Cisco IOS NetFlow Command Reference

February 2008

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

Customer Order Number:

Cisco IOS NetFlow Command Reference

CONTENTS

About Cisco IOS Software Documentation vii

- Documentation Objectives vii
- Audience vii
- Documentation Conventions vii
  - Typographic Conventions viii
  - Command Syntax Conventions viii
  - Software Conventions viii
  - Reader Alert Conventions ix
- Documentation Organization ix
  - Cisco IOS Documentation Set x
  - Cisco IOS Documentation on Cisco.com x
  - Configuration Guides, Command References, and Supplementary Resources xi
- Additional Resources and Documentation Feedback xvi

Using the Command-Line Interface in Cisco IOS Software xvii

- Initially Configuring a Device xvii
- Using the CLI xviii
  - Understanding Command Modes xviii
  - Using the Interactive Help Feature xx
  - Understanding Command Syntax xxi
  - Understanding Enable and Enable Secret Passwords xxii
  - Using the Command History Feature xxiii
  - Abbreviating Commands xxiv
  - Using Aliases for CLI Commands xxiv
  - Using the no and default Forms of Commands xxiv
  - Using the debug Command xxv
  - Filtering Output Using Output Modifiers xxv
  - Understanding CLI Error Messages xxvi
- Saving Changes to a Configuration xxvi
- Additional Information xxvii

NetFlow Commands NF-1

- backup (NetFlow SCTP) NF-2
- cache NF-5

cache-timeout NF-7
clear fm netflow counters NF-10
clear ip flow stats NF-11
clear mls nde flow counters NF-12
clear mls netflow NF-13
enabled (aggregation cache) NF-16
export destination NF-18
export destination sctp (NetFlow aggregation cache) NF-21
export template NF-23
export version NF-26
flow hardware mpls-vpn ip NF-29
flow-sampler NF-30
flow-sampler-map NF-32
ip flow NF-34
ip flow layer2-switched NF-36
ip flow-aggregation cache NF-38
ip flow-cache entries NF-41
ip flow-cache mpls label-positions NF-43
ip flow-cache timeout NF-46
ip flow-capture NF-48
ip flow-egress input-interface NF-54
ip flow-export destination NF-56
ip flow-export destination sctp NF-60
ip flow-export hardware version NF-62
ip flow-export interface-names NF-63
ip flow-export source NF-65
ip flow-export template NF-67
ip flow-export version NF-70
ip flow-export version (Supervisor Engine 2) NF-73
ip flow-export version (Supervisor Engine 720) NF-75
ip flow-top-talkers NF-77
ip multicast netflow NF-80
ip multicast netflow output-counters NF-82
ip multicast netflow rpf-failure NF-84
ip route-cache flow NF-85

mask (IPv4) **NF-86**
match (NetFlow) **NF-90**
mls aging fast **NF-95**
mls aging long **NF-96**
mls aging normal **NF-97**
mls flow **NF-98**
mls ip nat netflow-frag-l4-zero **NF-100**
mls nde flow **NF-101**
mls nde interface **NF-103**
mls nde sender **NF-105**
mls netflow **NF-106**
mls netflow interface **NF-107**
mls netflow maximum-flows **NF-108**
mls netflow sampling **NF-109**
mls netflow usage notify **NF-111**
mls sampling **NF-112**
mode (flow sampler configuration) **NF-115**
netflow-sampler **NF-117**
reliability (NetFlow SCTP) **NF-120**
show flow-sampler **NF-122**
show fm nat netflow data **NF-124**
show ip cache flow **NF-125**
show ip cache flow aggregation **NF-131**
show ip cache verbose flow **NF-139**
show ip cache verbose flow aggregation **NF-150**
show ip flow export **NF-157**
show ip flow top **NF-166**
show ip flow top-talkers **NF-167**
show mls ip non-static **NF-186**
show mls ip routes **NF-188**
show mls ip static **NF-190**
show mls nde **NF-192**
show mls netflow **NF-194**
show mls netflow ip **NF-199**
show mls netflow ip dynamic **NF-205**

show mls netflow ip routes **NF-207**
show mls netflow ip sw-installed **NF-209**
show mls netflow ipx **NF-211**
show mls sampling **NF-213**
sort-by **NF-214**
top **NF-216**

About Cisco IOS Software Documentation

This document describes the objectives, audience, conventions, and organization used in Cisco IOS software documentation. Also included are resources for obtaining technical assistance, additional documentation, and other information from Cisco. This document is organized into the following sections:

- Documentation Objectives, page v
- Audience, page v
- Documentation Conventions, page v
- Documentation Organization, page vii
- Additional Resources and Documentation Feedback, page xiv

Documentation Objectives

Cisco IOS software documentation describes the tasks and commands available to configure and maintain Cisco networking devices.

Audience

The Cisco IOS software documentation set is intended for users who configure and maintain Cisco networking devices (such as routers and switches) but who may not be familiar with the configuration and maintenance tasks, the relationship among tasks, or the Cisco IOS software commands necessary to perform particular tasks. The Cisco IOS software documentation set is also intended for those users experienced with Cisco IOS software who need to know about new features, new configuration options, and new software characteristics in the current Cisco IOS software release.

Documentation Conventions

In Cisco IOS software documentation, the term *router* may be used to refer to various Cisco products; for example, routers, access servers, and switches. These and other networking devices that support Cisco IOS software are shown interchangeably in examples and are used only for illustrative purposes. An example that shows one product does not necessarily mean that other products are not supported.

This section includes the following topics:

- Typographic Conventions, page vi
- Command Syntax Conventions, page vi
- Software Conventions, page vi
- Reader Alert Conventions, page vii

Typographic Conventions

Cisco IOS documentation uses the following typographic conventions:

Convention	Description
^ or Ctrl	Both the ^ symbol and Ctrl represent the Control (Ctrl) key on a keyboard. For example, the key combination **^D** or **Ctrl-D** means that you hold down the Control key while you press the D key. (Keys are indicated in capital letters but are not case sensitive.)
string	A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to *public*, do not use quotation marks around the string; otherwise, the string will include the quotation marks.

Command Syntax Conventions

Cisco IOS documentation uses the following command syntax conventions:

Convention	Description
bold	Bold text indicates commands and keywords that you enter as shown.
italics	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
|	A vertical line, called a pipe, indicates a choice within a set of keywords or arguments.
[x | y]	Square brackets enclosing keywords or arguments separated by a pipe indicate an optional choice.
{x | y}	Braces enclosing keywords or arguments separated by a pipe indicate a required choice.
[x {y | z}]	Braces and a pipe within square brackets indicate a required choice within an optional element.

Software Conventions

Cisco IOS software uses the following program code conventions:

Convention	Description
`Courier font`	Courier font is used for information that is displayed on a PC or terminal screen.
`Bold Courier font`	Bold Courier font indicates text that the user must enter.

Convention	Description
< >	Angle brackets enclose text that is not displayed, such as a password. Angle brackets also are used in contexts in which the italic font style is not supported; for example, ASCII text.
!	An exclamation point at the beginning of a line indicates that the text that follows is a comment, not a line of code. An exclamation point is also displayed by Cisco IOS software for certain processes.
[ ]	Square brackets enclose default responses to system prompts.

Reader Alert Conventions

The Cisco IOS documentation set uses the following conventions for reader alerts:

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

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

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

Documentation Organization

This section describes the Cisco IOS documentation set, how it is organized, and how to access it on Cisco.com. Included are lists of configuration guides, command references, and supplementary references and resources that make up the documentation set. The following topics are included:

- Cisco IOS Documentation Set, page viii
- Cisco IOS Documentation on Cisco.com, page viii
- Configuration Guides, Command References, and Supplementary Resources, page ix

Cisco IOS Documentation Set

Cisco IOS software documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS software code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS software release.
  - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS software features.
  - Command references—Compilations of commands that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides.
- Lists of all the commands in a specific release and all commands that are new, modified, removed, or replaced in the release.
- Command reference book for **debug** commands. Commands are listed in alphabetical order.
- Reference book for system messages for all Cisco IOS releases.

Cisco IOS Documentation on Cisco.com

The following sections describe the documentation organization and how to access various document types.

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

New Features List

The New Features List for each release provides a list of all features in the release with hyperlinks to the feature guides in which they are documented.

Feature Guides

Cisco IOS features are documented in feature guides. Feature guides describe one feature or a group of related features that are supported on many different software releases and platforms. Your Cisco IOS software release or platform may not support all the features documented in a feature guide. See the Feature Information table at the end of the feature guide for information about which features in that guide are supported in your software release.

Configuration Guides

Configuration guides are provided by technology and release and comprise a set of individual feature guides relevant to the release and technology.

Command References

Command reference books contain Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about Cisco IOS commands, see the Cisco IOS Master Commands List, or the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page xiii.

Configuration Guides, Command References, and Supplementary Resources

Table 1 lists in alphabetical order Cisco IOS software configuration guides and command references, including brief descriptions of the contents of the documents. The configuration guides and command references listed support many different software releases and platforms. Your Cisco IOS software release or platform may not support all these technologies.

Table 2 lists documents and resources that supplement the Cisco IOS software configuration guides and command references. These supplementary resources include release notes and caveats; master command lists; new, modified, removed, and replaced command lists; system messages; and the debug command reference.

Table 1 Cisco IOS Configuration Guides and Command References

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS AppleTalk Configuration Guide *Cisco IOS AppleTalk Command Reference*	AppleTalk protocol.
Cisco IOS Asynchronous Transfer Mode Configuration Guide *Cisco IOS Asynchronous Transfer Mode Command Reference*	LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM.
Cisco IOS Bridging and IBM Networking Configuration Guide *Cisco IOS Bridging Command Reference* *Cisco IOS IBM Networking Command Reference*	• Transparent and source-route transparent (SRT) bridging, source-route bridging (SRB), Token Ring Inter-Switch Link (TRISL), and token ring route switch module (TRRSM). • Data-link switching plus (DLSw+), serial tunnel (STUN), block serial tunnel (BSTUN); logical link control, type 2 (LLC2), synchronous data link control (SDLC); IBM Network Media Translation, including Synchronous Data Logical Link Control (SDLLC) and qualified LLC (QLLC); downstream physical unit (DSPU), Systems Network Architecture (SNA) service point, SNA frame relay access, advanced peer-to-peer networking (APPN), native client interface architecture (NCIA) client/server topologies, and IBM Channel Attach.
Cisco IOS Broadband and DSL Configuration Guide *Cisco IOS Broadband and DSL Command Reference*	Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).
Cisco IOS Carrier Ethernet Configuration Guide *Cisco IOS Carrier Ethernet Command Reference*	Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).
Cisco IOS Configuration Fundamentals Configuration Guide *Cisco IOS Configuration Fundamentals Command Reference*	Autoinstall, Setup, Cisco IOS command-line interface (CLI), Cisco IOS file system (IFS), Cisco IOS web browser user interface (UI), basic file transfer services, and file management.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS DECnet Configuration Guide *Cisco IOS DECnet Command Reference*	DECnet protocol.
Cisco IOS Dial Technologies Configuration Guide *Cisco IOS Dial Technologies Command Reference*	Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).
Cisco IOS Flexible NetFlow Configuration Guide *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.
Cisco IOS H.323 Configuration Guide	Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing.
Cisco IOS High Availability Command Reference	A variety of High Availability (HA) features and technologies that are available for different network segments (from enterprise access to service provider core) to facilitate creation of end-to-end highly available networks. Cisco IOS HA features and technologies can be categorized in three key areas: system-level resiliency, network-level resiliency, and embedded management for resiliency.
Cisco IOS Intelligent Service Gateway Configuration Guide *Cisco IOS Intelligent Service Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring.
Cisco IOS Interface and Hardware Component Configuration Guide *Cisco IOS Interface and Hardware Component Command Reference*	LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration.
Cisco IOS IP Addressing Services Configuration Guide *Cisco IOS IP Addressing Services Command Reference*	Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP).
Cisco IOS IP Application Services Configuration Guide *Cisco IOS IP Application Services Command Reference*	Enhanced Object Tracking (EOT), Gateway Load Balancing Protocol (GLBP), Hot Standby Router Protocol (HSRP), IP Services, Server Load Balancing (SLB), Stream Control Transmission Protocol (SCTP), TCP, Web Cache Communication Protocol (WCCP), User Datagram Protocol (UDP), and Virtual Router Redundancy Protocol (VRRP).
Cisco IOS IP Mobility Configuration Guide *Cisco IOS IP Mobility Command Reference*	Mobile ad hoc networks (MANet) and Cisco mobile networks.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS IP Multicast Configuration Guide *Cisco IOS IP Multicast Command Reference*	Protocol Independent Multicast (PIM) sparse mode (PIM-SM), bidirectional PIM (bidir-PIM), Source Specific Multicast (SSM), Multicast Source Discovery Protocol (MSDP), Internet Group Management Protocol (IGMP), and Multicast VPN (MVPN).
Cisco IOS IP Routing Protocols Configuration Guide *Cisco IOS IP Routing Protocols Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP).
Cisco IOS IP SLAs Configuration Guide *Cisco IOS IP SLAs Command Reference*	Cisco IOS IP Service Level Agreements (IP SLAs).
Cisco IOS IP Switching Configuration Guide *Cisco IOS IP Switching Command Reference*	Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS).
Cisco IOS IPv6 Configuration Guide *Cisco IOS IPv6 Command Reference*	For IPv6 features, protocols, and technologies, go to the IPv6 "Start Here" document at http://www.cisco.com/en/US/products/ps6441/products_configuration_guide_chapter09186a00801d65ed.html
Cisco IOS ISO CLNS Configuration Guide *Cisco IOS ISO CLNS Command Reference*	ISO connectionless network service (CLNS).
Cisco IOS LAN Switching Configuration Guide *Cisco IOS LAN Switching Command Reference*	VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS).
Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide *Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference*	Cisco IOS Gateway GPRS Support Node (GGSN) in a 2.5-generation general packet radio service (GPRS) and 3-generation universal mobile telecommunication system (UMTS) network.
Cisco IOS Mobile Wireless Home Agent Configuration Guide *Cisco IOS Mobile Wireless Home Agent Command Reference*	Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided.
Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide *Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference*	Cisco Packet Data Serving Node (PDSN), a wireless gateway that is between the mobile infrastructure and standard IP networks and that enables packet data services in a code division multiple access (CDMA) environment.
Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide *Cisco IOS Mobile Wireless Radio Access Networking Command Reference*	Cisco IOS radio access network products.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Multiprotocol Label Switching Configuration Guide *Cisco IOS Multiprotocol Label Switching Command Reference*	MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs.
Cisco IOS Multi-Topology Routing Configuration Guide *Cisco IOS Multi-Topology Routing Command Reference*	Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support.
Cisco IOS NetFlow Configuration Guide *Cisco IOS NetFlow Command Reference*	Network traffic data analysis, aggregation caches, export features.
Cisco IOS Network Management Configuration Guide *Cisco IOS Network Management Command Reference*	Basic system management; system monitoring and logging; troubleshooting, logging, and fault management; Cisco Discovery Protocol; Cisco IOS Scripting with Tool Control Language (Tcl); Cisco networking services (CNS); DistributedDirector; Embedded Event Manager (EEM); Embedded Resource Manager (ERM); Embedded Syslog Manager (ESM); HTTP; Remote Monitoring (RMON); SNMP; and VPN Device Manager Client for Cisco IOS Software (XSM Configuration).
Cisco IOS Novell IPX Configuration Guide *Cisco IOS Novell IPX Command Reference*	Novell Internetwork Packet Exchange (IPX) protocol.
Cisco IOS Optimized Edge Routing Configuration Guide *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization.
Cisco IOS Quality of Service Solutions Configuration Guide *Cisco IOS Quality of Service Solutions Command Reference*	Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED).
Cisco IOS Security Configuration Guide *Cisco IOS Security Command Reference*	Access control lists (ACLs), authentication, authorization, and accounting (AAA), firewalls, IP security and encryption, neighbor router authentication, network access security, network data encryption with router authentication, public key infrastructure (PKI), RADIUS, TACACS+, terminal access security, and traffic filters.
Cisco IOS Service Selection Gateway Configuration Guide *Cisco IOS Service Selection Gateway Command Reference*	Subscriber authentication, service access, and accounting.

Table 1 Cisco IOS Configuration Guides and Command References (continued)

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
Cisco IOS Software Modularity Installation and Configuration Guide *Cisco IOS Software Modularity Command Reference*	Installation and basic configuration of software modularity images, including installations on single and dual route processors, installation rollbacks, software modularity binding, software modularity processes and patches.
Cisco IOS Terminal Services Configuration Guide *Cisco IOS Terminal Services Command Reference*	DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD).
Cisco IOS Virtual Switch Command Reference	Virtual switch redundancy, high availability, and packet handling; converting between standalone and virtual switch modes; virtual switch link (VSL); Virtual Switch Link Protocol (VSLP).
Cisco IOS Voice Configuration Library *Cisco IOS Voice Command Reference*	Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications.
Cisco IOS VPDN Configuration Guide *Cisco IOS VPDN Command Reference*	Layer 2 Tunneling Protocol (L2TP) dial-out load balancing and redundancy, L2TP extended failover, L2TP security VPDN, multihop by Dialed Number Identification Service (DNIS), timer and retry enhancements for L2TP and Layer 2 Forwarding (L2F), RADIUS Attribute 82: tunnel assignment ID, shell-based authentication of VPDN users, tunnel authentication via RADIUS on tunnel terminator.
Cisco IOS Wide-Area Networking Configuration Guide *Cisco IOS Wide-Area Networking Command Reference*	Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25.
Cisco IOS Wireless LAN Configuration Guide *Cisco IOS Wireless LAN Command Reference*	Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA).

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title	Description
Cisco IOS Master Commands List	Alphabetical list of all the commands documented in the Cisco IOS release.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for the Cisco IOS release.
Cisco IOS Software System Messages	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.

Table 2 Cisco IOS Supplementary Documents and Resources (continued)

Document Title	Description
Release Notes and Caveats	Information about new and changed features, system requirements, and other useful information about specific software releases; information about defects in specific Cisco IOS software releases.
MIBs	Files used for network monitoring. To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator at http://www.cisco.com/go/mibs
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS software documentation references where applicable. The full text of referenced RFCs may be obtained at http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

- Technical documentation
- Cisco product security overview
- Product alerts and field notices
- Technical assistance

Cisco IOS technical documentation includes embedded feedback forms where you can rate documents and provide suggestions for improvement. Your feedback helps us improve our documentation.

