates that Filtering and sampling is active.

Example:

```
Router# show flow-sampler
```

```
Sampler : icmp-dos-fs-map, id : 1, packets matched : 63226, mode : random sampling mode
  sampling interval is : 2
Router
```

Monitoring and Analyzing the Sampled and Filtered NetFlow Top Talkers Flows

To monitor and analyze the filtered and sampled NetFlow top talkers flows use the following step.

SUMMARY STEPS

1. **show ip flow top-talkers**
2. **show ip flow top-talkers verbose**

DETAILED STEPS

Step 1 **show ip flow top-talkers**

The following sample output shows the six traffic flows that are being sent to the host with IP address 172.16.10.2.

Example:

```
Router# show ip flow top-talkers
SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.231.185.254  Et1/0.1       172.16.10.2     01 0000 0C01  5460
Et0/0.1       10.106.1.1      Et1/0.1       172.16.10.2     01 0000 0800  5124
Et0/0.1       10.132.221.111  Et1/0.1       172.16.10.2     01 0000 0800  5012
Et0/0.1       10.251.138.218  Et1/0.1       172.16.10.2     01 0000 0C01  4844
Et0/0.1       10.10.12.1      Et1/0.1       172.16.10.2     01 0000 0C01  4704
Et0/0.1       10.71.200.138   Et1/0.1       172.16.10.2     01 0000 0C01  4396
6 of 50 top talkers shown. 6 of 7 flows matched.
```

Step 2 **show ip flow top-talkers verbose**

The following sample output below shows the details for the six traffic flows that are being sent to the host with IP address 172.16.10.2.

Example:

```
Router# show ip flow top-talkers verbose

SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs Bytes
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.106.1.1      Et1/0.1        172.16.10.2     01 00  10    2884
0000 /0  0                     0800 /0  0     0.0.0.0                28    64.6
Sampler: 1  Class: 1
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:       8                            ICMP code:        0
IP id:           0
Et0/0.1        10.132.221.111  Et1/0.1        172.16.10.2     01 00  10    2828
0000 /0  0                     0800 /0  0     0.0.0.0                28    64.6
Sampler: 1  Class: 1
```

```
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:       8                            ICMP code:        0
IP id:           0
Et0/0.1        10.231.185.254  Et1/0.1        172.16.10.2     01 00  10    2716
0000 /0  0                     0C01 /0  0     0.0.0.0                28    64.6
Sampler: 1  Class: 1
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
Et0/0.1        10.71.200.138   Et1/0.1        172.16.10.2     01 00  10    2548
0000 /0  0                     0C01 /0  0     0.0.0.0                28    58.0
Sampler: 1  Class: 1
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
Et0/0.1        10.251.138.218  Et1/0.1        172.16.10.2     01 00  10    2436
0000 /0  0                     0C01 /0  0     0.0.0.0                28    64.6
Sampler: 1  Class: 1
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
Et0/0.1        10.10.12.1      Et1/0.1        172.16.10.2     01 00  10    2352
0000 /0  0                     0C01 /0  0     0.0.0.0                28    57.7
Sampler: 1  Class: 1
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       28                            Max plen:        28
Min TTL:        59                            Max TTL:         59
ICMP type:      12                            ICMP code:        1
IP id:           0
6 of 50 top talkers shown. 6 of 7 flows matched.
```

Configuration Examples for Detecting and Analyzing Network Threats With NetFlow

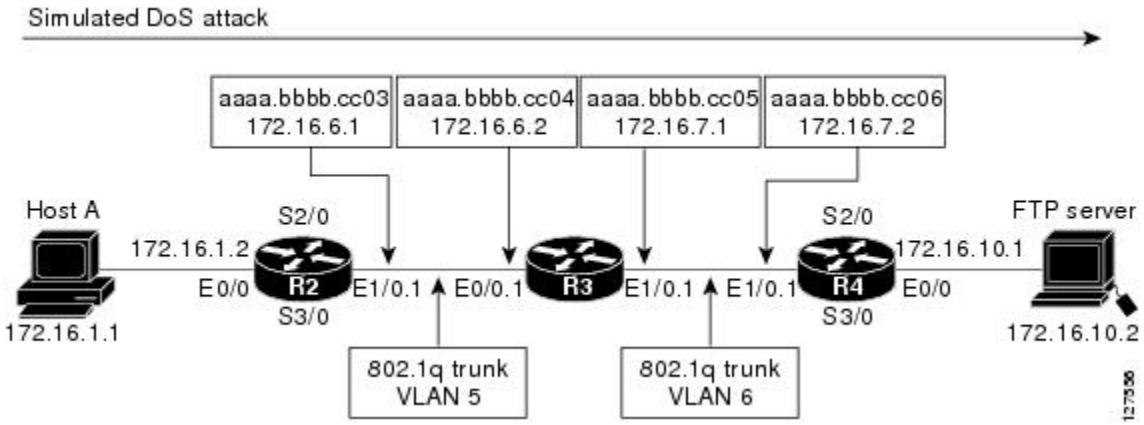
Configuring NetFlow Layer 2 and Sec Mon Exports to Capture Traffic From a Simulated FTP Attack Example

The following example shows how to use the NetFlow Layer 2 and Security Monitoring Exports feature to find out whether your network is being attacked by a host that is sending fake FTP traffic in an attempt to overwhelm the FTP server. This attack might cause end users to see a degradation in the ability of the FTP server to accept new connections or to service existing connections.

This example uses the network shown in the figure below. Host A is sending fake FTP packets to the FTP server.

This example also shows you how to use the Layer 2 data captured by the NetFlow Layer 2 and Security Monitoring Exports feature to learn where the traffic is originating and what path it is taking through the network.

Figure 39: Test Network



Tip Keep track of the MAC addresses and IP addresses of the devices in your network. You can use them to analyze attacks and to resolve problems.

Note This example does not include the **ip flow-capture icmp**command that captures the value of the ICMP type and code fields. The use of the **ip flow-capture icmp** command is described in "Configuring NetFlow Layer 2 and Sec Mon Exports to Capture Traffic From a Simulated ICMP Attack Example, on page 370."

R2

```
!
hostname R2
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc02
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc03
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.1 255.255.255.0
!
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R3

```
!
hostname R3
!
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture ip-id
ip flow-capture mac-addresses
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc04
 no ip address
!
interface Ethernet0/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.2 255.255.255.0
 ip accounting output-packets
 ip flow ingress
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc05
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.1 255.255.255.0
 ip accounting output-packets
 ip flow egress
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R4

```
!
hostname R4
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc07
 ip address 172.16.10.1 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc06
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.2 255.255.255.0
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

Analyze an FTP DoS Attack Using the show ip cache verbose flow command Example

The **show ip cache verbose flow** command displays the NetFlow flows. You can use this display output to identify the path that the FTP traffic from Host A is taking as it is received and transmitted by R3.

Note To reduce the space required to display the output from the **show ip flow cache verbose flow**command only the FTP flows are shown.

Tip Look for the flows that have FTP in them and make a note of the interfaces, MAC addresses, and VLANs (if applicable) for the flows.

```
R3# show ip cache verbose flow

IP packet size distribution (189118 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .043 .610 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .173 .000 .173 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  25 active, 4071 inactive, 615 added
  263794 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  50 active, 974 inactive, 1648 added, 615 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-FTP             12      0.0       895    40      0.9    1363.8       5.5
TCP-FTPD            12      0.0       895    40      0.9    1363.8       5.6
Total:             590      0.0       317   383     16.1     430.1      12.4
Et0/0.1        192.168.87.200  Et1/0.1        172.16.10.2     06 00  00       63
0015 /0  0                     0015
 /0  0     0.0.0.0               40    94.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       40                            Max plen:        40
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        192.168.87.200  Et1/0.1        172.16.10.2     06 00  00       63
0014 /0  0                     0014
 /0  0     0.0.0.0               40    94.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       40                            Max plen:        40
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        10.10.10.2      Et1/0.1        172.16.10.2     06 00  00       64
0015 /0  0                     0015
 /0  0     0.0.0.0               40    96.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:       40                            Max plen:        40
Min TTL:        59                            Max TTL:         59
IP id:           0
Et0/0.1        10.10.10.2      Et1/0.1        172.16.10.2     06 00  00       64
0014 /0  0                     0014
 /0  0     0.0.0.0               40    96.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
```