Using the Command-Line Interface in Cisco IOS Software

This document provides basic information about the command-line interface (CLI) in Cisco IOS software and how you can use some of the CLI features. This document contains the following sections:

- Initially Configuring a Device, page xv
- Using the CLI, page xvi
- Saving Changes to a Configuration, page xxiv
- Additional Information, page xxv

For more information about using the CLI, see the "Using the Cisco IOS Command-Line Interface (CLI)" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

For information about the Cisco IOS software documentation set, see "About Cisco IOS Software Documentation."

Initially Configuring a Device

Initially configuring a device varies by platform. For information about performing an initial configuration, see the hardware installation documentation that is provided with the original packaging of the product or go to the Product Support area of Cisco.com at http://www.cisco.com/web/psa/products/index.html.

After you have performed the initial configuration and connected the device to your network, you can configure the device either by using the console port or Telnet to access the Cisco IOS CLI or by using the configuration method provided on the device, such as Security Device Manager.

Changing the Default Settings for a Console or AUX Port

There are only two changes that you can make to a console port and an AUX port:

- Change the port speed with the **config-register 0x** command. Changing the port speed is not recommended. The well-known default speed is 9600.
- Change the behavior of the port; for example, by adding a password or changing the timeout value.

Using the CLI

This section describes the following topics:

- Understanding Command Modes, page xvi
- Using the Interactive Help Feature, page xviii
- Understanding Command Syntax, page xix
- Understanding Enable and Enable Secret Passwords, page xx
- Using the Command History Feature, page xxi
- Abbreviating Commands, page xxii
- Using Aliases for CLI Commands, page xxii
- Using the no and default Forms of Commands, page xxii
- Using the debug Command, page xxiii
- Filtering Output Using Output Modifiers, page xxiii
- Understanding CLI Error Messages, page xxiv

Understanding Command Modes

The CLI command mode structure is hierarchical, and each mode supports a set of specific commands. This section describes the most common of the many modes that exist.

Table 3 lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 3 CLI Command Modes

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
User EXEC	Log in.	`Router>`	Issue the **logout** or **exit** command.	• Change terminal settings. • Perform basic tests. • Display device status.
Privileged EXEC	From user EXEC mode, issue the **enable** command.	`Router#`	Issue the **disable** command or the **exit** command to return to user EXEC mode.	• Issue **show** and **debug** commands. • Copy images to the device. • Reload the device. • Manage device configuration files. • Manage device file systems.

Table 3 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
Global configuration	From privileged EXEC mode, issue the **configure terminal** command.	`Router(config)#`	Issue the **exit** command or the **end** command to return to privileged EXEC mode.	Configure the device.
Interface configuration	From global configuration mode, issue the **interface** command.	`Router(config-if)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual interfaces.
Line configuration	From global configuration mode, issue the **line vty** or **line console** command.	`Router(config-line)#`	Issue the **exit** command to return to global configuration mode or the **end** command to return to privileged EXEC mode.	Configure individual terminal lines.
ROM monitor	From privileged EXEC mode, issue the **reload** command. Press the **Break** key during the first 60 seconds while the system is booting.	`rommon # >` # is the line number and increments at each prompt.	Issue the **continue** command.	• Runs as the default operating mode when a valid Cisco IOS image cannot be loaded. • Access the fall-back procedure for loading a Cisco IOS image when the device lacks a valid Cisco IOS image and cannot be booted. • Perform password recovery when a CTRL-Break sequence is issued within 60 seconds of a power-on or reload event.

EXEC commands are not saved when the software reboots. Commands that you issue in a configuration mode can be saved to the startup configuration. If you save the running configuration to the startup configuration, these commands will execute when the software is rebooted. Global configuration mode is the highest level of configuration mode. From global configuration mode, you can enter a variety of other configuration modes, including protocol-specific modes.

ROM monitor mode is a separate mode that is used when the Cisco IOS software cannot load properly. If a valid software image is not found when the software boots or if the configuration file is corrupted at startup, the software might enter ROM monitor mode. Use the question symbol (?) to view the commands that you can use while the device is in ROM monitor mode.

```
rommon 1 > ?
alias              set and display aliases command
boot               boot up an external process
confreg            configuration register utility
```

```
cont                continue executing a downloaded image
context             display the context of a loaded image
cookie              display contents of cookie PROM in hex
.
.
.
rommon 2 >
```

The following example shows how the command prompt changes to indicate a different command mode:

```
Router> enable
Router# configure terminal
Router(config)# interface ethernet 1/1
Router(config-if)# ethernet
Router(config-line)# exit
Router(config)# end
Router#
```

Note A keyboard alternative to the **end** command is Ctrl-Z.

Using the Interactive Help Feature

The Cisco IOS CLI includes an interactive Help feature. Table 4 describes how to use the Help feature.

Table 4 CLI Interactive Help Commands

Command	Purpose
help	Provides a brief description of the help feature in any command mode.
?	Lists all commands available for a particular command mode.
partial command?	Provides a list of commands that begin with the character string (no space between the command and the question mark).
partial command<**Tab**>	Completes a partial command name (no space between the command and <Tab>).
command **?**	Lists the keywords, arguments, or both associated with the command (space between the command and the question mark).
command keyword **?**	Lists the arguments that are associated with the keyword (space between the keyword and the question mark).

The following examples show how to use the help commands:

help

```
Router> help

Help may be requested at any point in a command by entering a question mark '?'.  If
nothing matches, the help list will be empty and you must backup until entering a '?'
shows the available options.

Two styles of help are provided:

1. Full help is available when you are ready to enter a command argument (e.g. 'show ?')
and describes each possible argument.

2. Partial help is provided when an abbreviated argument is entered and you want to know
what arguments match the input (e.g. 'show pr?'.)
```

?

```
Router# ?
Exec commands:
  access-enable        Create a temporary access-List entry
  access-profile       Apply user-profile to interface
  access-template      Create a temporary access-List entry
  alps                 ALPS exec commands
  archive              manage archive files
<snip>
```

***partial command*?**

```
Router(config)# zo?
zone  zone-pair
```

***partial command*<Tab>**

```
Router(config)# we<Tab> webvpn
```

***command* ?**

```
Router(config-if)# pppoe ?
  enable        Enable pppoe
  max-sessions  Maximum PPPOE sessions
```

***command keyword* ?**

```
Router(config-if)# pppoe enable ?
  group  attach a BBA group
  <cr>
```

Understanding Command Syntax

Command syntax is the format in which a command should be entered in the CLI. Commands include the name of the command, keywords, and arguments. Keywords are alphanumeric strings that are used literally. Arguments are placeholders for values that a user must supply. Keywords and arguments may be required or optional.

Specific conventions convey information about syntax and command elements. Table 5 describes these conventions.

Table 5 CLI Syntax Conventions

Symbol/Text	Function	Notes
< > (angle brackets)	Indicate that the option is an argument.	Sometimes arguments are displayed without angle brackets.
A.B.C.D.	Indicates that you must enter a dotted decimal IP address.	Angle brackets (< >) are not always used to indicate that an IP address is an argument.
WORD (all capital letters)	Indicates that you must enter one word.	Angle brackets (< >) are not always used to indicate that a WORD is an argument.

Table 5 CLI Syntax Conventions (continued)

Symbol/Text	Function	Notes
LINE (all capital letters)	Indicates that you must enter more than one word.	Angle brackets (< >) are not always used to indicate that a LINE is an argument.
<cr> (carriage return)	Indicates the end of the list of available keywords and arguments, and also indicates when keywords and arguments are optional. When <cr> is the only option, you have reached the end of the branch or the end of the command if the command has only one branch.	—

The following examples show syntax conventions:

```
Router(config)# ethernet cfm domain ?
  WORD  domain name
Router(config)# ethernet cfm domain dname ?
  level
Router(config)# ethernet cfm domain dname level ?
  <0-7>  maintenance level number
Router(config)# ethernet cfm domain dname level 7 ?
  <cr>
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
Router(config)# logging host ?
  Hostname or A.B.C.D  IP address of the syslog server
  ipv6                 Configure IPv6 syslog server
Router(config)# snmp-server file-transfer access-group 10 ?
  protocol  protocol options
  <cr>
```

Understanding Enable and Enable Secret Passwords

Some privileged EXEC commands are used for actions that impact the system, and it is recommended that you set a password for these commands to prevent unauthorized use. Two types of passwords, enable (not encrypted) and enable secret (encrypted), can be set. The following commands set these passwords and are issued in global configuration mode:

- **enable** *password*
- **enable secret** *password*

Using an enable secret password is recommended because it is encrypted and more secure than the enable password. When you use an enable secret password, text is encrypted (unreadable) before it is written to the config.text file. When you use an enable password, the text is written as entered (readable) to the config.text file.

Each type of password is case sensitive, can contain from 1 to 25 uppercase and lowercase alphanumeric characters, and can start with a number. Spaces are also valid password characters; for example, “two words” is a valid password. Leading spaces are ignored, but trailing spaces are recognized.

Note Both password commands have numeric keywords that are single integer values. If you choose a number for the first character of your password followed by a space, the system will read the number as if it were the numeric keyword and not as part of your password.

When both passwords are set, the enable secret password takes precedence over the enable password.

To remove a password, use the **no** form of the commands: **no enable** *password* or **no enable secret** *password*.

For more information about password recovery procedures for Cisco products, see http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml.

Using the Command History Feature

The CLI command history feature saves the commands you enter during a session in a command history buffer. The default number of commands saved is 10, but the number is configurable within the range of 0 to 256. This command history feature is particularly useful for recalling long or complex commands.

To change the number of commands saved in the history buffer for a terminal session, issue the **terminal history size** command:

```
Router# terminal history size num
```

A command history buffer is also available in line configuration mode with the same default and configuration options. To set the command history buffer size for a terminal session in line configuration mode, issue the **history** command:

```
Router(config-line)# history [size num]
```

To recall commands from the history buffer, use the following methods:

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- Press Ctrl-N or the down arrow key—Recalls the most recent commands in the history buffer after they have been recalled using Ctrl-P or the up arrow key. Repeat the key sequence to recall successively more recent commands.

Note The arrow keys function only on ANSI-compatible terminals such as the VT100.

- Issue the **show history** command in user EXEC or privileged EXEC mode—Lists the most recent commands that you entered. The number of commands that are displayed is determined by the setting of the **terminal history size** and **history** commands.

  The CLI command history feature is enabled by default. To disable this feature for a terminal session, issue the **terminal no history** command in user EXEC or privileged EXEC mode or the **no history** command in line configuration mode.

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The Cisco IOS CLI recognizes an abbreviated command when the abbreviation contains enough characters to uniquely identify the command. For example, the **show version** command can be abbreviated as **sh ver**. It cannot be abbreviated as **s ver** because **s** could mean **show**, **set**, or **systat**. The **sh v** abbreviation also is not valid because the **show** command has **vrrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

To save time and the repetition of entering the same command multiple times, you can use a command alias. An alias can be configured to do anything that can be done at the command line, but an alias cannot move between modes, type in passwords, or perform any interactive functions.

Table 6 shows the Cisco IOS software default command aliases.

Table 6 Default Command Aliases

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show
u or **un**	undebug
w	where

To create a command alias, issue the **alias** command in global configuration mode. The syntax of the command is **alias** *mode command-alias original-command*. Following are some examples:

- Router(config)# **alias exec prt partition**—privileged EXEC mode
- Router(config)# **alias configure sb source-bridge**—global configuration mode
- Router(config)# **alias interface rl rate-limit**—interface configuration mode

To view both default and user-created aliases, issue the **show alias** command.

For more information about the **alias** command, see http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

Most configuration commands have a **no** form that is used to reset a command to its default value or disable a feature or function. For example, the **ip routing** command is enabled by default. To disable this command, you would issue the **no ip routing** command. To re-enable IP routing, you would issue the **ip routing** command.

Configuration commands may also have a **default** form, which returns the command settings to their default values. For commands that are disabled by default, using the **default** form has the same effect as using the **no** form of the command. For commands that are enabled by default and have default settings, the **default** form enables the command and returns the settings to their default values.

The **no** and **default** forms of commands are described in the command pages of Cisco IOS software command references.

Using the debug Command

A **debug** command produces extensive output that helps you troubleshoot problems in your network. These commands are available for many features and functions within Cisco IOS software. Some **debug** commands are **debug all**, **debug aaa accounting**, and **debug mpls packets**. To use **debug** commands during a Telnet session with a device, you must first enter the **terminal monitor** command. To turn off debugging completely, you must enter the **undebug all** command.

For more information about **debug** commands, see the *Cisco IOS Debug Command Reference* at http://www.cisco.com/en/US/docs/ios/debug/command/reference/db_book.html.

Caution Debugging is a high priority and high CPU utilization process that can render your device unusable. Use **debug** commands only to troubleshoot specific problems. The best times to run debugging are during periods of low network traffic and when few users are interacting with the network. Debugging during these periods decreases the likelihood that the **debug** command processing overhead will affect network performance or user access or response times.

Filtering Output Using Output Modifiers

Many Cisco IOS commands produce lengthy output that may use several screens to display. Using output modifiers, you can filter this output to show only the information that you want to see.

Three output modifiers are available and are described as follows:

- **begin** *regular expression*—Displays the first line in which a match of the regular expression is found and all lines that follow.
- **include** *regular expression*—Displays all lines in which a match of the regular expression is found.
- **exclude** *regular expression*—Displays all lines except those in which a match of the regular expression is found.

To use one of these output modifiers, type the command followed by the pipe symbol (|), the modifier, and the regular expression that you want to search for or filter. A regular expression is a case-sensitive alphanumeric pattern. It can be a single character or number, a phrase, or a more complex string.

The following example illustrates how to filter output of the **show interface** command to display only lines that include the expression “protocol.”

```
Router# show interface | include protocol

FastEthernet0/0 is up, line protocol is up
Serial4/0 is up, line protocol is up
Serial4/1 is up, line protocol is up
Serial4/2 is administratively down, line protocol is down
Serial4/3 is administratively down, line protocol is down
```

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. Table 7 shows the common CLI error messages.

Table 7 Common CLI Error Messages

Error Message	Meaning	How to Get Help
% Ambiguous command: "show con"	You did not enter enough characters for the command to be recognized.	R-enter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Incomplete command.	You did not enter all the keywords or values required by the command.	Reenter the command followed by a space and a question mark (?). The keywords that you are allowed to enter for the command appear.
% Invalid input detected at "^" marker.	You entered the command incorrectly. The caret (^) marks the point of the error.	Enter a question mark (?) to display all the commands that are available in this command mode. The keywords that you are allowed to enter for the command appear.

For more system error messages, see the following documents:

- *Cisco IOS Release 12.2SR System Message Guide*
- *Cisco IOS System Messages, Volume 1 of 2* (Cisco IOS Release 12.4)
- *Cisco IOS System Messages, Volume 2 of 2* (Cisco IOS Release 12.4)

Saving Changes to a Configuration

To save changes that you made to the configuration of a device, you must issue the **copy running-config startup-config** command or the **copy system:running-config nvram:startup-config** command. When you issue these commands, the configuration changes that you made are saved to the startup configuration and saved when the software reloads or power to the device is turned off or interrupted. The following example shows the syntax of the **copy running-config startup-config** command:

```
Router# copy running-config startup-config
Destination filename [startup-config]?
```

You press Enter to accept the startup-config filename (the default), or type a new filename and then press Enter to accept that name. The following output is displayed indicating that the configuration was saved:

```
Building configuration...
[OK]
Router#
```

On most platforms, the configuration is saved to NVRAM. On platforms with a Class A flash file system, the configuration is saved to the location specified by the CONFIG_FILE environment variable. The CONFIG_FILE variable defaults to NVRAM.

Additional Information

- "Using the Cisco IOS Command-Line Interface (CLI)" section of the *Cisco IOS Configuration Fundamentals Configuration Guide*.

  http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
- Cisco Product Support Resources

  http://www.cisco.com/web/psa/products/index.html
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- *White Paper: Cisco IOS Reference Guide*

  http://www.cisco.com/en/US/products/sw/iosswrel/ps1828/products_white_paper09186a008018305e.shtml
- Software Download Center (downloads; tools; licensing, registration, advisory, and general information) (requires Cisco.com User ID and password)

  http://www.cisco.com/kobayashi/sw-center/
- Error Message Decoder, a tool to help you research and resolve error messages for Cisco IOS software

  http://www.cisco.com/pcgi-bin/Support/Errordecoder/index.cgi
- Command Lookup Tool, a tool to help you find detailed descriptions of Cisco IOS commands (requires Cisco.com User ID and password)

  http://tools.cisco.com/Support/CLILookup/cltSearchAction.do
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

  https://www.cisco.com/pcgi-bin/Support/OutputInterpreter/home.pl\

NetFlow Commands

backup (NetFlow SCTP)

To configure a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries, use the **backup** command in NetFlow ip flow export stream control transmission protocol (SCTP) configuration mode. To remove a destination for the reliable export of NetFlow accounting information, use the **no** form of this command.

backup {**destination** {*ip-address* | *hostname*} *sctp-port* | **fail-over** *time* | **mode** {**fail-over** | **redundant**} | **restore-time** *time*}

no backup {**destination** {*ip-address* | *hostname*} *sctp-port* | **fail-over** | **mode** {**fail-over** | **redundant**} | **restore-time**}

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
port	Specifies the number of the stream control transmission protocol (SCTP) port on which the workstation is listening for the exported NetFlow datagrams.
fail-over *time*	(Optional) Specifies the length of time that the primary export destination must be unavailable before SCTP starts using the backup export destination. The default fail-over time for sctp to start using a backup export destination is 25 milliseconds (msec). Range: 0 to 3600 msec.
mode {**fail-over** | **redundant**}	(Optional) Specifies the mode that SCTP will use to establish a connection to the backup export destination: • **fail-over**—Opens an association with the backup export destination when the primary export destination becomes unavailable • **redundant**—Maintains a permanent association with the backup export destination.
restore-time *time*	(Optional) Specifies the length of time that the primary export destination must be available after an outage before SCTP reverts back to it. This is applicable only when SCTP is using the backup export destination. Range: 0 to 3600 seconds.

Command Default

Backup destinations for the reliable export of NetFlow information are not configured.