```
Min plen:       40                              Max plen:        40
Min TTL:        59                              Max TTL:         59
IP id:           0
Et0/0.1        10.234.53.1     Et1/0.1         172.16.10.2     06 00  00      63
0015 /0  0                     0015
 /0  0     0.0.0.0               40    94.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       40                              Max plen:        40
Min TTL:        59                              Max TTL:         59
IP id:           0
Et0/0.1        10.234.53.1     Et1/0.1         172.16.10.2     06 00  00      63
0014 /0  0                     0014
 /0  0     0.0.0.0               40    94.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       40                              Max plen:        40
Min TTL:        59                              Max TTL:         59
IP id:           0
Et0/0.1        172.30.231.193  Et1/0.1         172.16.10.2     06 00  00      63
0015 /0  0                     0015
 /0  0     0.0.0.0               40    94.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       40                              Max plen:        40
Min TTL:        59                              Max TTL:         59
IP id:           0
Et0/0.1        172.30.231.193  Et1/0.1         172.16.10.2     06 00  00      63
0014 /0  0                     0014
 /0  0     0.0.0.0               40    94.5
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       40                              Max plen:        40
Min TTL:        59                              Max TTL:         59
IP id:           0
```

There are 8 FTP flows shown in the output. You can use the Layer 2 information in the flows that is captured by the **ip flow-capture** command to identify the path the traffic is taking through the network. In this example, the traffic is being sent to R3 on VLAN 5 by R2. You can demonstrate that R2 is transmitting the traffic over interface 1/0.1 because the source MAC address (aaaa.bbb.cc03) belongs to 1/0.1 on R2. You can demonstrate that R3 is transmitting the traffic using VLAN 6 on interface 1/0.1 to interface 1/0.1 on R4, because the destination MAC address (aaaa.bbbb.cc06) belongs to interface 1/0.1 on R4.

Note For more information on the **ip flow-capture** command, and the fields in the display output of the **show ip cache verbose flow** command, refer to the *Cisco IOS NetFlow Command Reference* .

You can use this information to mitigate this attack. One possible way to mitigate this attack is by configuring an extended IP access list that blocks all FTP traffic from the source IP addresses that Host A is spoofing and applying it Ethernet 0/0 on R2.

Analyze an FTP DoS Attack Using NetFlow Dynamic Top Talkers CLI Example

You can use the NetFlow Dynamic Top Talkers CLI feature to quickly identify the FTP top talkers in the network traffic that might be sending the traffic. This will show you the IP source addresses that Host A is using as it sends the DoS attack traffic.

```
R3# show ip flow top 50 aggregate source-address sorted-by bytes descending match
destination-port min 20 max 21
There are 5 top talkers:
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
10.231.185.254         5640         141           2
10.132.221.111         3680          92           2
10.10.12.1             3640          91           2
10.251.138.218         3600          90           2
```

```
10.71.200.138          1880          47           1
9 of 34 flows matched.
```

Note Only source IP addresses from FTP traffic are shown because of the **match destination-port min** *20* **max** *21* criteria. The source addresses are aggregated together so only the most relevant sources are shown.

Note Only nine of the 34 flows matched because the rest of the flows are not FTP flows, therefore they do not meet the match criteria (**match destination-port min** *20* **max** *21*).

Tip The top talkers are displayed in descending order of the aggregated field by default.

Tip You can enter the port numbers in their decimal values as shown, or in their hexadecimal equivalents of 0x14 and 0x15.

After you have identified FTP top talkers traffic you need to identify the source IP addresses of IP traffic that is being sent to the host that you believe is under attack.

```
R3# show ip flow top 50 aggregate source-address match destination-prefix 172.16.10.2/32
There are 6 top talkers:
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
10.251.138.218          6642          18           4
10.231.185.254          5068          28           4
10.132.221.111         14818          25           4
10.106.1.1             12324          12           2
10.71.200.138          12564          18           3
10.10.12.1               560          14           2
19 of 33 flows matched.
```

Tip You can specify the host that you believe is under attack by using a prefix value of 32 with the **match destination-prefix** command.

Note Only 19 of the 33 flows matched because the rest of the flows do not contain traffic that is destined for the host with the IP address of 172.16.10.2, therefore they do not meet the match criteria (**match destination-prefix** *172.16.10.2/32*).

The final step is to cross reference the source IP addresses of any hosts that are sending any IP traffic to the host under attack with the list of source IP addresses from the FTP top talkers. This is required because the **show ip flow top** command does not support multiple match criteria. Therefore you cannot limit the top talkers to FTP traffic being sent to a specific host with a single **show ip flow top** command (**match destination-port min** *20* **max** *21* <and> **match destination-prefix** *172.16.10.2/32*).

The host with the IP address of 10.106.1.1 is apparently not involved in this DoS attack because it is not in the display output from the **show ip flow top** *50* a**ggregate source-address sorted-by bytes descending match destination-port min** *20* **max** *21* command. This means that it is not sending FTP traffic to the host that is under attack.

Therefore the host IP addressees involved in this FTP DoS attack are likely to be:

- 10.231.185.254
- 10.132.221.111
- 10.10.12.1
- 10.251.138.218
- 10.71.200.138

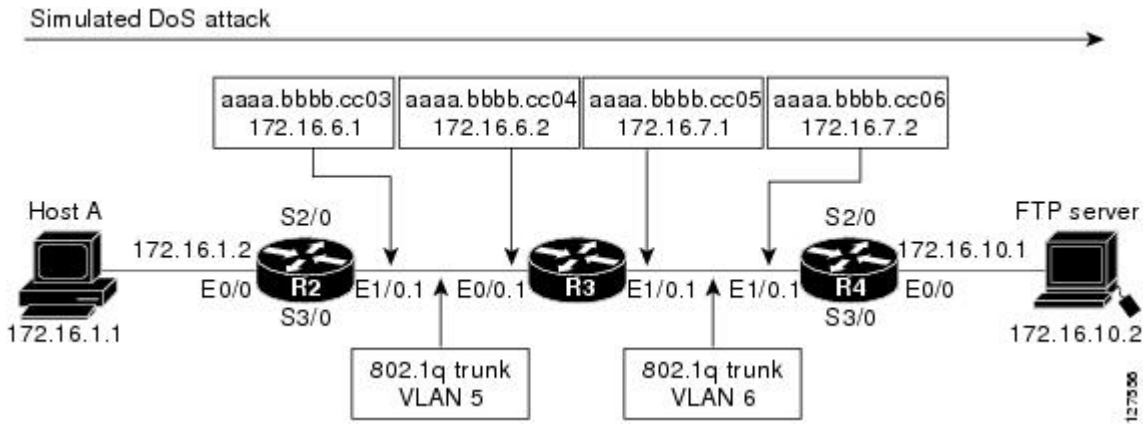
Now that you know the source addresses of the FTP traffic you can configure an extended access list that blocks FTP traffic from these address, and apply it to the interface that is closest to the point the traffic is entering your network.

Note Unless you recognize that some of the source IP addresses are not legitimate IP addresses for your network it might not be possible to identify legitimate FTP traffic from FTP DoS attack traffic.

Configuring NetFlow Layer 2 and Sec Mon Exports to Capture Traffic From a Simulated ICMP Attack Example

The following example shows how to use the NetFlow Layer 2 and Security Monitoring Exports feature to find out that your network is being attacked by ICMP traffic. It uses the network shown in the figure below. Host A is sending ICMP ping packets to the FTP server.

Figure 40: Test Network



Tip Keep track of the MAC addresses and IP addresses of the devices in your network. You can use them to analyze attacks and to resolve problems.

R2

```
!
hostname R2
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc02
 ip address 172.16.1.2 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc03
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.1 255.255.255.0
!
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R3

```
!
hostname R3
!
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture icmp
ip flow-capture ip-id
ip flow-capture mac-addresses
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc04
 no ip address
!
interface Ethernet0/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.2 255.255.255.0
 ip accounting output-packets
 ip flow ingress
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc05
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.1 255.255.255.0
 ip accounting output-packets
 ip flow egress
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

R4

```
!
hostname R4
!
```

```
interface Ethernet0/0
 mac-address aaaa.bbbb.cc07
 ip address 172.16.10.1 255.255.255.0
!
interface Ethernet1/0
 mac-address aaaa.bbbb.cc06
 no ip address
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.2 255.255.255.0
!
router rip
 version 2
 network 172.16.0.0
 no auto-summary
!
```

Analyze an ICMP Ping DoS Attack Using the show ip cache verbose flow command Example

The **show ip cache verbose flow** command displays the NetFlow flows. You can use this display output to identify the path that the ICMP traffic from Host A is taking as it is received and transmitted by R3.

Note To reduce the space required to display the output from the **show ip flow cache verbose flow**command only the ICMP flows are shown.

Tip Look for the flows that have ICMP in them and make a note of the interfaces, MAC addresses, and VLANs (if applicable) for the flows.