Command Modes

NetFlow ip flow export SCTP (config-flow-export-sctp)

Usage Guidelines

When you configure a backup export destination for SCTP messages are sent to the destination if the primary export destination becomes unavailable. When connectivity with the primary export destination has been lost and a backup export destination is configured, SCTP begins using the backup export destination. The default period of time that SCTP waits until it starts using the backup export destination is 25 sec. You can configure a different with the **fail-over** *time* command.

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.

The router sends periodic SCTP heart beat messages to the SCTP export destinations that you have configured. The router uses the SCTP heart-beat message acknowledgments from the export destinations to monitor the status of each export destination. This allows an application, such as NetFlow, to be quickly informed when connectivity to an export destination 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 export destination until the router has not received acknowledgments for the SCTP heart beat messages from the primary export destination for the time specified by the **fail-over** *time* command. When the router is configured with SCTP backup in redundant mode, the router activates the association with the backup export destination immediately instead of waiting for the primary export destination to fail. The router will not start sending SCTP messages to a backup export destination in redundant mode until the router has not received acknowledgements for the SCTP heart beat messages from the primary export destination for the time specified by the **fail-over** *time* command. Fail-over mode is the preferred method when the backup export destination is on the end of an expensive lower-bandwidth link such as ISDN.

During the time that SCTP is using the backup export destination, SCTP continues to try to restore the association with the primary export destination. SCTP makes this attempt until connectivity is restored or the primary SCTP export destination is removed from the configuration.

When connectivity to the primary export destination is available again, the router waits for a period of time before reverting to using it as the primary destination. You use the **restore-time** *time command to* configure the value of the period of time that SCTP waits until reverting. The default period of time that SCTP waits is 25 msecs.

Under either fail-over mode, any records which have been queued between loss of connectivity with the primary destination and, the establishing of the association with the backup export destination might be lost. A count of how many records were lost can be viewed through the use of the **show ip flow export sctp verbose** command.

To avoid a flapping SCTP association with an export destination (the SCTP association going 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). This causes the IP route to the primary export destination to be added to and removed from the routing table (route flapping) every 2000 msec (2 sec) you need to configure the restore time for a value greater than 2000 msec.

The backup connection uses stream 0 for sending templates, options templates, and option records. The data stream(s) inherit the reliability settings of the primary export destination.

Command History

Release	Modification
12.4(4)T	This command was introduced.

Examples

The following example shows how to configure the networking device to use SCTP as the transport protocol for transmissions to multiple export destinations in redundant mode. The router activates the association with the backup export destination immediately instead of waiting until the primary export destination fails. The router starts sending SCTP messages to the backup export destination over the

preexisting association after it fails to receive acknowledgments for its SCTP heart-beat messages from the primary export destination for 1500 msec. The router waits 3000 msec after the primary export destination is reachable again before resuming the association with the primary export destination.

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# backup destination 172.16.10.3 78
Router(config-flow-export-sctp)# backup mode redundant
Router(config-flow-export-sctp)# backup fail-over 1500
Router(config-flow-export-sctp)# backup restore-time 3000
```

The following example shows how to configure the networking device to use SCTP as the transport protocol to multiple export destinations in fail-over mode. The router activates the association with the backup export destination and starts sending SCTP messages to the backup export destination after it fails to receive acknowledgments for its SCTP heart beat messages from the primary export destination for 1500 msec. The router waits 3000 sec after the primary export destination is reachable again before resuming the association with the primary export destination. The SCTP association with the backup export destination is closed after the router resumes sending SCTP messages to the primary export destination.

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# backup destination 172.16.10.3 78
Router(config-flow-export-sctp)# backup mode fail-over
Router(config-flow-export-sctp)# backup fail-over 1500
Router(config-flow-export-sctp)# backup restore-time 3000
```

Related Commands

Command	Description
ip flow-export destination sctp	Enables the reliable export of NetFlow accounting information in NetFlow cache entries.
reliability	Specifies the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

cache

To configure operational parameters for NetFlow accounting aggregation caches, use the **cache** command in NetFlow aggregation cache configuration mode. To disable the NetFlow aggregation cache operational parameters for NetFlow accounting, use the **no** form of this command.

cache {**entries** *number* | **timeout** {**active** *minutes* | **inactive** *seconds*}}

no cache {**entries** | **timeout** {**active** | **inactive**}}

Syntax Description

entries *number*	(Optional) The number of cached entries allowed in the aggregation cache. The number of entries can be 1024 to 524288. The default is 4096.
timeout	(Optional) Configures aggregation cache time-outs.
active *minutes*	(Optional) The number of minutes that an active entry will stay in the aggregation cache before it is exported and removed. The range is from 1 to 60 minutes. The default is 30 minutes.
inactive *seconds*	(Optional) The number of seconds that an inactive entry will stay in the aggregation cache before it times out. The range is from 10 to 600 seconds. The default is 15 seconds.

Command Default

The default for cache entries is 4096.
The default for active cache entries is 30 minutes.
The default for inactive cache entries is 15 seconds.

Command Modes

NetFlow aggregation cache configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(7)T	This command function was modified to support cache entries for IPv6.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to set the NetFlow aggregation cache entry limits and timeout values for the NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# cache entries 2046
Router(config-flow-cache)# cache timeout inactive 199
Router(config-flow-cache)# cache timeout active 45
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

cache-timeout

To specify the length of time for which the list of NetFlow top talkers (unaggregated top flows) is retained, use the **cache-timeout** command in NetFlow top talkers configuration mode. To return the timeout parameters for the list of top talkers to the default of 5 seconds, use the **no** form of this command.

cache-timeout *milliseconds*

no cache-timeout

Syntax Description

milliseconds	Length in milliseconds for which the list of top talkers is retained. The range is from 1 to 3,600,000 (1 millisecond to one hour). The default is 5000 (5 seconds).

Defaults

The default time for which the list of top talkers is retained is 5 seconds.

Command Modes

NetFlow top talkers configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring NetFlow top talkers

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands. Optionally, the **match** command can be configured to specify additional matching criteria.

Cache Timeout

The cache timeout starts after the list of top talkers is requested by entering the **show ip flow top-talkers** command or through the netflow MIB.

A long timeout period limits the system resources that are used by NetFlow top talkers. However, the list of top talkers is calculated only once during the timeout period. If a request to display the top talkers is made more than once during the timeout period, the same results are displayed for each request, and the list of top talkers is not recalculated until the timeout period expires.

A short timeout period ensures that the latest list of top talkers is retrieved; however too short a period can have undesired effects:

- 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.
- The list of top talkers is updated every time the top talkers information is requested, possibly causing unnecessary usage of system resources.

A good method to ensure that the latest information is displayed, while also conserving system resources, is to configure a large value for the timeout period, but recalculate the list of top talkers by changing the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers** command to display the top talkers. Changing the parameters of the **cache-timeout**, **top**, or **sort-by** command causes the list of top talkers to be recalculated upon receipt of the next command line interface (CLI) or MIB request.

Examples

In the following example, the list of top talkers is configured to be retained for 2 seconds (2000 milliseconds). There is a maximum of 4 top talkers, and the sort criterion is configured to sort the list of top talkers by the total number of bytes in each top talker.

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# cache-timeout 2000
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command using the configuration from the previous example:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   349K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   349K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   328K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   303K
4 of 4 top talkers shown. 11 flows processed
```

Related Commands

Command	Description
ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip flow top-talkers	Displays the statistics for the top talkers (heaviest traffic patterns and most-used applications in the network).
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.

Command	Description
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

clear fm netflow counters

To clear the NetFlow counters, use the **clear fm netflow counters** command in privileged EXEC mode.

clear fm netflow counters

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on systems that are configured with a Supervisor Engine 2.

Examples

This example shows how to clear the NetFlow counters:

```
Router# clear fm netflow counters
Router#
```

clear ip flow stats

To clear the NetFlow accounting statistics, use the **clear ip flow stats** command in privileged EXEC mode.

clear ip flow stats

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
11.1CA	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2(17d)SXB release.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

The **show ip cache flow** command displays the NetFlow accounting statistics. Use the **clear ip flow stats** command to clear the NetFlow accounting statistics.

Examples

The following example shows how to clear the NetFlow accounting statistics on the router:

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

Related Commands

Command	Description
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.

clear mls nde flow counters

To clear the NDE counters, use the **clear mls nde flow counters** command.

clear mls nde flow counters

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to reset the NDE counters:

```
Router# clear mls nde flow counters
Router#
```

Related Commands

Command	Description
show mls nde	Displays information about the NDE hardware-switched flow.

clear mls netflow

To clear the MLS NetFlow-shortcut entries, use the **clear mls netflow** command.

clear mls netflow ip [**destination** *ip-addr* [**source** *ip-addr-spec*]] [**dynamic** | {**sw-installed** [**non-static** | **static**]}] [**module** *mod*]

clear mls netflow ipv6 [**destination** *ipv6-addr* [**/***ipv6-prefix*] [**source** *ipv6-addr*[**/***ipv6-prefix*]]] [**flow** {**tcp** | **udp**}] [{**destination** | **source**} *port-num*]] [**dynamic** | {**sw-installed** [**non-static** | **static**]}] [**module** *mod*]

clear mls netflow mpls [**top-label** *entry*] [**dynamic** | {**sw-installed** [**non-static** | **static**]}] [**module** *mod*]

clear mls ipx [[**module** *mod*] [**destination** *ipx-network* [*ipx-node*]] [**source** *ipx-network*] [**macs** *mac-addr*] [**macd** *mac-addr*] [**interface** *interface-num*] | [**all**]]

Syntax Description

ip	Clears IP MLS entries.
destination *ip-addr*	(Optional) Specifies a destination full IP address or a subnet address. See the "Usage Guidelines" section for formatting guidelines.
source *ip-addr*	(Optional) Specifies a source full IP address or a subnet address. See the "Usage Guidelines" section for formatting guidelines.
dynamic	(Optional) Clears NetFlow-statistics entries that are created in the hardware.
sw-installed non-static	(Optional) Clears software-installed nonstatic entries.
sw-installed static	(Optional) Clears software-installed static entries.
module *mod*	(Optional) Specifies a module number.
ipv6	Clears IP version 6 software-installed entries.
destination *ipv6-addr*	(Optional) Specifies a destination full IPv6 address or a subnet address. See the "Usage Guidelines" section for formatting guidelines.
/ipv6-prefix	(Optional) IPv6 prefix; valid values are from 0 to 128.
source *iv6p-addr*	(Optional) Specifies a source full IPv6 address or a subnet address. See the "Usage Guidelines" section for formatting guidelines.
flow tcp	(Optional) Clears TCP flow information.
flow udp	(Optional) Clears UDP flow information.
destination *port-num*	(Optional) Specifies a destination port number.
source *port-num*	(Optional) Specifies a source port number.
mpls	Clears MPLS software-installed entries.
top-label *entry*	(Optional) Clears top-label entries; valid values are from 1 to 4294967295.
ipx	Clears IPX MLS entries.
destination *ipx-network*	(Optional) Specifies the destination IPX address. See the "Usage Guidelines" section for formatting guidelines.
ipx-node	(Optional) IPX node address. See the "Usage Guidelines" section for formatting guidelines.

source *ipx-network*	(Optional) Specifies the source IPX address. See the "Usage Guidelines" section for formatting guidelines.
macs *mac-addr*	(Optional) Specifies the source MAC addresses to consider when searching for entries to purge.
macd *mac-addr*	(Optional) Specifies the destination MAC addresses to consider when searching for entries to purge.
interface *interface-num*	(Optional) Clears entries that are associated with the specified VLAN or interface.
all	(Optional) Clears all entries.

Defaults

This command has no default settings.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed as follows: • Replaced the **routes** keyword with **sw-installed**. • Replaced the **statistics** keyword with **dynamic**. • Changed the syntax from **clear mls** [**ip** | **ipv6** | **mpls**] to **clear mls netflow** [**ip** | **ipv6** | **mpls**]
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXF	This command was changed as follows: • Removed support for the **any** keyword. • Added the */ipv6-prefix* argument.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **destination** *ipx-network*, *ipx-node*, and **source** *ipx-network* keywords and arguments are supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2 only.

When entering the IPX address syntax, use the following format:

- IPX network address—1..FFFFFFFE
- IPX node address—x.x.x where x is 0..FFFF
- IPX address—ipx_net.ipx_node (for example, 3.0034.1245.AB45, A43.0000.0000.0001)

Entering any combination of input parameters narrows the search of entries to be cleared. The **destination** or **source** *port-num* keyword and argument should be specified as one of the following: telnet, FTP, WWW, SMTP, X, or DNS.

Up to 16 routers can be included explicitly as MLS-RPs.

Use the following syntax to specify an IP subnet address:

- *ip-subnet-addr* or *ipv6-subnet-addr*—Short subnet address format. The trailing decimal number 00 in an IP or IPv6 address YY.YY.YY.00 specifies the boundary for an IP or IPv6 subnet address. For example, 172.22.36.00 indicates a 24-bit subnet address (subnet mask 172.22.36.00/255.255.255.0), and 173.24.00.00 indicates a 16-bit subnet address (subnet mask 173.24.00.00/255.255.0.0). However, this format can identify only a subnet address of 8, 16, or 24 bits.
- *ip-addr/subnet-mask* or *ipv6-addr/subnet-mask*—Long subnet address format. For example, 172.22.252.00/255.255.252.00 indicates a 22-bit subnet address. This format can specify a subnet address of any bit number. To provide more flexibility, the *ip-addr* or *ipv6-addr* is a full host address, such as 172.22.253.1/255.255.252.00.
- *ip-addr/maskbits* or *ipv6-addr/maskbits*—Simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip-addr* or *ipv6-addr* is a full host address, such as 193.22.253.1/22, which has the same subnet address as the *ip-subnet-addr* or *ipv6-subnet-addr*.

If you do not use the **all** keyword, you must specify at least one of the other four keywords (**source**, **destination**, **flow**, or **interface**) and its arguments.

A 0 value for the **destination** or **source** *port-num* keyword and argument clears all entries. Unspecified options are treated as wildcards, and all entries are cleared.

Examples

This example shows how to clear all the entries that are associated with a specific module (2) and that have a specific destination IP address (173.11.50.89):

```
Router# clear mls netflow ip destination 173.11.50.89 module 2
Router#
```

This example shows how to clear the IPv6 software-installed entries:

```
Router# clear mls netflow ipv6
Router#
```

This example shows how to clear the statistical information:

```
Router# clear mls netflow dynamic
Router#
```

Related Commands

Command	Description
show mls netflow ip	Displays information about the hardware NetFlow IP.
show mls netflow ipv6	Displays information about the hardware NetFlow IPv6 configuration.

enabled (aggregation cache)

To enable a NetFlow accounting aggregation cache, use the **enabled** command in NetFlow aggregation cache configuration mode. To disable a NetFlow accounting aggregation cache, use the **no** form of this command.

enabled

no enabled

Syntax Description

This command has no arguments or keywords.

Defaults

No aggregation cache is enabled.

Command Modes

NetFlow aggregation cache configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable a NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# enabled
```

The following example shows how to disable a NetFlow protocol-port aggregation cache:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# no enabled
```

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.

Command	Description
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

export destination

To enable the exporting of NetFlow accounting information from NetFlow aggregation caches, use the **export destination** command in NetFlow aggregation cache configuration mode. To disable the export of NetFlow accounting information from NetFlow aggregation caches, use the **no** form of this command.

export destination {*hostname* | *ip-address*} *port* [**vrf** *vrf-name*] [**udp**]

no export destination {*hostname* | *ip-address*} *port* [**vrf** *vrf-name*] [**udp**]

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information
port	Specifies the number of the user datagram protocol (UDP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF
udp	(Optional) Specifies UDP as the transport protocol. UDP is the default transport protocol.

Command Default

Export of NetFlow information from NetFlow aggregation caches is disabled.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2T	This command was modified to enable multiple NetFlow export destinations to be used.
12.3(1)	Support for the NetFlow v9 Export Format feature was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S, and support for the Multiple Export Destinations feature was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If the version of Cisco IOS that you have installed on your networking device supports the NetFlow Multiple Export Destinations feature, you can configure your networking device to export NetFlow data to a maximum of 2 export destinations (collectors) per cache (main and aggregation caches), using any combination of UDP and SCTP as the transport protocol for the destinations. A destination is identified by a unique combination of hostname or IP address and port number or port type.

Note UDP is the default transport protocol used by the **export destination** command. In some Cisco IOS releases you can configure SCTP as the transport protocol if you need reliability and additional redundancy. Refer to the **export destination sctp** command for more information.

Table 8 shows examples of the 2 permitted NetFlow export destinations for each cache.

Table 8 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>".

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Releases 12.4(4)T and 12.2(18)SXH, only one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the export destinations you specified.

Cisco IOS 12.4(4)T, 12.2(18)SXH, and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf** *vrf-name* keyword and argument with the **ip flow-export destination** *ip-address port* command. To configure the global routing table option, enter this command without the optional **vrf** *vrf-name* keyword and argument.

Examples

The following example shows how to configure two export destinations for a NetFlow accounting protocol-port aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export destination 10.41.41.1 9992
Router(config-flow-cache)# export destination 172.16.89.1 9992
Router(config-flow-cache)# enabled
```

The following example shows how to configure the networking device for exporting from the NetFlow **source-prefix-tos** aggregation cache to an export destination that is reachable in VRF group1:

```
Router(config)# ip flow-aggregation cache source-prefix-tos
Router(config-flow-cache)# export destination 172.16.10.2 78 vrf group1
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
export template	Configures template options for the export of NetFlow accounting information in NetFlow aggregation cache entries
export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow aggregation cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

export destination sctp (NetFlow aggregation cache)

To enable the reliable export of NetFlow accounting information from NetFlow aggregation caches, use the **export destination sctp** command in NetFlow aggregation cache configuration mode. To disable the reliable export of NetFlow accounting information from NetFlow aggregation caches, use the **no** form of this command.

export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

no export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
port	Specifies the number of the stream control transmission protocol (SCTP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF

Command Default

Reliable export of NetFlow information from NetFlow aggregation caches is disabled.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.4(4)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

NetFlow Reliable Export Using SCTP

SCTP can be used as an alternative to UDP when you need a more robust and flexible transport protocol than UDP. 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 (connection) between two end-points (peers), which can contain one or more logical channels called streams. The default mode of transmission for a stream is to guarantee reliable ordered delivery of messages using a selective-acknowledgment scheme. SCTP buffers messages until their receipt has been acknowledged by the receiving end-point. SCTP has a congestion control mechanism which limits how much memory is consumed by the SCTP stack, in packet buffering.

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Release 12.4(4)T, one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the destinations you specified.

Cisco IOS 12.4(4)T and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf** *vrf-name* keyword and argument with the **export destination** *ip-address port* command. To configure the global routing table option, enter this command without the optional **vrf** *vrf-name* keyword and argument.

Examples

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data from a NetFlow AS aggregation cache to a host:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# export destination 172.16.10.2 78 sctp
Router(config-flow-cache)# enabled
```

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data from a NetFlow AS aggregation cache to a host that is reachable in VRF group1:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# export destination 172.16.10.2 78 vrf group1 sctp
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
backup	Configures a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries
export destination	Enables the export of NetFlow accounting information in NetFlow aggregation cache entries to a remote device such as a server running an application that analyzes NetFlow data.
export template	Configures template options for the export of NetFlow accounting information in NetFlow aggregation cache entries
export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow aggregation cache entries
reliability	Specifies the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

export template

To configure template options for the export of NetFlow accounting information from NetFlow aggregation caches, use the **export template** command in NetFlow aggregation cache configuration mode. To return to the default behavior, use the **no** form of this command.