```
R3# show ip cache verbose flow
IP packet size distribution (122369 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .065 .665 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000 .000
    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .134 .000 .134 .000 .000 .000 .000 .000 .000
IP Flow Switching Cache, 278544 bytes
  24 active, 4072 inactive, 404 added
  176657 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  48 active, 976 inactive, 1088 added, 404 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
ICMP                27      0.0      1131   763      3.9    1557.4       3.6
Total:              380      0.0       267   257     13.0     382.8      12.6
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.106.1.1      Et1/0.1        172.16.10.2     01 00  10     864
0000 /0  0                     0800 /0  0     0.0.0.0               1500  1089.9
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      1500                           Max plen:       1500
Min TTL:        59                            Max TTL:         59
ICMP type:       8                            ICMP code:        0
IP id:           0
```

```
Et0/0.1         10.71.200.138   Et1/0.1         172.16.10.2     01 00  00     864
0000 /0  0                      0000 /0  0      0.0.0.0               554  1090.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       554                            Max plen:       554
Min TTL:         59                            Max TTL:         59
ICMP type:        0                            ICMP code:        0
IP id:            0                            FO:             185
Et0/0.1         10.231.185.254  Et1/0.1         172.16.10.2     01 00  00     864
0000 /0  0                      0000 /0  0      0.0.0.0               554  1090.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       554                            Max plen:       554
Min TTL:         59                            Max TTL:         59
ICMP type:        0                            ICMP code:        0
IP id:            0                            FO:             185
Et0/0.1         10.10.12.1      Et1/0.1         172.16.10.200   01 00  00     864
0000 /0  0                      0000 /0  0      0.0.0.0               554  1090.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       554                            Max plen:       554
Min TTL:         59                            Max TTL:         59
ICMP type:        0                            ICMP code:        0
IP id:            0                            FO:             185
Et0/0.1         10.132.221.111  Et1/0.1         172.16.10.2     01 00  10     864
0000 /0  0                      0800 /0  0      0.0.0.0              1500  1089.9
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       1500                            Max plen:       1500
Min TTL:         59                            Max TTL:         59
ICMP type:        8                            ICMP code:        0
IP id:            0
Et0/0.1         10.251.138.218  Et1/0.1         172.16.10.2     01 00  00     864
0000 /0  0                      0000 /0  0      0.0.0.0               554  1089.9
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       554                            Max plen:       554
Min TTL:         59                            Max TTL:         59
ICMP type:        0                            ICMP code:        0
IP id:            0                            FO:             185
Et0/0.1         10.10.12.1      Et1/0.1         172.16.10.200   01 00  10     864
0000 /0  0                      0C01 /0  0      0.0.0.0              1500  1090.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       1500                            Max plen:       1500
Min TTL:         59                            Max TTL:         59
ICMP type:       12                            ICMP code:        1
IP id:            0
Et0/0.1         10.106.1.1      Et1/0.1         172.16.10.2     01 00  00     864
0000 /0  0                      0000 /0  0      0.0.0.0               554  1089.9
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       554                            Max plen:       554
Min TTL:         59                            Max TTL:         59
ICMP type:        0                            ICMP code:        0
IP id:            0                            FO:             185
Et0/0.1         10.251.138.218  Et1/0.1         172.16.10.2     01 00  10     864
0000 /0  0                      0C01 /0  0      0.0.0.0              1500  1089.9
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       1500                            Max plen:       1500
Min TTL:         59                            Max TTL:         59
ICMP type:       12                            ICMP code:        1
IP id:            0
Et0/0.1         10.71.200.138   Et1/0.1         172.16.10.2     01 00  10     864
0000 /0  0                      0C01 /0  0      0.0.0.0              1500  1090.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       1500                            Max plen:       1500
Min TTL:         59                            Max TTL:         59
ICMP type:       12                            ICMP code:        1
IP id:            0
Et0/0.1         10.132.221.111  Et1/0.1         172.16.10.2     01 00  00     864
0000 /0  0                      0000 /0  0      0.0.0.0               554  1089.9
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
Min plen:       554                            Max plen:       554
Min TTL:         59                            Max TTL:         59
ICMP type:        0                            ICMP code:        0
IP id:            0                            FO:             185
Et0/0.1         10.231.185.254  Et1/0.1         172.16.10.2     01 00  10     864
0000 /0  0                      0C01 /0  0      0.0.0.0              1500  1090.0
MAC: (VLAN id) aaaa.bbbb.cc03  (005)           aaaa.bbbb.cc06  (006)
```

```
Min plen:       1500                            Max plen:       1500
Min TTL:         59                             Max TTL:         59
ICMP type:       12                             ICMP code:        1
IP id:            0
```

There are 12 ICMP flows shown in the output. You can use the Layer 2 information in the flows that is captured by the **ip flow-capture** command to identify the path the traffic is taking through the network. In this example, the traffic is being sent to R3 on VLAN 5 by R2. You can demonstrate that R2 is transmitting the traffic over interface 1/0.1 because the source MAC address (aaaa.bbb.cc03) belongs to 1/0.1 on R2. You can demonstrate that R3 is transmitting the traffic using VLAN 6 on interface 1/0.1 to interface 1/0.1 on R4, because the destination MAC address (aaaa.bbbb.cc06) belongs to interface 1/0.1 on R4.

Note For more information on the **ip flow-capture** command, and the fields in the display output of the **show ip cache verbose flow** command, refer to the *Cisco IOS NetFlow Command Reference* .

You can use this information to mitigate this attack. One possible way to mitigate this attack is by configuring an extended IP access list that blocks all ICMP traffic from the source IP addresses that Host A is spoofing and applying it Ethernet 0/0 on R2.

Analyze an ICMP Ping DoS Attack Using NetFlow Dynamic Top Talkers CLI Example

You can use the NetFlow Dynamic Top Talkers CLI feature to quickly identify the ICMP top talkers in the network traffic that might be sending the traffic. This will show you the IP source addresses that Host A is using as it sends the DoS attack traffic.

```
R3# show ip flow top 50 aggregate icmp
There are 3 top talkers:
ICMP TYPE  ICMP CODE       bytes        pkts       flows
=========  =========  ==========  ==========  ==========
       12          1     2466000        1644           4
        8          0     1233000         822           2
        0          0     1366164        2466           6
12 of 25 flows matched.
```

Note Only 12 of the 25 flows matched because the rest of the flows are not ICMP flows.

Tip The top talkers are displayed in descending order of the aggregated field by default.

After you have identified the ICMP types and code values in the network traffic, you need to determine the source IP addresses for the ICMP traffic that being sent to the FTP server.

```
R3# show ip flow top 50 aggregate source-address match icmp type 12 code 1
There are 4 top talkers:
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
10.251.138.218       867000         578           1
10.231.185.254       865500         577           1
10.71.200.138        865500         577           1
10.10.12.1           867000         578           1
4 of 24 flows matched.
```

Note Only source IP addresses from ICMP traffic are shown because of the **match icmp type** *12* **code** *1* criteria. No aggregation is performed on the source IP addresses because there is only one flow for IP each address.

Note Only four of the 24 flows matched because the rest of the flows did not meet the match criteria (**match icmp type** *12* **code** *1*).

```
R3# show ip flow top 50 aggregate source-address match icmp type 8 code 0

There are 2 top talkers:
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
10.132.221.111      1095000         730           1
10.106.1.1          1095000         730           1
2 of 24 flows matched.
```

Note Only source IP addresses from ICMP traffic are shown because of the **match icmp type** *8* **code** *0* criteria. No aggregation is performed on the source IP addresses because there is only one flow for IP each address.

Note Only two of the 24 flows matched because the rest of the flows did not meet the match criteria (**match icmp type** *8* **code** *0*).