Configure template only

export template {**refresh-rate** *packets* | **timeout-rate** *minutes*}

no export template {**refresh-rate** | **timeout-rate**}

Configure template options

ip export template options {**export-stats** | **refresh-rate** *packets* | **timeout-rate** *minutes* | **sampler**}

no export template options {**export-stats** | **refresh-rate** | **timeout-rate** | **sampler**}

Syntax Description

template	Enables the **refresh-rate** and **timeout-rate** keywords for the configuring of Version 9 export templates.
refresh-rate *packets*	(Optional) Specifies the number of export packets that are sent before the options and flow templates are resent. Range:1 to 600 packets. The default is 20 packets. **Note** This applies to the **export template refresh-rate** *packets* command.
timeout-rate *minutes*	(Optional) Specifies the interval (in minutes) that the router waits after sending the templates (flow and options) before sending them again. Range: 1 to 3600 minutes. The default is 30 minutes. **Note** This applies to the **export template timeout-rate** *minutes* command.
options	(Optional) Enables the **export-stats**, **refresh-rate**, **sampler** and **timeout-rate** keywords for configuring Version 9 export options.
export-stats	(Optional) Enables the export of statistics including the total number of flows exported and the total number of packets exported.
sampler	(Optional) When Version 9 export is configured, this keyword enables the export of an option containing a random-sampler configuration, including the sampler ID, sampling mode, and sampling interval for each configured random sampler. **Note** You must have a flow sampler map configured before you can configure the sampler keyword for the **export template options** command.

refresh-rate *packets*	(Optional) Specifies the number of packets that are sent before the configured options records are resent. Range: 1 to 600 packets. The default is 20 packets. **Note** This applies to the **export template options refresh-rate** *packets* command.
timeout-rate *minutes*	(Optional) Specifies the interval (in minutes) that the router will wait after sending the options records before they are sent again. Range: 1 to 3600 minutes. The default is 30 minutes. **Note** This applies to the **export template options timeout-rate** *minutes* command.

Command Default

The default parameters as noted in the Syntax Description table are used.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **export template options export-stats** command requires that the NetFlow Version 9 export format be already configured on the router.

The **export template options sampler** command requires that the NetFlow Version 9 export format and a flow sampler map be already configured on the router.

Examples

The following example shows how to configure a NetFlow accounting protocol-port aggregation cache so that the networking device sends the export statistics (total flows and packets exported) as options data:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export template options export-stats
Router(config-flow-cache)# enabled
```

The following example shows how to configure a NetFlow accounting protocol-port aggregation cache to wait until 100 export packets have been sent, or 60 minutes have passed since the last time the templates were sent (whichever comes first) before the templates are resent to the destination host:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export template refresh-rate 100
Router(config-flow-cache)# export template timeout-rate 60
Router(config-flow-cache)# enabled
```

The following example shows how to configure a NetFlow accounting protocol-port aggregation cache to enable the export of information about NetFlow random samplers:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export template option sampler
Router(config-flow-cache)# enabled
```

Tip You must have a **flow-sampler** map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

Related Commands

Command	Description
export destination	Enables the export of NetFlow accounting information in NetFlow aggregation cache entries to a remote device such as a server running an application that analyzes NetFlow data.
export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow aggregation cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

export version

To specify the version of the export format of NetFlow accounting information from NetFlow aggregation caches, use the **export version** command in NetFlow aggregation cache configuration mode. To return to the default behavior, use the **no** form of this command.

export version {**8** | **9**}

no export version

Syntax Description

version {**8**	**9**}	Version of the format for NetFlow data export.

Command Default

Version 9 is the default format for the exporting of NetFlow accounting information from NetFlow aggregation caches.

Command Modes

NetFlow aggregation cache configuration (config-flow-cache)

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.4(4)T	The **sctp** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

NetFlow aggregation caches export data in UDP datagrams using either the Version 9 or Version 8 export format.

Table 9 describes how to determine the most appropriate export format for your requirements.

Table 9 Selecting a NetFlow Export Format

Export Format	Select When…
Version 9	You need 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, IPv6 NetFlow, Egress NetFlow, NetFlow Layer 2 and security exports, 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 because the format is extensible you can use the same export format with future features.
Version 8	Version 8 export format is available only for export from aggregation caches. Use Version 8 when your NetFlow Collection Engine (NFC) does not support Version 9.

The **export version** command supports two export data formats: Version 8, and Version 9. Version 8 should be used only when it is the only NetFlow data export format version that is supported by the application that you are using to analyze the exported NetFlow data. Version 9 is the only flexible export format version.

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 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.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow do not need to 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.

NetFlow Version 9 has the following characteristics:

- 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 (UDP, TCP, SCTP, and so on).

Note In order for the BGP information to be populated in the main cache, you must have either a NetFlow export destination configured or a NetFlow aggregation configured.

Note The AS values for the **peer-as** and the **origin-as** keywords are captured only if you have configured an export destination with the **ip flow-export destination** command.

Note The AS values for the **peer-as** and the **origin-as** keywords are captured only if you have configured an export destination with the **ip flow-export destination** command.

For more information on the available export data formats, see the *Cisco IOS NetFlow Configuration Guide,* Release 12.4T. For more information on the Version 9 data format, see the *Cisco IOS NetFlow Version 9 Export Format Feature Guide*.

Examples

The following example shows how to configure version 9 as the export format for a NetFlow accounting protocol-port aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache protocol-port
Router(config-flow-cache)# export version 9
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
export destination	Enables the export of NetFlow accounting information in NetFlow aggregation cache entries to a remote device such as a server running an application that analyzes NetFlow data.
export template	Configures template options for the export of NetFlow accounting information in NetFlow aggregation cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

flow hardware mpls-vpn ip

To ensure the creation and export of hardware NetFlow cache entries for traffic entering the router on the last MPLS hop of an IPv4 MPLS VPN network, use the flow **hardware mpls-vpn ip** command in global configuration mode. To disable the creation and export of hardware NetFlow cache entries for this traffic, use the **no** form of this command.

flow hardware mpls-vpn ip *vrf-id*

no flow hardware mpls-vpn ip *vrf-id*

Syntax Description

vrf-id	The name of a VRF that you have previously configured.

Command Default

Creation and export of hardware NetFlow cache entries for traffic entering the router on the last MPLS hop of an IPv4 MPLS VPN network is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(33)SRB	This command was introduced.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

NetFlow Aggregation

If you want to include IPV4 MPLS VPN traffic in a NetFlow aggregation scheme on your router, you must configure the **flow hardware mpls-vpn ip** command.

NetFlow Sampling

If you want to include IPV4 MPLS VPN traffic in the traffic that is analyzed using NetFlow sampling on your router, you must configure the **flow hardware mpls-vpn ip** command.

Examples

The following example configures NDE for VRF vpn1:

```
Router(config)# flow hardware mpls-vpn ip vpn1
```

Related Commands

Command	Description
show mls netflow ip	Displays information about the hardware NetFlow IP flows.

flow-sampler

To apply a flow sampler map for random sampled NetFlow accounting to an interface, use the **flow-sampler** command in interface configuration mode. To remove a flow sampler map for random sampled NetFlow accounting from an interface, use the **no** form of this command.

flow-sampler *sampler-map-name* [**egress**]

no flow-sampler *sampler-map-name* [**egress**]

Syntax Description

sampler-map-name	Name of the flow sampler map to apply to the interface.
egress	(Optional) Specifies that the sampler map is to be applied to egress traffic.

Command Default

Flow sampler maps for NetFlow accounting are not applied to interfaces by default.

Command Modes

Interface configuration
Subinterface configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.3(11)T	NetFlow egress support was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must create and enable the random sampler NetFlow map for random sampled NetFlow accounting using the **flow-sampler-map** and **mode** commands before you can use the **flow-sampler** command to apply the random sampler NetFlow map to an interface.

Random sampled NetFlow accounting cannot be run concurrently with (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the same interface, or subinterface. You must disable ingress NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the interface, or subinterface, if you want to enable random sampled NetFlow accounting on the interface, or subinterface.

You must enable either Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this command.

Tip If you disable CEF or DCEF globally using the **no ip cef [distributed]** command the **flow-sampler** *sampler-map-name* command is removed from any interfaces that you previously configured for random sampled NetFlow accounting. You must reenter the **flow-sampler** *sampler-map-name* command after

you reenable CEF or dCEF to reactivate random sampled NetFlow accounting.

Tip If your router is running Cisco IOS release 12.2(14)S or a later release, or Cisco IOS Release 12.2(15)T or a later release, NetFlow accounting might be enabled through the use of the **ip flow ingress** command instead of the **ip route-cache flow** command. If your router has NetFlow accounting enabled through the use of **ip flow ingress** command you must disable NetFlow accounting, using the **no** form of this command, before you apply a random sampler map for random sampled NetFlow accounting on an interface otherwise the full, un-sampled traffic will continue to be seen.

Examples

The following example shows how to create and enable a random sampler map for random sampled (ingress) NetFlow accounting with CEF switching on Ethernet interface 0/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 0/0
Router(config-if)# no ip route-cache flow
Router(config-if)# ip route-cache cef
Router(config-if)# flow-sampler my-map
```

The following example shows how to create and enable a random sampler map for random sampled egress NetFlow accounting with CEF switching on Ethernet interface 1/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 1/0
Router(config-if)# no ip flow egress
Router(config-if)# ip route-cache cef
Router(config-if)# flow-sampler my-map egress
```

The following output from the **show flow-sampler** command verifies that random sampled NetFlow accounting is active:

```
Router# show flow-sampler

 Sampler : my-map, id : 1, packets matched : 7, mode : random sampling mode
  sampling interval is : 100
```

Related Commands

Command	Description
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
mode (flow sampler configuration)	Specifies a packet interval for NetFlow accounting random sampling mode and enables the flow sampler map.
netflow-sampler	Enables NetFlow accounting with input filter sampling.
show flow-sampler	Displays the status of random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler).
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

flow-sampler-map

To define a flow sampler map for random sampled NetFlow accounting, use the **flow-sampler-map** command in global configuration mode. To remove a flow sampler map for random sampled NetFlow accounting, use the **no** form of this command.

flow-sampler-map *sampler-map-name*

no flow-sampler-map *sampler-map-name*

Syntax Description

sampler-map-name	Name of the flow sampler map to be defined for random sampled NetFlow accounting.

Command Default

No flow sampler maps for random sampled NetFlow accounting are defined.

Command Modes

Global configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Random sampled NetFlow accounting does not start sampling traffic until (1) the random sampler map is activated through the use of the **mode** command and (2) the sampler map has been applied to an interface through the use of the **flow-sampler** command.

Random Sampled NetFlow accounting cannot be run concurrently with (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the same interface, or subinterface. You must disable (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the interface or subinterface, if you want to enable random sampled NetFlow accounting on that interface or subinterface.

You must enable either Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this command.

Tip If you disable dCEF globally using the **no ip cef [distributed]** command, the **flow-sampler** *sampler-map-name* command is removed from any interfaces that you previously configured for random sampled NetFlow accounting. You must reenter the **flow-sampler** *sampler-map-name* command after you reenable CEF or dCEF to reactivate random sampled NetFlow accounting.

Tip If your router is running Cisco IOS release 12.2(14)S or a later release, or Cisco IOS Release 12.2(15)T or a later release, NetFlow accounting might be enabled through the use of the **ip flow ingress** command instead of the **ip route-cache flow** command. If your router has NetFlow accounting enabled through the use of **ip flow ingress** command you must disable NetFlow accounting, using the **no** form of this command, before you apply a random sampler map for random sampled NetFlow accounting on an interface otherwise the full, un-sampled traffic will continue to be seen.

Examples

The following example shows how to create and enable a random sampler map for random sampled (ingress) NetFlow accounting with CEF switching on Ethernet interface 0/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 0/0
Router(config-if)# no ip route-cache flow
Router(config-if)# ip route-cache cef
Router(config-if)# flow-sampler my-map
```

The following example shows how to create and enable a random sampler map for random sampled egress NetFlow accounting with CEF switching on Ethernet interface 1/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 1/0
Router(config-if)# no ip flow egress
Router(config-if)# ip route-cache cef
Router(config-if)# flow-sampler my-map egress
```

The following output from the **show flow-sampler** command verifies that random sampled NetFlow accounting is active:

```
Router# show flow-sampler

 Sampler : my-map, id : 1, packets matched : 7, mode : random sampling mode
  sampling interval is : 100
```

Related Commands

Command	Description
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
mode (flow sampler configuration)	Specifies a packet interval for NetFlow accounting random sampling mode and enables the flow sampler map.
netflow-sampler	Enables NetFlow accounting with input filter sampling.
show flow-sampler	Displays the status of random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler).
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow

To enable NetFlow accounting for inbound (received) or outbound (transmitted) network traffic, use the **ip flow** command in interface or subinterface configuration mode. To disable NetFlow accounting, use the **no** form of this command.

ip flow {**ingress** | **egress**}

no ip flow {**ingress** | **egress**}

Syntax Description

ingress	Enables NetFlow accounting for traffic that is received on an interface. **Note** This is also known as ingress NetFlow accounting.
egress	Enables NetFlow accounting for traffic that is transmitted on an interface. **Note** This is also known as egress NetFlow accounting.

Command Default

NetFlow accounting is disabled.

Command Modes

Interface configuration (config-if)
Subinterface configuration (config-sub-if)

Command History

Release	Modification
12.2(14)S	This command was introduced.
12.2(25)S	Output of the **show running configuration** command was modified so that the **ip route-cache flow** command as well as the **ip flow ingress** command will appear when either command is configured.
12.2(15)T	This command was integrated into Cisco IOS Release 12.2(15)T.
12.3(11)T	The egress keyword was added.
12.2(28)SBB	This command was integrated into Cisco IOS Release 12.2(27)SBB and implemented for the Cisco 10000 series routers.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF. This command was changed to allow you to dynamically create NetFlow entries on a 7600.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Cisco 7600 Series Platforms

The **ip flow ingress** command is supported on the Supervisor Engine 720 in PFC3B and PFC3BXL mode.

The **ip flow ingress** command is supported on the Supervisor Engine 2 with a PFC2.

In Release 12.2(18)SXF and later releases, to create a NetFlow entry, you need to enter the **ip flow ingress** command. In releases prior to Release 12.2(18)SXF, the NetFlow entries are created automatically.

Other Platforms

Use this command on an interface or subinterface to enable NetFlow accounting for traffic.

You must enable CEF or dCEF globally on the networking device, and on the interface or subinterface that you want to enable NetFlow accounting on before you enable either ingress or egress NetFlow accounting.

Examples

The following example shows how to configure ingress NetFlow accounting for traffic that is received on FastEthernet interface 0/0:

```
Router(config)# interface fastethernet0/0
Router(config-if)# ip flow ingress
```

The following example shows how to configure egress NetFlow accounting for traffic that is transmitted on FastEthernet interface 0/0:

```
Router(config)# interface fastethernet0/0
Router(config-if)# ip flow egress
```

Related Commands

Command	Description
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow layer2-switched

To enable the creation of switched, bridged, and Layer 2 IP flows for a specific VLAN, use the **ip flow layer2-switched** command in global configuration mode. Use the **no** form of this command to return to the default settings.

ip flow {**ingress** | **export**} **layer2-switched** {**vlan** {*num* | *vlanlist*}}

no ip flow {**ingress** | **export**} **layer2-switched** {**vlan** {*num* | *vlanlist*}}

Syntax Description

ingress	Enables the collection of switched, bridged, and IP flows in Layer 2.
export	Enables the export of switched, bridged, and IP flows in Layer 2.
vlan *num* | *vlanlist*	Specifies the VLAN or range of VLANs; valid values are from 1 to 4094. See the "Usage Guidelines" section for additional information.

Command Default

The defaults are as follows:

- **ip flow ingress layer2switch** is disabled.
- **ip flow export layer2switched** is enabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(18)SXE	Support for this command was introduced on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

The **ip flow layer2-switched** command is supported on the Supervisor Engine 720 in PFC3B and PFC3BXL mode only.

The **ip flow layer2-switched** command is supported on the Supervisor Engine 2 with a PFC2.

Before using this command on Cisco 7600 series routers that are configured with a Supervisor Engine 720, you must ensure that a corresponding VLAN interface is available and has a valid IP address. This guideline does not apply to Cisco 7600 series routers that are configured with a Supervisor Engine 2.

You can enter one or multiple VLANs. The following examples are samples of valid VLAN lists: 1; 1,2,3; 1-3,7.

Examples

This example shows how to enable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# ip flow ingress layer2-switched vlan 2
Router(config)#
```

This example shows how to enable export of Layer 2-switched flows on a range of VLANs:

```
Router(config)# ip flow export layer2-switched vlan 1-3,7
Router(config)#
```

This example shows how to disable the collection of Layer 2-switched flows on a specific VLAN:

```
Router(config)# no ip flow ingress layer2-switched vlan 2
Router(config#
```

ip flow-aggregation cache

To enable NetFlow accounting aggregation cache schemes, use the **ip flow-aggregation cache** command in global configuration mode. To disable NetFlow accounting aggregation cache schemes, use the **no** form of this command.

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** | **exp-bgp-prefix**}

no 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** | **exp-bgp-prefix**}

Syntax Description

as	Configures the autonomous system aggregation cache scheme.
as-tos	Configures the autonomous system type of service (ToS) aggregation cache scheme.
bgp-nexthop-tos	Configures the Border Gateway Protocol (BGP) next hop ToS aggregation cache scheme.
destination-prefix	Configures the destination-prefix aggregation cache scheme.
destination-prefix-tos	Configures the destination prefix ToS aggregation cache scheme.
prefix	Configures the prefix aggregation cache scheme.
prefix-port	Configures the prefix port aggregation cache scheme.
prefix-tos	Configures the prefix ToS aggregation cache scheme.
protocol-port	Configures the protocol-port aggregation cache scheme.
protocol-port-tos	Configures the protocol-port ToS aggregation cache scheme.
source-prefix	Configures the source-prefix aggregation cache scheme.
source-prefix-tos	Configures the source-prefix ToS aggregation cache scheme.
exp-bgp-prefix	Configures the exp-bgp-prefix aggregation cache scheme.

Command Default

This command is not enabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(15)S	This command was modified to include the ToS aggregation scheme keywords.
12.2(2)T	This command was modified to enable multiple NetFlow export destinations.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the BGP Next Hop Support feature was added.

Release	Modification
12.2(18)S	Support for the BGP Next Hop Support feature was added.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix** aggregation cache keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command. The **export destination** command supports a maximum of two concurrent export destinations.

The ToS aggregation cache scheme keywords enable NetFlow accounting aggregation cache schemes that include the ToS byte in their export records. The ToS byte is an 8-bit field in the IP header. The ToS byte specifies the quality of service for a datagram during its transmission through the Internet.

You can enable only one aggregation cache configuration scheme per command line. The following rules apply to configuring source and destination masks.

- The source mask can only be configured in the prefix, prefix-port, prefix-tos, source-prefix and source-prefix-tos aggregation modes.
- The destination mask can only be configured in the prefix, prefix-port, prefix-tos, destination-prefix and destination-prefix-tos aggregation modes.
- No masks can be configured in non-prefix aggregation modes

To enable aggregation (whether or not an aggregation cache is fully configured), you must enter the **enabled** command in aggregation cache configuration mode. (You can use the **no** form of this command to disable aggregation. The cache configuration remains unchanged even if aggregation is disabled.)

Examples

The following example shows how to configure a NetFlow accounting autonomous system aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache as
Router(config-flow-cache)# enabled
```

The following example shows how to configure a minimum prefix mask of 16 bits for the NetFlow accounting destination-prefix aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# mask destination minimum 16
Router(config-flow-cache)# enabled
```

The following example shows how to configure a minimum prefix mask of 16 bits for the NetFlow accounting source-prefix aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache source-prefix
Router(config-flow-cache)# mask source minimum 16
Router(config-flow-cache)# enabled
```

The following example shows how to configure multiple export destinations for the NetFlow accounting autonomous system ToS aggregation cache scheme:

```
Router(config)# ip flow-aggregation cache as-tos
Router(config-flow-cache)# export destination 172.17.24.65 9991
Router(config-flow-cache)# export destination 172.16.10.2 9991
Router(config-flow-cache)# enabled
```

Related Commands

Command	Description
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
enabled (aggregation cache)	Enables the NetFlow aggregation cache.
mask	Specifies the source or destination prefix mask.
show ip cache flow aggregation	Displays a summary of the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-cache entries

To change the number of entries maintained in the NetFlow accounting cache, use the **ip flow-cache entries** command in global configuration mode. To return to the default number of entries, use the **no** form of this command.

ip flow-cache entries *number*

no ip flow-cache entries

Syntax Description

number	Number of entries to maintain in the NetFlow cache. The valid range is from 1024 to 524288 entries. The default is 65536 (64K).

Defaults

65536 entries (64K)

Command Modes

Global configuration

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Normally the default size of the NetFlow cache will meet your needs. However, you can increase or decrease the number of entries maintained in the cache to meet the needs of your flow traffic rates. For environments with a high amount of flow traffic (such as an internet core router), a larger value such as 131072 (128K) is recommended. To obtain information on your flow traffic, use the **show ip cache flow** EXEC command.

The default is 64K flow cache entries. Each cache entry is approximately 64 bytes of storage. Assuming a cache with the default number of entries, approximately 4 MB of DRAM would be required. Each time a new flow is taken from the free flow queue, the number of free flows is checked. If only a few free flows remain, NetFlow attempts to age 30 flows using an accelerated timeout. If only one free flow remains, NetFlow automatically ages 30 flows regardless of their age. The intent is to ensure that free flow entries are always available.

Caution We recommend that you not change the number of NetFlow cache entries. To return to the default number of NetFlow cache entries, use the **no ip flow-cache entries** global configuration command.

Examples

The following example shows how to increase the number of NetFlow cache entries to 131,072 (128K):

```
Router(config)# ip flow-cache entries 131072
%The change in number of entries will take effect after either the next reboot or when
netflow is turned off on all interfaces
```

Tip You turn off NetFlow accounting on interfaces by removing the command that you enabled NetFlow accounting with. For example, if you enabled NetFlow accounting on an interface with the **ip flow ingress** command you turn off NetFlow accounting for the interface using the **no** form of the command –**no ip flow ingress**. Remember to turn NetFlow accounting back on for the interface after you have turned it off.

Related Commands

Command	Description
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-cache mpls label-positions

To enable Multiprotocol Label Switching (MPLS)-Aware NetFlow, use the **ip flow-cache mpls label-positions** command in global configuration mode. To disable MPLS-aware NetFlow, use the **no** form of this command.

ip flow-cache mpls label-positions [*label-position-1* [*label-position-2* [*label-position-3*]]] [**exp-bgp-prefix-fields**] [**no-ip-fields**] [**mpls-length**]

no ip flow-cache mpls label-positions

Syntax Description

label-position-l	(Optional) Position of an MPLS label in the incoming label stack. Label positions are counted from the top of the stack, starting with 1.
exp-bgp-prefix-fields	(Optional) Generates a MPLS Provider Edge (PE) PE-to-PE traffic matrix. The following IP-related flow fields are included: • Input interface • BGP Nexthop • MPLS Experimental (EXP) bits The MPLS label values will be set to zero on the Cisco 10000 in the display output of the **show ip cache verbose flow aggregation exp-bgp-prefix** command.
no-ip-fields	(Optional) Controls the capture and reporting of MPLS flow fields. If the **no-ip-fields** keyword is not specified, the following IP-related flow fields are 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 If the **no-ip-fields** keyword is specified, the IP-related fields are reported with a value of 0.
mpls-length	(Optional) 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.

Defaults

MPLS-Aware NetFlow is not enabled.

Command Modes

Global configuration

Command History

Release	Modification
12.0(24)S	This command was introduced.
12.0(25)S	The **no-ip-fields** and **mpls-length** keywords were.
12.3(8)T	This command was integrated into Cisco IOS Release 12.3(8)T.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix-fields** keyword was added.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to configure the MPLS-aware NetFlow feature on a label switch router (LSR) and to specify labels of interest in the incoming label stack. Label positions are counted from the top of the stack, starting with 1. The position of the top label is 1, the position of the second label is 2, and so forth.

With MPLS-aware NetFlow enabled on the router, NetFlow collects data for incoming IP packets and for incoming MPLS packets on all interfaces where NetFlow is enabled in full or in sampled mode.

Caution When you enter the **ip flow-cache mpls label-positions** command on a Cisco 12000 series Internet router, NetFlow will stop collecting data for incoming IP packets on any Engine 4P line cards installed in the router on which NetFlow is enabled in full or in sampled mode. Engine 4P line cards in a Cisco 12000 series Internet router do not support NetFlow data collection of incoming IP packets and MPLS packets concurrently.

Tip MPLS-aware NetFlow is enabled in global configuration mode. NetFlow is enabled per interface.

Examples

The following example shows how to configure MPLS-aware NetFlow to capture the first (top), third, and fifth label:

```
Router(config)# ip flow-cache mpls label-positions 1 3 5
```

The following example shows how to configure MPLS-aware NetFlow to capture only MPLS flow information (no IP-related flow fields) and the length that represents the sum of the MPLS packet payload length and the MPLS label stack length:

```
Router(config)# ip flow-cache mpls label-positions no-ip-fields mpls-length
```

The following example shows how to configure MPLS PE-to-PE Traffic Statistics for Netflow:

```
Router(config)# ip flow-cache mpls label-positions 1 2 exp-bgp-prefix-fields
```

Related Commands

Command	Description
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.

Command	Description
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-cache timeout

To specify NetFlow accounting flow cache parameters, use the **ip flow-cache timeout** command in global configuration mode. To disable the flow cache parameters, use the **no** form of this command.

ip flow-cache timeout [**active** *minutes* | **inactive** *seconds*]

no ip flow-cache timeout [**active** | **inactive**]

Syntax Description

active	Specifies the active flow timeout.
minutes	(Optional) The number of minutes that an active flow remains in the cache before it times out. The range is from 1 to 60. The default value is 30.
inactive	Specifies the inactive flow timeout.
seconds	(Optional) 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 value is 15.

Defaults

The flow-cache timeout values are set to the default values.

Command Modes

Global configuration.

Command History

Release	Modification
12.3(7)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Use this command to specify active and inactive timeout parameters.

A flow is considered to be active if packets belonging to the flow are detected wherever the NetFlow statistics are being collected. A flow is considered to be inactive if no further packets are detected for the flow at the collection point for NetFlow statistics.

Examples

In the following example, an active flow is allowed to remain in the cache for 20 minutes:

```
Router(config)# ip flow-cache timeout active 20
```

In the following example, an inactive flow is allowed to remain in the cache for 10 seconds before it times out and is removed:

```
Router(config)# ip flow-cache timeout inactive 10
```

Related Commands

Command	Description
ip flow egress	Enables NetFlow (egress) accounting for traffic that the router is forwarding.
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-capture

To enable the capture of values from Layer 2 or additional Layer 3 fields in NetFlow traffic, use the **ip flow-capture** command in global configuration mode. To disable capturing Layer 2 or Layer 3 fields from NetFlow traffic, use the **no** form of this command.

ip flow-capture {**fragment-offset | icmp | ip-id | mac-addresses | packet-length | ttl | vlan-id**}

no ip flow-capture{**fragment-offset | icmp | ip-id | mac-addresses | packet-length | ttl | vlan-id**}

Syntax Description

fragment-offset	Captures the value of the 13 bit IP fragment offset field from the first fragmented IP datagram in a flow.
icmp	Captures the value of the ICMP type and code fields from the first ICMP datagram in a flow.
ip-id	Captures the value of the IP-ID field from the first IP datagram in a flow.
mac-addresses	Captures the values of the source MAC addresses from ingress packets and the destination MAC addresses from egress packets from from the first packet in a flow. **Note** This command only applies to traffic that is received or transmitted over Ethernet interfaces
packet-length	Captures the value of the packet length field from IP datagrams in a flow.
ttl	Captures the value of the Time-to-Live (TTL) field from IP datagrams in a flow.
vlan-id	Captures the value of the 802.1q or ISL VLAN-ID field from VLAN-encapsulated frames in a flow when the frames are received or transmitted on trunk ports.

Command Default

The **ip flow-capture** command is not enabled by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(14)T	This command was introduced.
12.4(2)T	The **fragment-offset** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must enable NetFlow accounting on an interface or a subinterface using the **ip flow** {**ingress | egress**} command for the **ip flow-capture** command to take effect. You can enable NetFlow accounting before or after you have entered the **ip flow-capture** command in global configuration mode.

If you want to export the information captured by the **ip flow-capture** command, you must configure NetFlow export using the **ip flow-export destination** command, and you must configure NetFlow to use the Version 9 export format. Use the **ip flow-export version 9** command to configure the NetFlow Version 9 export format.

The fields captured by the **ip flow-capture** command are currently not available in the NetFlow MIB.

ip flow-capture fragment-offset

IP fragmentation occurs when the size of an IP datagram exceeds the maximum transmission unit (MTU) of the Layer 2 frame type used by the next-hop network. For example, the IP MTU size of an ATM network is 4470 bytes. When a host needs to transmit an IP datagram that exceeds 4470 bytes on an ATM network, it must first fragment the datagram into two or more smaller IP datagrams.

An IP datagram sent by a host system such as a web server can also be fragmented by a router in the network if the router needs to transmit the IP datagram on a next-hop network that has an MTU that is smaller than the current size of the IP datagram. For example if a router receives a 4470-byte IP datagram on an ATM interface and the next hop network is a 100-Mbps Fast Ethernet network with an MTU of 1514, the router must fragment the IP datagram into three smaller IP datagrams (4470/1514). It is possible for an IP datagram to be fragmented two or more times on its path from the sending host to the destination host.

A fragmented IP datagram is reassembled by the destination host. The last fragment of an IP datagram is identified when the “more fragments” flag is set to 0. The length of a complete IP datagram is calculated by the receiving host by means of the fragment offset field and the length of the last fragment.

The **ip flow-capture fragment-offset** command captures the value of the IP fragment offset field from the first fragmented IP packet in the flow. If you are seeing several flows with the same value for the IP fragment offset field, it is possible that your network is being attacked by a host that is sending the same IP packets over and over.

ip flow-capture icmp

ICMP is used for several purposes. "One of the most common is the ping command. ICMP echo requests are sent by a host to a destination to verify that the destination is reachable by IP. If the destination is reachable, it should respond by sending an ICMP echo reply. Refer to RFC 792 (http://www.ietf.org/rfc/rfc0792.txt) for more information on ICMP.

ICMP packets have been used in many types of attacks on networks. Two of the most common attacks are denial-of-service (DoS) attacks and the “ping of death” attack.

- DoS attack—Any action or actions that prevent any part of a system from functioning in accordance with its intended purpose. This includes any action that causes unauthorized delay of service. Generally, DoS attacks do not destroy data or resources, but prevent access or use. In network operations, flooding a device with ping packets when the device has not been configured to block or ignore them might effect a denial of service.
- “ping of death”—An attack that sends an improperly large ping echo request packet with the intent of overflowing the input buffers of the destination machine and causing it to crash.

Finding out the types of ICMP traffic in your network can help you decide if your network is being attacked by ICMP packets.

The **ip flow-capture icmp** command captures the value of the ICMP type field and the ICMP code field from the first ICMP packet detected in a flow.

ip flow-capture ip-id

It is possible for a host to receive IP datagrams from two or more senders concurrently. It is also possible for a host to receive multiple IP datagrams from the same host for different applications concurrently. For example, a server might be transferring email and HTTP traffic from the same host concurrently. When a host is receiving multiple IP datagrams concurrently it must be able to identify the fragments from each of the incoming datagrams to ensure that they do not get mixed up during the datagram reassembly process. The receiving host uses the IP header identification field and the source IP address of the IP datagram fragment to ensure that it rebuilds the IP datagrams correctly.

The **ip flow-capture ip-id** command captures the value of the IP header identification field from the first packet in the flow. The value in the IP header identification field is a sequence number assigned by the host that originally transmitted the IP datagram. All of the fragments of an IP datagram have the same identifier value. This ensures that the destination host can match the IP datagram to the fragment during the IP datagram reassembly process. The sending host is responsible for ensuring that each subsequent IP datagram it sends to the same destination host has a unique value for the IP header identification field.

If you are seeing several flows with the same value for the IP header identification field, it is possible that your network is being attacked by a host that is sending the same IP packets over and over.

ip flow-capture packet-length

The value in the packet length field in an IP datagram indicates the length of the IP datagram, excluding the IP header.

Use the **ip flow-capture packet-length** command to capture the value of the IP header packet length field for packets in the flow. The **ip flow-capture packet-length** command keeps track of the minimum and maximum values captured from the flow. The minimum and maximum packet length values are stored in separate fields. This data is updated when a packet with a packet length that is lower or higher than the currently stored value is received. For example if the currently stored value for the minimum packet length is 1024 bytes and the next packet received has a packet length of 512 bytes, the 1024 is replaced with 512.

If you are seeing several IP datagrams in the flow with the same value for the packet-length field, it is possible that your network is being attacked by a host that is constantly sending the same IP packets over-and-over.

ip flow-capture ttl

The TTL field is used to prevent the indefinite forwarding of IP datagrams. The TTL field contains a counter value set by the source host. Each router that processes this datagram decreases the TTL value by 1. When the TTL value reaches 0, the datagram is discarded.

There are two scenarios where an IP packet without a TTL field could live indefinitely in a network:

- The first scenario occurs when a host sends an IP datagram to an IP network that doesn't exist and all of the routers in the network have a gateway of last resort configured—that is, a gateway to which they forward IP datagrams for unknown destinations. Each router in the network receives the datagram and attempts to determine the best interface to use to forward it. Because the destination network is unknown, the best interface for the router to use to forward the datagram to the next hop is always the interface to which the gateway of last resort is assigned.
- The second scenario occurs when there is a mis-configuration in the network that results in a routing loop. For example, suppose that one router forwards an IP datagram to another router because it appears to be the correct next-hop router. The receiving router sends it back because it believes that the correct next-hop router is the router that it received the IP datagram from in the first place.

The **ip flow-capture ttl** command keeps track of the TTL values captured from packets in the flow. The minimum and maximum TTL values are stored in separate fields. This data is updated when a packet with a TTL that is lower or higher than the currently stored value is received. For example if the currently stored value for the minimum TTL is 64 and the next packet received has a TTL of 12, the 64 is replaced by 12.

If you are seeing several flows with the same value for the TTL, it is possible that your network is being attacked by a host that is constantly sending the same IP packets over and over. Under normal circumstances, flows come from many sources, each a different distance away. Therefore you should see a variety of TTLs across all the flows that NetFlow is capturing.

ip flow-capture mac-addresses

The **ip flow-capture mac-addresses** command captures the incoming source mac-address and the outgoing destination mac-address from the first Layer 2 frame in the flow. If you discover that your network is being attacked by Layer 3 traffic, you can use these addresses to identify the device that is transmitting the traffic that is being received by the router and the next hop or final destination device to which the router is forwarding the traffic.

Note This command only applies to traffic that is received or transmitted over Ethernet interfaces.

ip flow-capture vlan-id

A VLAN is a broadcast domain within a switched network. A broadcast domain is defined by the network boundaries within which a network propagates a broadcast frame generated by a station. Some switches can be configured to support single or multiple VLANs. Whenever a switch supports multiple VLANs, broadcasts within one VLAN never appear in another VLAN.

Each VLAN is also a separate Layer 3 network. A router or a multilayer switch must be used to interconnect the Layer 3 networks that are assigned to the VLANs. For example, in order for a device on VLAN 2 with an IP address of 172.16.0.76 to communicate with a device on VLAN 3 with an IP address of 172.17.0.34, the two devices must use a router as an intermediary device, because they are on different Class B IP networks. This is typically accomplished by connecting a switch to a router and configuring the link between them as a VLAN trunk. In order for the link to be used as a VLAN trunk, the interfaces on the router and the switch must be configured for the same VLAN encapsulation type.

Note When a router is configured to route traffic between VLANs, it is often referred to as an inter-VLAN router.

When a router or a switch needs to send traffic on a VLAN trunk, it must either tag the frames using the IEEE 802.1q protocol or encapsulate the frames using the Cisco Inter-Switch Link (ISL) protocol. The VLAN tag or encapsulation header must contain the correct VLAN ID to ensure that the device receiving the frames can process them properly. The device that receives the VLAN traffic examines the VLAN ID from each frame to find out how it should process the frame. For example, when a switch receives an IP broadcast datagram such as an Address Resolution Protocol (ARP) datagram with an 802.1q tagged VLAN ID of 6 from a router, it forwards the datagram to every interface that is assigned to VLAN 6 and any interfaces that are configured as VLAN trunks.

The **ip flow-capture vlan-id** command captures the VLAN ID number from the first frame in the flow it receives that has an 802.1q tag or that is encapsulated with ISL. When the received traffic in the flow is transmitted over an interface that is configured with either 802.1q or ISL trunking, the **ip flow-capture vlan-id** command captures the destination VLAN ID number from the 802.1q or ISL VLAN header from the first frame in the flow.

Note The **ip flow-capture vlan-id** command does not capture the type of VLAN encapsulation in use. The receiving and transmitting interfaces can use different VLAN protocols. If only one of the interfaces is configured as a VLAN trunk, the VLAN ID field is blank for the other interface.

Your router configuration must meet the following criteria before NetFlow can capture the value in the VLAN-ID field:

- It must have at least one LAN interface that is configured with one or more subinterfaces.
- The subinterfaces where you want to receive VLAN traffic must have either 802.1q or ISL enabled.
- The subinterfaces that are configured to receive VLAN traffic must have the **ip flow ingress** command configured on them.

If you discover that your network is being attacked by Layer 3 traffic, you can use the VLAN-ID information to help you find out which VLAN the device that is sending the traffic is on. The information can also help you identify the VLAN to which the router is forwarding the traffic.

Examples

The following example shows how to configure NetFlow to capture the value of the IP fragment-offset field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture fragment-offset
```