```
R3# show ip flow top 50 aggregate source-address match icmp type 0 code 0
There are 6 top talkers:
IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
10.251.138.218       416608         752           1
10.231.185.254       416608         752           1
10.132.221.111       416608         752           1
10.106.1.1           416608         752           1
10.71.200.138        416608         752           1
10.10.12.1           416608         752           1
6 of 24 flows matched.
```

Note Only source IP addresses from ICMP traffic are shown because of the **match icmp type** *0* **code** *0* criteria. No aggregation is performed on the source IP addresses because there is only one flow for IP each address.

Note Only six of the 24 flows matched because the rest of the flows did not meet the match criteria (**match icmp type** *0* **code** *0*).

The next step is to create a list of the source IP addresses that Host A is using.

- 10.251.138.218
- 10.231.185.254
- 10.71.200.138
- 10.10.12.1

- 10.132.221.111
- 10.106.1.1.

Now that you know the source addresses of the ICMP DoS attack traffic, you can mitigate this attack by configuring an extended access list that blocks ICMP traffic from these address and applying it to the interface that is closest to the point that the traffic is entering your network.

Configure NetFlow Filtering and Sampling Example

This example configuration contains the configuration commands required to use NetFlow filtering and sampling on the NetFlow router.

```
!
hostname Router
!
ip cef
!
flow-sampler-map icmp-dos-fs-map
 mode random one-out-of 2
!
!
class-map match-any icmp-dos-class-map
 match access-group 101
!
!
policy-map icmp-dos-policy-map
  class icmp-dos-class-map
   netflow-sampler icmp-dos-fs-map
!
interface Ethernet0/0
 mac-address aaaa.bbbb.cc04
 no ip address
!
interface Ethernet0/0.1
 encapsulation dot1Q 5
 ip address 172.16.6.2 255.255.255.0
 service-policy input icmp-dos-policy-map
!
interface Ethernet1/0.1
 encapsulation dot1Q 6
 ip address 172.16.7.1 255.255.255.0
 ip flow egress
!
ip flow-capture fragment-offset
ip flow-capture packet-length
ip flow-capture ttl
ip flow-capture vlan-id
ip flow-capture icmp
ip flow-capture ip-id
ip flow-capture mac-addresses
!
ip flow-top-talkers
 top 5
 sort-by bytes
 match class-map icmp-dos-class-map
!
access-list 101 permit icmp any host 172.16.10.2
!
end
```

Where to Go Next

See the "Additional References" section for links to configuration information about additional NetFlow features and services.

Additional References

Related Documents

Related Topic	Document Title
Overview of Cisco IOS NetFlow	"Cisco IOS NetFlow Overview"
The minimum information about and tasks required for configuring NetFlow and NetFlow Data Export	"Getting Started with Configuring NetFlow and NetFlow Data Export"
Tasks for configuring NetFlow to capture and export network traffic data	"Configuring NetFlow and NetFlow Data Export"
Tasks for configuring Configuring MPLS Aware NetFlow	Configuring MPLS Aware NetFlow
Tasks for configuring MPLS egress NetFlow accounting	Configuring MPLS Egress NetFlow Accounting and Analysis
Tasks for configuring NetFlow input filters	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring Random Sampled NetFlow	"Using NetFlow Filtering or Sampling to Select the Network Traffic to Track"
Tasks for configuring NetFlow aggregation caches	"Configuring NetFlow Aggregation Caches"
Tasks for configuring NetFlow BGP next hop support	"Configuring NetFlow BGP Next Hop Support for Accounting and Analysis"
Tasks for configuring NetFlow multicast support	"Configuring NetFlow Multicast Accounting"
Tasks for configuring NetFlow Reliable Export With SCTP	NetFlow Reliable Export With SCTP
Tasks for configuring NetFlow Layer 2 and Security Monitoring Exports	"NetFlow Layer 2 and Security Monitoring Exports"
Tasks for configuring the SNMP NetFlow MIB	"Configuring SNMP and using the NetFlow MIB to Monitor NetFlow Data"

Related Topic	Document Title
Tasks for configuring the NetFlow MIB and Top Talkers feature	"Configuring NetFlow Top Talkers using Cisco IOS CLI Commands or SNMP Commands"
Information for installing, starting, and configuring the CNS NetFlow Collection Engine	"Cisco CNS NetFlow Collection Engine Documentation"

Standards

Standards	Title
There are no new or modified standards associated with this feature	--

MIBs

MIBs	MIBs Link
There are no new or modified MIBs associated with this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFCs	Title
There are no new or modified RFCs associated with this feature.	--

Technical Assistance

Description	Link