The following example shows how to configure NetFlow to capture the value of the ICMP Type field and the value of the Code field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture icmp
```

The following example shows how to configure NetFlow to capture the value of the IP-ID field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture ip-id
```

The following example shows how to configure NetFlow to capture the value of the packet length field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture packet-length
```

The following example shows how to configure NetFlow to capture the TTL field from the IP datagrams in the flow:

```
Router(config)# ip flow-capture ttl
```

The following example shows how to configure NetFlow to capture the MAC addresses from the IP datagrams in the flow:

```
Router(config)# ip flow-capture mac-addresses
```

The following example shows how to configure NetFlow to capture the vlan-id from the IP datagrams in the flow:

```
Router(config)# ip flow-capture vlan-id
```

Related Commands

Command	Description
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-egress input-interface	Removes the NetFlow egress accounting flow key that specifies an output interface and adds a flow key that specifies an input interface for NetFlow egress accounting.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-egress input-interface

To remove the NetFlow egress accounting flow key that specifies an output interface and to add a flow key that specifies an input interface for NetFlow egress accounting, use the **ip flow-egress input-interface** command in global configuration mode. To change the flow key back from an input interface to an output interface for NetFlow egress statistics, use the **no** form of this command.

ip flow-egress input-interface

no ip flow-egress input-interface

Syntax Description

This command has no arguments or keywords.

Defaults

By default NetFlow egress statistics use the output interface as part of the flow key.

Command Modes

Global configuration

Command History

Release	Modification
12.3(11)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must have NetFlow egress accounting configured on your router before you can use this command.

When the NetFlow Egress Support feature is configured, by default it uses the output interface as part of the flow key. The **ip flow-egress input-interface** command changes the key for egress flows so that the ingress interface is used instead of the output interface. This command is used to create a new flow for each input interface.

Examples

In the following example the key for NetFlow reporting of egress traffic is changed from the output interface to the input interface:

```
Router(config)# ip flow-egress input-interface
```

Related Commands

Command	Description
ip flow ingress	Enables NetFlow (ingress) accounting for traffic arriving on an interface.
ip flow egress	Enables NetFlow egress accounting for traffic that the router is forwarding.
ip flow-cache timeout	Specifies NetFlow accounting flow cache parameters.

Command	Description
ip flow-cache entries	Changes the number of entries maintained in the NetFlow accounting cache.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip flow-export destination

To enable the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data, use the **ip flow-export destination** command in global configuration mode. To remove an export destination, use the **no** form of this command.

ip flow-export destination {*hostname* | *ip-address*} *port* [**vrf** *vrf-name*] [**udp**]

no ip flow-export destination {*hostname* | *ip-address*} *port* [**vrf** *vrf-name*] [**udp**]

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information
port	Specifies the number of the user datagram protocol (UDP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF
udp	(Optional) Specifies UDP as the transport protocol. UDP is the default transport protocol.

Command Default

Export of NetFlow information is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1 CA	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S, and support for the Multiple Export Destinations feature was added.
12.2(2)T	This command was modified to enable multiple NetFlow export destinations to be used.
12.2(14)SX	This command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXD	This command was changed to allow you to configure multiple NetFlow export destinations to a router.
12.2(18)SXE	This command was changed to allow you to enter two destination IP addresses on the Supervisor Engine 720 only. See the “Usage Guidelines” section for more information.

Release	Modification
12.2(18)SXH	The **vrf** *name* keyword and argument were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.4(4)T	The **vrf** keyword was added.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Cisco Catalyst 6500 Series Switches

With a PFC3 and Release 12.2(18)SXE and later releases, you can enter multiple NetFlow export destinations on the Supervisor Engine 720 only.

Multiple Export Destinations

If the version of Cisco IOS that you have installed on your networking device supports the NetFlow Multiple Export Destinations feature, you can configure your networking device to export NetFlow data to a maximum of 2 export destinations (collectors) per cache (main and aggregation caches), using any combination of UDP and SCTP as the transport protocol for the destinations. A destination is identified by a unique combination of hostname or IP address and port number or port type.

Note UDP is the default transport protocol used by the **export destination** command. In some Cisco IOS releases you can configure SCTP as the transport protocol if you need reliability and additional redundancy. Refer to the **ip flow-export sctp** command for more information.

Table 10 shows examples of the 2 permitted NetFlow export destinations for each cache.

Table 10 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>".

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Releases 12.4(4)T and 12.2(18)SXH, only one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the export destinations you specified.

Cisco IOS 12.4(4)T, 12.2(18)SXH, and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf** *vrf-name* keyword and argument with the **ip flow-export destination** *ip-address port* command. To configure the global routing table option, enter this command without the optional **vrf** *vrf-name* keyword and argument.

More Information on NetFlow Data Export

For more information on NetFlow Data Export (NDE) on a Cisco Catalyst 6500 series switch, refer to the "Configuring NDE" chapter in the *Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide*.

For more information on NetFlow Data Export (NDE) on a Cisco 7600 series router, refer to the "Configuring NDE" chapter in the *Cisco 7600 Series Cisco IOS Software Configuration Guide*.

For more information on NetFlow Data Export (NDE) on Cisco routers, refer to the "Configuring NetFlow and NetFlow Data Export" chapter in the *Cisco IOS NetFlow Configuration Guide*.

Examples

The following example shows how to configure the networking device to export the NetFlow cache entry to a single export destination system:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
```

The following example shows how to configure the networking device to export the NetFlow cache entry to multiple destination systems:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
Router(config)# ip flow-export destination 10.0.101.254 9991
```

The following example shows how to configure the networking device to export the NetFlow cache entry to two different UDP ports on the same destination system:

```
Router(config)# ip flow-export destination 10.42.42.1 9991
Router(config)# ip flow-export destination 10.42.42.1 9992
%Warning: Second destination address is the same as previous address 10.42.42.1
```

The following example shows how to configure the networking device to export NetFlow data to a export destination that is reachable in VRF group1:

```
Router(config)# ip flow-export destination 172.16.10.2 78 vrf group1
```

Related Commands

Command	Description
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.

Command	Description
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export destination sctp

To enable the reliable export of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export destination sctp** command in global configuration mode. To disable the reliable export of information, use the **no** form of this command.

ip flow-export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

no ip flow-export destination {*ip-address* | *hostname*} *port* [**vrf** *vrf-name*] **sctp**

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
port	Specifies the number of the stream control transmission protocol (SCTP) port on which the workstation is listening for the exported NetFlow datagrams.
vrf *vrf-name*	(Optional) The **vrf** keyword specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing forwarding instance (VRF) for routing to the destination, instead of to the global routing table. **Note** The *vrf-name* argument is the name of the VRF

Command Default

Reliable export of NetFlow information is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

NetFlow Reliable Export Using SCTP

SCTP can be used as an alternative to UDP when you need a more robust and flexible transport protocol than UDP. 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 (connection) between two end-points (peers), which can contain one or more logical channels called streams. The default mode of transmission for a stream is to guarantee reliable ordered delivery of messages using a selective-acknowledgment scheme. SCTP buffers messages until their receipt has been acknowledged by the receiving end-point. SCTP has a congestion control mechanism which limits how much memory is consumed by the SCTP stack, in packet buffering.

VRF Destinations for Exporting NetFlow Data

Before Cisco IOS Release 12.4(4)T, one routing option existed for NetFlow export data packets. NetFlow sent all export data packets to the global routing table for routing to the destinations you specified.

Cisco IOS 12.4(4)T and later releases provide an additional routing option for NetFlow export data packets. You can send NetFlow data export packets to a Virtual Private Network (VPN) routing/forwarding instance (VRF) for routing to the destinations that you specify.

To send NetFlow data export packets to a VRF for routing to a destination, you enter the optional **vrf** *vrf-name* keyword and argument with the **ip flow-export destination** *ip-address port* command. To configure the global routing table option, enter this command without the optional **vrf** *vrf-name* keyword and argument.

Examples

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data:

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
```

The following example shows how to configure the networking device to use SCTP as the transport protocol when exporting NetFlow data to a host that is reachable in VRF group1:

```
Router(config)# ip flow-export destination 172.16.10.2 78 vrf group1 sctp
```

Related Commands

Command	Description
backup	Configures a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries
reliability	Specifies the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export hardware version

To specify the NetFlow Data Export (NDE) version for hardware-switched flows, use the **ip flow-export hardware version** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip flow-export hardware version [**5** | **7**]

no ip flow-export hardware version

Syntax Description

5	Specifies that the export packet uses the version 5 format; see the "Usage Guidelines" section for additional information.
7	Specifies that the export packet uses the version 7 format; see the "Usage Guidelines" section for additional information.

Defaults

Version 7

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.

Usage Guidelines

The **ip flow-export hardware version** command is only supported on systems that have a version 2 Supervisior Engine.

Examples

This example shows how to specify the NDE version for hardware-switched flows:

```
Router(config)# ip flow-export hardware version 5
Router(config)#
```

Related Commands

Command	Description
ip flow-export interface	Enables the interface-based ingress NDE for hardware-switched flows.
ip flow-export version (Supervisor Engine 2)	Specifies the version for the export of information in NetFlow cache entries.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-export interface-names

To enable the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export interface-names** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip flow-export interface-names

no ip flow-export interface-names

Syntax Description

There are no keywords or arguments for this command.

Command Default

Inclusion the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries is disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(2)T	This command was introduced.

Usage Guidelines

The **interface-names** keyword for the **ip flow-export** command configures NetFlow to include the interface names from the flows when it exports the NetFlow cache entry to a destination system.

Prior to the addition of the **interface-names** keyword you had to poll the SNMP MIB for this information and correlate IF-index entries to interface names. After you enable the **ip flow-export interface-names** command the information is included in the exported NetFlow cache entries.

Note Interface names are exported as options templates/records.

Examples

The following example shows how to configure the networking device to include the interface names from the flows when it exports the NetFlow cache entry to a destination system:

```
Router(config)# ip flow-export interface-names
```

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.

Command	Description
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export source

To specify the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries, use the **ip flow-export source** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip flow-export source

no ip flow-export source

Syntax Description

This command has no arguments or keywords.

Command Default

NetFlow uses the IP address of the interface that the datagram is transmitted over as the source IP address for the NetFlow datagrams.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1 CA	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

After you configure NetFlow data export, use the **ip flow-export source** command to specify the interface that NetFlow will use to obtain the source IP address for the NetFlow datagrams that it sends to destination systems, such as a system running NFC Engine. This will override the default behavior (using the IP address of the interface that the datagram is transmitted over as the source IP address for the NetFlow datagrams).

Some of the benefits of using a consistent IP source address for the datagrams that NetFlow sends are:

- The source IP address of the datagrams exported by NetFlow is used by the destination system to determine which router the NetFlow data is arriving from. If your network has two or more paths that can be used to send NetFlow datagrams from the router to the destination system and you do not specify the source interface from which the source IP address is to obtained, the router uses the IP address of the interface that the datagram is transmitted over as the source IP address of the datagram. In this situation the destination system might receive NetFlow datagrams from the same router, but with different source IP addresses. This causes the destination system to treat the NetFlow datagrams as if they were being sent from different routers unless you have configured the destination system to aggregate the NetFlow datagrams it receives from all of the possible source IP addresses in the router into a single NetFlow flow.

- If your router has multiple interfaces that can be used to transmit datagrams to the CNS NFC, and you do not configure the **ip flow-export source interface** command, you will have to add an entry for the IP address of each interface into any access lists that you create for permitting NetFlow traffic. It is easier to create and maintain access-lists for permitting NetFlow traffic from known sources and blocking it from unknown sources when you limit the source IP address for NetFlow datagrams to a single IP address for each router that is exporting NetFlow traffic.

You can use the IP address of a loopback interface as the source IP address for NetFlow traffic by entering the **ip flow-export source interface** *type* [*number* | *slot*/*port*] command (for example, **ip flow-export source interface** *loopback 0*)**.** Doing so makes it more difficult for people who want to attack your network by spoofing the source IP address of your NetFlow-enabled routers to determine which IP address to use. This is because the IP addresses assigned to loopback interfaces are not as easy to discover as the IP addresses assigned to physical interfaces on the router. For example, it is easy to determine the IP address of a Fast Ethernet interface on a router that is connected to a LAN that has end user devices on it. You simply check the configuration of one of the devices for its IP default gateway address.

Examples

The following example shows how to configure NetFlow to use a loopback interface as the source interface for NetFlow traffic.

Caution The interface that you configure as the **ip flow-export source** interface must have an IP address configured and it must be up.

```
Router(config)# ip flow-export source loopback0
```

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export template

To configure template options for the export of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export template** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

Configure template only

ip flow-export template {**refresh-rate** *packets* | **timeout-rate** *minutes*}

no ip flow-export template {**refresh-rate** | **timeout-rate**}

Configure template options

ip flow-export template options {**export-stats** | **refresh-rate** *packets* | **timeout-rate** *minutes* | **sampler**}

no ip flow-export template options {**export-stats** | **refresh-rate** | **timeout-rate** | **sampler**}

Syntax Description

template	Enables the **refresh-rate** and **timeout-rate** keywords for the configuring of Version 9 export templates.
refresh-rate *packets*	(Optional) Specifies the number of export packets that are sent before the options and flow templates are resent. Range:1 to 600 packets. The default is 20 packets. **Note** This applies to the **ip flow-export template refresh-rate** *packets* command.
timeout-rate *minutes*	(Optional) Specifies the interval (in minutes) that the router waits after sending the templates (flow and options) before sending them again. Range: 1 to 3600 minutes. The default is 30 minutes. **Note** This applies to the **ip flow-export template timeout-rate** *minutes* command.
options	(Optional) Enables the **export-stats**, **refresh-rate**, **sampler** and **timeout-rate** keywords for configuring Version 9 export options.
export-stats	(Optional) Enables the export of statistics including the total number of flows exported and the total number of packets exported.
sampler	(Optional) When Version 9 export is configured, this keyword enables the export of an option containing a random-sampler configuration, including the sampler ID, sampling mode, and sampling interval for each configured random sampler. **Note** You must have a flow sampler map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

refresh-rate *packets*	(Optional) Specifies the number of packets that are sent before the configured options records are resent. Range: 1 to 600 packets. The default is 20 packets. **Note** This applies to the **ip flow-export template options refresh-rate** *packets* command.
timeout-rate *minutes*	(Optional) Specifies the interval (in minutes) that the router will wait after sending the options records before they are sent again. Range: 1 to 3600 minutes. The default is 30 minutes. **Note** This applies to the **ip flow-export template options timeout-rate** *minutes* command.

Command Default

The default parameters as noted in the Syntax Description table are used.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip flow-export template options export-stats** command requires that the NetFlow Version 9 export format be already configured on the router.

The **ip flow-export template options sampler** command requires that the NetFlow Version 9 export format and a flow sampler map be already configured on the router.

Examples

The following example shows how to configure NetFlow so that the networking device sends the export statistics (total flows and packets exported) as options data:

```
Router(config)# ip flow-export template options export-stats
```

The following example shows how to configure NetFlow to wait until 100 export packets have been sent, or 60 minutes have passed since the last time the templates were sent (whichever comes first) before the templates are resent to the destination host:

```
Router(config)# ip flow-export template refresh-rate 100
Router(config)# ip flow-export template timeout-rate 60
```

The following example shows how to configure NetFlow to enable the export of information about NetFlow random samplers:

```
Router(config)# ip flow-export template option sampler
```

Tip You must have a **flow-sampler** map configured before you can configure the sampler keyword for the **ip flow-export template options** command.