The Cisco Technical Support website contains thousands of pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/techsupport

Feature Information for Detecting and Analyzing Network Threats With 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 . An account on Cisco.com is not required.

Table 67: Feature Information for NetFlow Layer 2 and Security Monitoring Exports

Feature Name	Releases	Feature Configuration Information
NetFlow Layer 2 and Security Monitoring Exports	12.3(14)T	The NetFlow Layer 2 and Security Monitoring Exports feature enables the capture of values from fields in Layer 3 and Layer 2 of IP traffic for accounting and security analysis. The following commands were modified by this feature: **ip flow-capture**, **ip flow-export** and **show ip cache verbose flow**.
Support for capturing the value from the fragment offset field of IP headers added to NetFlow Layer 2 and Security Monitoring Exports[10]	12.4(2)T	The **fragment-offset** keyword for the **ip flow-capture** command **e**nables capturing the value of the IP fragment offset field from the first fragmented IP datagram in a flow.
NetFlow Top Talkers	12.3(11)T, 12.2(25)S	This document references the Top Talkers feature from the NetFlow MIB and Top Talkers feature documentation. Top Talkers uses NetFlow functionality to obtain information regarding heaviest traffic patterns and most-used applications in the network. The following commands were introduced by this feature: **cache-timeout**, **ip flow-top-talkers**, **match**, **show ip flow top-talkers**, **sort-by**, and **top**.

Feature Name	Releases	Feature Configuration Information
NetFlow Dynamic Top Talkers CLI	12.4(4)T	The NetFlow Dynamic Top Talkers CLI allows you to se an overview of the traffic characteristics on your router by aggregating flows based on the fields such as source IP address, destination prefix, and so forth.
NetFlow Input Filters	12.3(4)T, 12.2(25)S	This document references the NetFlow Input Filters feature from the NetFlow Filtering and Sampling feature documentation.
Random Sampled NetFlow	12.3(4)T, 12.2(18)S, 12.0(26)S	This document references the Random Sampled NetFlow feature from the NetFlow Filtering and Sampling feature documentation.

10 This is a minor enhancement. Minor enhancements are not typically listed in Feature Navigator.

Glossary

data flowset --A collection of data records that are grouped in an export packet.

export packet --A type of packet built by a device (for example, a router) with NetFlow services enabled. The packet is addressed to another device (for example, the NetFlow Collection Engine). The packet contains NetFlow statistics. The other device processes the packet (parses, aggregates, and stores information about IP flows).

flow --A set of packets with the same source IP address, destination IP address, protocol, source/destination ports, and type-of-service, and the same interface on which flow is monitored. Ingress flows are associated with the input interface, and egress flows are associated with the output interface.

flowset --A collection of flow records that follow the packet header in an export packet. A flowset contains information that must be parsed and interpreted by the NetFlow Collection Engine. There are two types of flowsets: template flowsets and data flowsets. An export packet contains one or more flowsets, and both template and data flowsets can be mixed in the same export packet.

NetFlow --Cisco IOS accounting feature that maintains per-flow information.

NetFlow Aggregation --A NetFlow feature that lets you summarize NetFlow export data on an IOS router before the data is exported to a NetFlow data collection system such as the NetFlow Collection Engine. This feature lowers bandwidth requirements for NetFlow export data and reduces platform requirements for NetFlow data collection devices.

NetFlow Collection Engine (formerly NetFlow FlowCollector)--Cisco application that is used with NetFlow on Cisco routers and Catalyst series switches. The NetFlow Collection Engine collects packets from the router that is running NetFlow and decodes, aggregates, and stores them. You can generate reports on various aggregations that can be set up on the NetFlow Collection Engine.

NetFlow v9 --NetFlow export format Version 9. A flexible and extensible means of carrying NetFlow records from a network node to a collector. NetFlow Version 9 has definable record types and is self-describing for easier NetFlow Collection Engine configuration.

template --Describes the layout of a data flowset.

template flowset --A collection of template records that are grouped in an export packet.

INDEX

B

N

T