Related Commands

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.
ip flow-export version	Specifies the export version format for the exporting of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export version

To specify the export version format for the exporting of NetFlow accounting information in NetFlow cache entries, use the **ip flow-export version** command in global configuration mode. To return to the default behavior, use the **no** form of this command.

ip flow-export version {**1** | {**5** | **9**} [**origin-as** | **peer-as**] [**bgp-nexthop**]}

no ip flow-export version {**1** | {**5** | **9**} [**origin-as** | **peer-as**] [**bgp-nexthop**]}

Syntax Description

version 1	Specifies that the export datagram uses the Version 1 format. This is the default.
version 5	Specifies that the export datagram uses the Version 5 format.
version 9	(Specifies that the export datagram uses the Version 9 format.
origin-as	(Optional) Specifies that export statistics include the originating autonomous system (AS) for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer AS for the source and destination.
bgp-nexthop	(Optional) Specifies that export statistics include Border Gateway Protocol (BGP) next-hop related information.

Command Default

Version 1 is the default export format for the exporting of NetFlow accounting information in NetFlow cache entries.

Command Modes

Global configuration (config)

Command History

Release	Modification
11.1 CA	This command was introduced.
12.0(24)S	This command was integrated into Cisco IOS Release 12.0(24)S, and the **9** keyword was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the BGP Next Hop Support, and NetFlow v9 Export Format features was added.
12.2(18)S	Support for the BGP Next Hop Support, NetFlow v9 Export Format was added.
12.0(26)S	Support for the BGP Next Hop Support feature was added
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **ip flow-export version** command supports three export data formats: Version 1, Version 5, and Version 9. Version 1 should be used only when it is the only NetFlow data export format version that is supported by the application that you are using to analyze the exported NetFlow data. Version 5 exports more fields than Version 1. Version 9 is the only flexible export format version.

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 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.

Third-party business partners who produce applications that provide NetFlow Collection Engine or display services for NetFlow do not need to 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.

NetFlow Version 9 has the following characteristics:

- Record formats are defined by templates.
- Template descriptions are communicated from the router to the NetFlow Collection (NFC) 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 (UDP, TCP, SCTP, and so on).

Note The values for the BGP nexthop IP address captured by the **bgp-nexthop** command are exported to a NetFlow export destination only when the Version 9 export format is configured.

Note In order for the BGP information to be populated in the main cache, you must have either a NetFlow export destination configured or a NetFlow aggregation configured.

Note The AS values for the **peer-as** and the **origin-as** keywords are captured only if you have configured an export destination with the **ip flow-export destination** command.

For more information on the available export data formats, see the *Cisco IOS NetFlow Configuration Guide,* Release 12.4T. For more information on the Version 9 data format, see the *Cisco IOS NetFlow Version 9 Export Format Feature Guide*.

Caution Entering the **ip flow-export** or **no ip flow-export** command on the Cisco 12000 Series Internet routers and specifying any format version other than Version 1 (in other words, entering the **ip flow-export** or **no ip flow-export** command and specifying either the **version 5** or **version 9** keyword) causes packet forwarding to stop for a few seconds while NetFlow reloads the route processor and line card Cisco Express Forwarding (CEF) tables. To avoid interruption of service to a live network, either apply this command during a change window or include it in the startup-config file to be executed during a router reboot.

Examples

The following example shows how to configure the networking device to use the NetFlow Version 9 format for the exported data and how to include the originating autonomous system (origin-as) with its corresponding next BGP hop (bgp-nexthop):

```
Router(config)# ip flow-export version 9 origin-as bgp-nexthop
```

Related Commandsi

Command	Description
ip flow-export destination	Enables the export of NetFlow accounting information in NetFlow cache entries to a remote device such as a server running an application that analyzes NetFlow data.
ip flow-export interface-names	Enables the inclusion of the interface names for the flows during the export of NetFlow accounting information in NetFlow cache entries.
ip flow-export source	Specifies the interface from which NetFlow will derive the source IP address for the NetFlow export datagrams containing NetFlow accounting information from NetFlow cache entries.
ip flow-export template	Configures template options for the export of NetFlow accounting information in NetFlow cache entries
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

ip flow-export version (Supervisor Engine 2)

To specify the version for the export of information in NetFlow cache entries, use the **ip flow-export version** command in global configuration mode. To disable information exporting, use the **no** form of this command.

ip flow-export version {**1** | **5** [**origin-as** | **peer-as**] | **6** [**origin-as** | **peer-as**]}

no ip flow-export version

Syntax Description

1	Specifies that the export packet uses the version 1 format; see the "Usage Guidelines" section for additional information.
5	Specifies that the export packet uses the version 5 format; see the "Usage Guidelines" section for additional information.
origin-as	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
6	Specifies that the export packet uses the version 6 format; see the "Usage Guidelines" section for additional information.

Defaults

Version 1

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.

Usage Guidelines

This command documentation applies only to systems that have a version 2 Supervisior Engine.

NDE makes traffic statistics available for analysis by an external data collector. You can use NDE to monitor all Layer 3 switched and all routed IP unicast traffic. In the Cisco 7600 series router, both the Policy Feature Card (PFC) and the Multilayer Switch Feature Card (MSFC) maintain NetFlow caches that capture flow-based traffic statistics. The cache on the PFC captures statistics for Layer 3-switched flows. The cache on the MSFC captures statistics for routed flows.

Note NDE can use NDE version 1, 5, or 6 to export the statistics that are captured on the MSFC for routed traffic.

The number of records stored in the datagram is a variable from 1 to 24 for version 1. The number of records stored in the datagram is a variable between 1 and 30 for version 5.

For more information on NDE, refer to the "Configuring NDE" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to export the data using the version 5 format and include the peer autonomous system information:

```
Router# configure terminal
Router(config)# interface loopback0
Router(config-if)# ip address 4.0.0.1 255.0.0.0
Router(config-if)# exit
Router(config)# interface serial 5/0:0
Router(config-if)# ip unnumbered loopback0
Router(config-if)# no ip mroute-cache
Router(config-if)# encapsulation ppp
Router(config-if)# ip route-cache flow
Router(config-if)# exit
Router(config)# ip flow-export version 5 peer-as
Router(config)# exit
```

Related Commands

Command	Description
ip flow-export destination	Exports the NetFlow cache entries to a specific destination.
ip flow-export source	Specifies the source interface IP address that is used in the NDE datagram.
ip route-cache flow	Enables NetFlow switching for IP routing.

ip flow-export version (Supervisor Engine 720)

To specify the version for the export of information in NetFlow cache entries, use the **ip flow-export version** command in global configuration mode. To return to the default settings, use the **no** form of this command.

ip flow-export version {**1** | {**5** [**origin-as** | **peer-as**]} | {**9** [**bgp-nexthop** | **origin-as** | **peer-as**]}}

no ip flow-export version

Syntax Description

1	Specifies that the export packet use the version 1 format; see the "Usage Guidelines" section for additional information.
5	Specifies that the export packet use the version 5 format; see the "Usage Guidelines" section for additional information.
origin-as	(Optional) Specifies that export statistics include the origin autonomous system for the source and destination.
peer-as	(Optional) Specifies that export statistics include the peer autonomous system for the source and destination.
9	Specifies that the export packet uses the version 9 format; see the "Usage Guidelines" section for additional information.
bgp-nexthop	(Optional) Specifies that export statistics include the BGP next hop for the source and destination.

Defaults

Export of information in NetFlow cache entries is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was changed to support NetFlow version 9 export format on the Supervisor Engine 720.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

NetFlow version 9 is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Version 5 and version 9 formats include the source and destination autonomous-system addresses and source and destination prefix masks. Also, version 9 includes BGP next-hop information.

The number of records stored in the datagram is a variable from 1 to 24 for version 1. The number of records stored in the datagram is a variable between 1 and 30 for version 5.

For more information on NDE, refer to the "Configuring NDE" chapter in the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to export the data using the version 5 format:

```
Router(config)# ip flow-export version 5
Router(config)#
```

Related Commands

Command	Description
ip flow-export version (Supervisor Engine 2)	Specifies the version for the export of information in NetFlow cache entries.
show mls nde	Displays information about the NDE hardware-switched flow.

ip flow-top-talkers

To configure NetFlow top talkers to capture traffic statistics for the unaggregated top flows of the heaviest traffic patterns and most-used applications in the network, use the **ip flow-top-talkers** command in global configuration mode. To disable NetFlow top talkers, use the **no** form of this command.

ip flow-top-talkers

no ip flow-top-talkers

Tip The **ip flow-top-talkers** command does not appear in the configuration until you have configured the **top** *number* and **sort-by** [**bytes** | **packets**] commands.

Syntax Description

This command has no arguments or keywords.

Defaults

NetFlow top talkers is disabled by default.

Command Modes

Global configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

Enabling NetFlow

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands. Optionally, the **match** command can be configured to specify additional matching criteria.

Cache Timeout

The timeout period as specified by the **cache-timeout** command does not start until the **show ip flow top-talkers** command is entered. From that time, the same top talkers are displayed until the timeout period expires. To recalculate a new list of top talkers before the timeout period expires, you can change the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers** command.

A long timeout period for the **cache-timeout** command limits the system resources that are used by the NetFlow top talkers feature. However, the list of top talkers is calculated only once during the timeout period. If a request to display the top talkers is made more than once during the timeout period, the same results are displayed for each request, and the list of top talkers is not recalculated until the timeout period expires.

A short timeout period ensures that the latest list of top talkers is retrieved; however too short a period can have undesired effects:

- 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.
- The list of top talkers is updated every time the top talkers information is requested, possibly causing unnecessary usage of system resources.

A good method to ensure that the latest information is displayed, while also conserving system resources, is to configure a large value for the timeout period, but cause the list of top talkers to be recalculated by changing the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers** command to display the top talkers. Changing the parameters of the **cache-timeout**, **top**, or **sort-by** command causes the list of top talkers to be recalculated upon receipt of the next command line interface (CLI) or MIB request.

Use the **show ip flow top-talkers** command to display the list of unaggregated top flows.

Examples

In the following example, a maximum of four top talkers is configured. The sort criterion is configured to sort the list of top talkers by the total number of bytes for each Top Talker.

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command with the configuration from the previous example:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   349K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   349K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   328K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   303K
4 of 4 top talkers shown. 11 flows processed
```

Related Commands

Command	Description
cache-timeout	Specifies the length of time for which the list of top talkers (heaviest traffic patterns and most-used applications in the network) for the NetFlow MIB and top talkers feature is retained.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip flow top-talkers	Displays the statistics for the top talkers (heaviest traffic patterns and most-used applications in the network).

Command	Description
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

ip multicast netflow

To configure multicast NetFlow accounting on an interface, use the **ip multicast netflow** command in interface configuration mode. To disable multicast NetFlow accounting, use the **no** form of this command.

ip multicast netflow {ingress | egress}

no ip multicast netflow {ingress | egress}

Syntax Description

ingress	Enables multicast NetFlow (ingress) accounting.
egress	Enables multicast NetFlow (egress) accounting.

Defaults

Multicast ingress NetFlow accounting is enabled.

Multicast egress NetFlow accounting is disabled.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.4(11)T	In Cisco IOS Release 12.4(11)T this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.4(12)	In Cisco IOS Release 12.4(12) this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.(33)SRB	In Cisco IOS Release 12.(33)SRB this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.
12.(33)SXH	In Cisco IOS Release 12.(33)SXH this command was moved to global configuration mode and the **ingress** and **egress** keywords were replaced by the **output-counters** keyword. See the **ip multicast netflow output-counters** command.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

ip multicast netflow ingress

NetFlow (ingress) accounting for multicast traffic is enabled by default. The **ip multicast netflow ingress** command does not appear in the configuration.

ip multicast netflow egress

You must enable multicast egress NetFlow accounting on all interfaces for which you want to count outgoing multicast streams.

To display the multicast entries, enter the **show mls netflow ip** command.

Examples

The following example shows how to enable multicast ingress NetFlow accounting on the ingress Ethernet 1/0 interface:

```
Router(config)# interface ethernet 1/0
Router(config-if)# ip multicast netflow ingress
```

The following example shows how to enable multicast egress NetFlow accounting on the egress Ethernet interface 0/0:

```
Router(config)# interface ethernet 0/0
Router(config-if)# ip multicast netflow egress
```

Related Commands

Command	Description
ip multicast netflow rpf-failure	Enables accounting for multicast data that fails the RPF check.
show ip cache flow	Displays a summary of the NetFlow statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip mroute	Displays the contents of the IP multicast routing (mroute) table.
show mls netflow ip	Displays information about the hardware NetFlow IP.

ip multicast netflow output-counters

To enable NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow, use the **ip multicast netflow output-counters** command in global configuration mode. To disable accounting for the number of bytes and packets forwarded, use the **no** form of this command.

ip multicast netflow output-counters

no ip multicast netflow output-counters

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting for the number of bytes and packets of multicast traffic that is forwarded is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.4(11)T	This command was integrated into Cisco IOS Release 12.4(11)T.
12.4(12)	This command was integrated into Cisco IOS Release 12.4(12).
12.2(33)SRB	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SXH	This command was integrated into Cisco IOS Release 12.2(33)SXH.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable NetFlow accounting for the number of bytes and packets of multicast traffic forwarded from an ingress flow:

```
Router# configure terminal
Router(config)# ip multicast netflow output-counters
Router(config)# end
```

Related Commands

Command	Description
ip multicast netflow	Configures multicast NetFlow accounting on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip mroute	Displays the contents of the IP multicast routing (mroute) table.

Command	Description
show ip rpf	Displays how IP multicast routing does RPF.
show ip rpf events	Displays the last 15 triggered multicast RPF check events.

ip multicast netflow rpf-failure

To enable NetFlow accounting for multicast data that fails the reverse path forwarding (RPF) check (meaning any IP packets that lack a verifiable IP source address), use the **ip multicast netflow rpf-failure** command in global configuration mode. To disable accounting for multicast data that fails the RPF check, use the **no** form of this command.

ip multicast netflow rpf-failure

no ip multicast netflow rpf-failure

Syntax Description

This command has no arguments or keywords.

Defaults

Accounting for multicast data that fails the RPF check is disabled.

Command Modes

Global configuration

Command History

Release	Modification
12.3(1)	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

Examples

The following example shows how to enable accounting for multicast data that fails the RPF check:

```
Router# configure terminal
Router(config)# ip multicast netflow rpf-failure
Router(config)# end
```

Related Commands

Command	Description
ip multicast netflow	Configures multicast NetFlow accounting on an interface.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip mroute	Displays the contents of the IP multicast routing (mroute) table.
show ip rpf	Displays how IP multicast routing does RPF.
show ip rpf events	Displays the last 15 triggered multicast RPF check events.

ip route-cache flow

Effective with Cisco IOS Releases 12.4(2)T and 12.2(18)SXD, the **ip route-cache flow** command is replaced by the **ip flow ingress** command. See the **ip flow ingress** command for more information.

To enable NetFlow (ingress) accounting for traffic arriving on an interface, use the **ip route-cache flow** command in interface configuration mode. To disable NetFlow (ingress) accounting for traffic arriving on an interface, use the **no** form of this command in interface configuration mode.

ip route-cache flow

no route-cache flow

Syntax Description

This command has no arguments or keywords.

Defaults

This command is not enabled by default.

Command Modes

Interface configuration

Command History

Release	Modification
11.1	This command was introduced.
12.4(2)T	The **ip route-cache flow** command is automatically remapped to the **ip flow-ingress** command.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(25)S	The **ip route-cache flow** command is automatically remapped to the **ip flow-ingress** command.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXD	The **ip route-cache flow** command is automatically remapped to the **ip flow-ingress** command.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Use this command on an interface or subinterface to enable NetFlow (ingress) accounting for traffic that is being received by the router.

mask (IPv4)

To specify the source or destination prefix mask for a NetFlow accounting prefix aggregation cache, use the **mask** command in aggregation cache configuration mode. To disable the source or destination mask, use the **no** form of this command.

mask {[**destination** | **source**] **minimum** *value*}

no mask {[**destination** | **source**] **minimum** *value*}

Syntax Description

destination	Specifies the destination mask for a NetFlow accounting aggregation cache.
source	Specifies the source mask for a NetFlow accounting aggregation cache.
minimum	Configures the minimum value for the mask.
value	Specifies the value for the mask. Range is from 1 to 32.

Defaults

The default value of the minimum source or destination mask is 0.

Command Modes

NetFlow aggregation cache configuration

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You must have NetFlow accounting configured on your router before you can use this command.

The NetFlow accounting minimum prefix mask allows you to set a minimum mask size for the traffic that will be added to the NetFlow aggregation cache. The source or destination IP address (depending on the type of aggregation cache that you are configuring) is ANDed with the larger of the two masks (the mask that you enter with the **mask** command and the mask in the IP routing table) to determine if the traffic should be added to the aggregation cache that you are configuring.

To enable the minimum prefix mask for a particular aggregation cache, configure the desired minimum mask value using the NetFlow aggregation cache commands. The minimum mask value in the range of 1–32 is used by the router defines the granularity of the NetFlow data that is collected:

- For coarse NetFlow collection granularity, select a low minimum mask value.
- For fine NetFlow collection granularity, select a high minimum mask value.

Specifying the minimum value for the source or destination mask of a NetFlow accounting aggregation cache is permitted only for the following NetFlow aggregation cache types:

- Destination prefix aggregation (destination mask only)
- Destination prefix TOS aggregation (destination mask only)
- Prefix aggregation (source and destination mask)
- Prefix-port aggregation (source and destination mask)
- Prefix-TOS aggregation (source and destination mask)
- Source prefix aggregation (source mask only)
- Source prefix TOS aggregation (source mask only)

Examples

- mask source
- mask destination

mask source

The following example shows how to configure the source-prefix aggregation cache:

```
Router(config)# ip flow-aggregation cache source-prefix
Router(config-flow-cache)# enable
```

The following output from the **show ip cache flow aggregation source-prefix** command shows that, with no minimum mask configured, nine flows are included in the NetFlow source prefix aggregation cache:

```
Router# show ip cache flow aggregation source-prefix

IP Flow Switching Cache, 278544 bytes
  9 active, 4087 inactive, 18 added
  950 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  9 active, 1015 inactive, 18 added, 18 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
Et0/0.1        10.10.10.0      /24  0        4   668   762   179.9
Et0/0.1        10.10.10.0      /24  0        4   668   762   180.8
Et0/0.1        10.10.11.0      /24  0        4   668  1115   180.9
Et0/0.1        10.10.11.0      /24  0        4   668  1115   181.9
Et0/0.1        10.1.0.0        /16  0        4   668  1140   179.9
Et0/0.1        10.1.0.0        /16  0        4   668  1140   179.9
Et0/0.1        172.16.6.0      /24  0        1     6    52   138.4
Et0/0.1        172.16.1.0      /24  0        8  1338  1140   182.1
Et0/0.1        172.16.1.0      /24  0        8  1339  1140   181.0
Router#
```

The following example shows how to configure the source-prefix aggregation cache using a minimum source mask of 8:

```
Router(config)# ip flow-aggregation cache source-prefix
Router(config-flow-cache)# mask source minimum 8
Router(config-flow-cache)# enable
```

The following output from the **show ip cache flow aggregation source-prefix** command shows that with a minimum mask of 8 configured, only five flows from the same traffic used in the previous example are included in the NetFlow source prefix aggregation cache:

```
Router# show ip cache flow aggregation source-prefix
IP Flow Switching Cache, 278544 bytes
  5 active, 4091 inactive, 41 added
  3021 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  5 active, 1019 inactive, 59 added, 59 added to flow
  0 alloc failures, 0 force free
  1 chunk, 7 chunks added

Minimum source mask is configured to /8

Src If         Src Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Et0/0.1        10.0.0.0        /8   0       12   681  1007    64.8
Et0/0.1        172.16.6.0      /24  0        1     3    52    56.1
Et0/0.1        10.0.0.0        /8   0       12   683  1006    64.8
Et0/0.1        172.16.1.0      /24  0        8   450  1140    61.8
Et0/0.1        172.16.1.0      /24  0        8   448  1140    61.5
Router#
```

mask destination

The following example shows how to configure the destination-prefix aggregation cache:

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# enable
```

The following output from the **show ip cache flow aggregation destination-prefix** command shows that, with no minimum mask configured, only two flows are included in the NetFlow source prefix aggregation cache:

```
Router# show ip cache flow aggregation destination-prefix

IP Flow Switching Cache, 278544 bytes
  3 active, 4093 inactive, 3 added
  4841 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  3 active, 1021 inactive, 9 added, 9 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

Dst If         Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Et1/0.1        172.16.10.0     /24  0      120  6737  1059   371.0
Et1/0.1        172.16.10.0     /24  0      120  6739  1059   370.9
```

The following example shows how to configure the destination-prefix aggregation cache using a minimum source mask of 32:

```
Router(config)# ip flow-aggregation cache destination-prefix
Router(config-flow-cache)# mask source minimum 32
Router(config-flow-cache)# enable
```

The following output from the **show ip cache flow aggregation destination-prefix** command shows that, with a minimum mask of 32 configured, 20 flows from the same traffic used in the previous example are included in the NetFlow source prefix aggregation cache:

```
Router# show ip cache flow aggregation destination-prefix

IP Flow Switching Cache, 278544 bytes
  20 active, 4076 inactive, 23 added
  4984 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 21640 bytes
  20 active, 1004 inactive, 29 added, 29 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added

Minimum destination mask is configured to /32

Dst If         Dst Prefix      Msk  AS    Flows  Pkts B/Pk  Active
Et1/0.1        172.16.10.12    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.12    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.14    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.9     /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.11    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.10    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.11    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.10    /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.5     /32  0         1    56  1040    59.5
Et1/0.1        172.16.10.4     /32  0         1    56   940    59.5
Et1/0.1        172.16.10.4     /32  0         1    56   940    59.5
Et1/0.1        172.16.10.7     /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.7     /32  0         1    57  1140    60.6
Et1/0.1        172.16.10.1     /32  0         1    56   628    59.5
Et1/0.1        172.16.10.2     /32  0         1    56   640    59.5
Et1/0.1        172.16.10.17    /32  0         1    56  1140    59.5
Et1/0.1        172.16.10.17    /32  0         1    56  1140    59.5
Et1/0.1        172.16.10.18    /32  0         1    56  1140    59.5
Et1/0.1        172.16.10.19    /32  0         1    56  1140    59.5
Et1/0.1        172.16.10.18    /32  0         1    56  1140    59.5
```

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
show ip cache flow aggregation	Displays the NetFlow accounting aggregation cache statistics.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

match (NetFlow)

To specify match criteria for the NetFlow top talkers (unaggregated top flows), use the **match** command in NetFlow top talkers configuration mode. To remove match criteria for NetFlow top talkers, use the **no** form of this command.

match {[**byte-range** [*max-byte-number min-byte-number* | **max** *max-byte-number* | **min** *min-byte-number*] | **class-map** *map-name* | **destination** [**address** *ip-address* [*mask* | */nn*] | **as** *as-number* | **port** [*max-port-number min-port-number* | **max** *max-port-number* | **min** *min-port-number*] | **direction** [**ingress** | **egress**] | **flow-sampler** *flow-sampler-name* | **input-interface** *interface-type interface-number* | **nexthop-address** *ip-address* [*mask* | */nn*] | **output-interface** *interface-type interface-number* | **packet-range** [*max-packets min-packets* | **max** *max-packets* | **min** *min-packets*] | **protocol** [*protocol-number* | **udp** | **tcp**] | **source** [**address** *ip-address* [*mask* | */nn*] | **as** *as-number* | **port** *max-port-number min-port-number* | **max** *max-port-number* | **min** *min-port-number*] | **tos** [*tos-byte* | **dscp** *dscp* | **precedence** *precedence*]

no match {**byte-range** | **class-map** | **destination** [**address** | **as** | **port**] | **direction** | **flow-sampler** | **input-interface** | **nexthop-address** | **output-interface** | **packet-range** | **protocol** | **source** [**address** | **as** | **port**] | **tos**}

Syntax Description

byte-range	The match criterion is based on the size in bytes of the IP datagrams in the flows.
max-byte-number min-byte-number	Range of sizes for IP datagrams to be matched in bytes. Range: 1–4294967295.
max *max-byte-number*	Maximum size for IP datagrams to be matched in bytes. Range: 1–4294967295.
min *min-byte-number*	Minimum size for IP datagrams to be matched in bytes. Range: 1–4294967295.
class-map	The match criterion is based on a class map.
map-name	Name of the class map to be matched.
destination address	The match criterion is based on the destination IP address.
ip-address	The destination IP address to be matched.
mask	Address mask, in dotted decimal format.
/nn	Address mask as entered in classless interdomain routing (CIDR) format. An address mask of 255.255.255.0 is equivalent to a /24 mask in CIDR format.
destination as	The match criterion is based on the destination autonomous system.
as-number	Autonomous system number to be matched.
destination port	The match criterion is based on the destination port.
max-port-number min-port-number	Range of port numbers for IP datagrams to be matched. Range: 0–65535.
max *max-port-number*	Maximum port number for IP datagrams to be matched. Range: 0–65535.
min *min-port-number*	Minimum port number for IP datagrams to be matched. Range: 0–65535.
direction	Direction of the flow to be matched.
ingress	The match criterion is based on ingress flows.
egress	The match criterion is based on egress flows.
flow-sampler	The match criterion is based on Top Talker sampling.

flow-sampler-name	Name of the Top Talker sampler to be matched.
input-interface	The match criterion is based on the input interface.
interface-type interface-number	The input interface to be used
nexthop address	The match criterion is based on the next-hop IP address.
ip-address	The next-hop IP address to be matched.
mask	Address mask, in dotted decimal format.
/nn	Address mask as entered in classless interdomain routing (CIDR) format. An address mask of 255.255.255.0 is equivalent to a /24 mask in CIDR format.
output-interface	The match criterion is based on the output interface.
interface-type interface-number	The output interface to be used
packet-range	The match criterion is based on the number of IP datagrams in the flows.
max-packets min-packets	Range of number of packets in the flows to be matched. Range: 1–4294967295.
max *max-packet*	Maximum number of packets in the flows to be matched. Range: 1–4294967295.
min *min-packets*	Minimum number of packets in the flows to be matched. Range: 1–4294967295.
protocol	The match criterion is based on protocol.
protocol-number	Protocol number to be matched. Range: 0 to 255.
tcp	Protocol number to be matched as TCP.
udp	Protocol number to be matched as UDP.
source address	The match criterion is based on the source IP address.
ip-address	The source IP address to be matched.
mask	Address mask, in dotted decimal format.
/nn	Address mask as entered in classless interdomain routing (CIDR) format. An address mask of 255.255.255.0 is equivalent to a /24 mask in CIDR format.
source as	The match criterion is based on the source autonomous system.
as-number	Autonomous system number to be matched.
source port	The match criterion is based on the source port.
max-port-number min-port-number	Range of port numbers for IP datagrams to be matched. Range: 0–65535.
max *max-port-number*	Maximum port number for IP datagrams to be matched. Range: 0–65535.
min *min-port-number*	Minimum port number for IP datagrams to be matched. Range: 0–65535.
tos	The match criterion is based on type of service (ToS).
tos-value	ToS to be matched.
dscp *dscp-value*	Differentiated services code point (DSCP) value to be matched.
precedence *precedence-value*	Precedence value to be matched.

Defaults

No matching criteria are specified by default. All top talkers are displayed.

Command Modes

NetFlow top talkers configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This command was integrated into Cisco IOS Release 12.3(11)T. The **direction, ingress,** and **egress** keywords were added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring NetFlow Top Talkers

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands.

Specifying Match Criteria

Use this command to specify match criteria for NetFlow top talkers. Using matching criteria is useful to restrict the list of top talkers.

If you are using a MIB and using simple network management protocol (SNMP) commands to configure this feature, refer to Table 11 for a mapping of the command-line interface (CLI) commands to the MIB SNMP commands:

Table 11 Router CLI Commands and Equivalent SNMP Commands

Router CLI Command	SNMP Command
match source address [*ip-address*] [*mask* | */nn*]	**cnfTopFlowsMatchSrcAddress** *ip-address* **cnfTopFlowsMatchSrcAddressType** *type*[1] **cnfTopFlowsMatchSrcAddressMask** *mask*
match destination address [*ip-address*] [*mask* | */nn*]	**cnfTopFlowsMatchDstAddress** *ip-address* **cnfTopFlowsMatchDstAddressType** *type*1 **cnfTopFlowsMatchDstAddressMask** *mask*
match nexthop address] [*ip-address*] [*mask* | */nn*]]	**cnfTopFlowsMatchNhAddress** *ip-address* **cnfTopFlowsMatchNhAddressType** *type*[1] **cnfTopFlowsMatchNhAddressMask** *mask*
match source port min *port*	**cnfTopFlowsMatchSrcPortLo** *port*
match source port max *port*	**cnfTopFlowsMatchSrcPortHi** *port*
match destination port min *port*	**cnfTopFlowsMatchDstPortLo** *port*
match destination port max *port*	**cnfTopFlowsMatchDstPortHi** *port*

Table 11 Router CLI Commands and Equivalent SNMP Commands (continued)

Router CLI Command	SNMP Command
match source as *as-number*	**cnfTopFlowsMatchSrcAS** *as-number*
match destination as *as-number*	**cnfTopFlowsMatchDstAS** *as-number*
match input-interface *interface*	**cnfTopFlowsMatchInputIf** *interface*
match output-interface *interface*	**cnfTopFlowsMatchOutputIf** *interface*
match tos [*tos-value* | **dscp** *dscp-value* | **precedence** *precedence-value*]	**cnfTopFlowsMatchTOSByte** *tos-value*[2]
match protocol [*protocol-number* | **tcp** | **udp**]	**cnfTopFlowsMatchProtocol** *protocol-number*
match flow-sampler *flow-sampler-name*	**cnfTopFlowsMatchSampler** *flow-sampler-name*
match class-map *class*	**cnfTopFlowsMatchClass** *class*
match packet-range min *minimum-range*	**cnfTopFlowsMatchMinPackets** *minimum-range*
match packet-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets** *maximum-range*
match byte-range min *minimum-range*	**cnfTopFlowsMatchMinBytes** *minimum-range*
match byte-range max *maximum-range*	**cnfTopFlowsMatchMaxPackets** *maximum-range*
direction [**ingress** | **egress**]	**cnfTopFlowsMatchDirection** [**flowDirNone(0)** | **flowDirIngress(1)** | **flowDirEgress(2)**]

1. The only IP version type that is currently supported is IPv4 (type 1).
2. The *tos-value* argument consists of 6 bits for DSCP, 3 bits for precedence, and 8 bits (one byte) for ToS.

Examples

The following example shows how you enter NetFlow top talkers configuration mode and specify that the top talkers are to contain the following characteristics:

- The list of top talkers will have a source IP address that begins with 10.10.0.0 and subnet a mask of 255.255.0.0 (/16).

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# match source address 10.10.0.0/16
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command when the configuration from the previous example is used:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et2/0         10.10.11.3      Et1/0.1       172.16.10.7     06 0041 0041    30K
Et0/0.1       10.10.11.4      Et1/0.1       172.16.10.8     06 0041 0041    30K
Et3/0         10.10.11.2      Et1/0.1       172.16.10.6     06 0041 0041    29K
Et3/0         10.10.18.1      Null          172.16.11.5     11 00A1 00A1    28K
4 of 4 top talkers shown. 10 of 27 flows matched
```

The following example shows how you enter NetFlow top talkers configuration mode and specify that the top talkers are to contain the following characteristics:

- The list of top talkers will have a source IP address that begins with 10.10.0.0 and subnet mask of 255.255.0.0 (/16).
- The list of top talkers will have a destination IP address that begins with 172.16.11.0 and a subnet mask of 255.255.255.0 (/24)

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# match source address 10.10.0.0/16
Router(config-flow-top-talkers)# match destination address 172.16.11.0/24
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command when the configuration from the previous example is used:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et3/0         10.10.18.1      Null          172.16.11.5     11 00A1 00A1    67K
Et3/0         10.10.19.1      Null          172.16.11.6     11 00A2 00A2    67K
2 of 4 top talkers shown. 2 of 30 flows matched
```

Related Commands

Command	Description
cache-timeout	Specifies the length of time for which the list of top talkers (heaviest traffic patterns and most-used applications in the network) for the NetFlow MIB and top talkers feature is retained.
ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip flow top-talkers	Displays the statistics for the top talkers (heaviest traffic patterns and most-used applications in the network).
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.

mls aging fast

To configure the fast-aging time for unicast entries in the Layer 3 table, use the **mls aging fast** command in global configuration mode. To restore the MLS fast-aging time to the default settings, use the **no** form of this command.

mls aging fast [{**threshold** *packet-count*} [{**time** *seconds*}]]

mls aging fast [{**time** *seconds*} [{**threshold** *packet-count*}]]

no mls aging fast

Syntax Description

threshold *packet-count*	(Optional) Specifies the packet count of the fast-aging threshold for Layer 3 fast aging; valid values are from 1 to 128.
time *seconds*	(Optional) Specifies how often entries are checked; valid values are from 1 to 128 seconds.

Defaults

The defaults are as follows:

- Fast aging is disabled.
- If fast aging is enabled, the default *packet-count* value is 100 packets and the *seconds* default is 32 seconds.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

Examples

This example shows how to configure the MLS fast-aging threshold:

```
Router(config)# mls aging fast threshold 50
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls aging long

To configure the long-aging time for unicast entries in the Layer 3 table, use the **mls aging long** command in global configuration mode. To restore the MLS long-aging time to the default settings, use the **no** form of this command.

mls aging long *seconds*

no mls aging long

Syntax Description

seconds	Layer 3 long-aging timeout; valid values are from 64 to 1920 seconds.

Defaults

1920 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

Examples

This example shows how to configure the MLS long-aging threshold:

```
Router(config)# mls aging long 800
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls aging normal

To configure the normal-aging time for unicast entries in the Layer 3 table, use the **mls aging normal** command in global configuration mode. To restore the MLS normal-aging time to the default settings, use the **no** form of this command.

mls aging normal *seconds*

no mls aging normal

Syntax Description

seconds	Normal aging timeout for Layer 3; valid values are from 32 to 4092 seconds.

Defaults

300 seconds

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command has no effect when you configure sampled NetFlow. You must disable sampled NetFlow to allow this command to take effect.

Examples

This example shows how to configure the MLS normal-aging threshold:

```
Router(config)# mls aging normal 200
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls flow

To configure the flow mask for NDE, use the **mls flow** command in global configuration mode. To specify a null flow mask, use the **no** form of this command. To restore the default flow mask, use the **default** form of this command.

mls flow {{**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}}

no mls flow {**ip** | **ipv6**}

default mls flow {**ip** | **ipv6**}

Syntax Description

ip	Enables the flow mask for MLS IP packets.
ipv6	Enables the flow mask for MLS IPv6 packets.
destination	Uses the destination IP address as the key to the Layer 3 table.
destination-source	Uses the destination and the source IP address as the key to the Layer 3 table.
full	Uses the source and destination IP address, the IP protocol (UDP or TCP), and the source and destination port numbers as the keys to the Layer 3 table.
interface-destination-source	Uses all the information in the destination and source flow mask and the source VLAN number as the keys to the Layer 3 table.
interface-full	Uses all the information in the full flow mask and the source VLAN number as the keys to the Layer 3 table.
source	Uses the source IP address as the key to the Layer 3 table.

Defaults

The defaults are as follows:

- For Cisco 7600 series routers that are configured with a Supervisor Engine 2, the default flow mask is **destination**.
- For Cisco 7600 series routers that are configured with a Supervisor Engine 720, the default flow mask is null.
- For IPv4, the default flow mask is null.
- For IPv6, the default flow mask is null.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	This command was changed to support the **ipv6** keyword.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was changed to accommodate per-interface NetFlow.

Usage Guidelines

This command collects statistics for the supervisor engine.

In Cisco IOS Release 12.2(33)SRB and later, the interface-destination-source and interface-full flow masks are the only masks supported for IPv4 traffic. This change was made to accommodate the per-interface NetFlow feature. If other flow mask values are used, the router upgrades them as follows:

- Source, destination, and destination-source flow masks are treated as interface-destination-source.
- Full flow masks are treated as interface-full.

Note To ensure that the Optimized Edge Routing passive-monitoring feature can use NetFlow, you must change the IPv4 flow mask to interface-full.

Examples

This example shows how to set the desired flow mask used to populate the hardware cache for IPv4 NetFlow Data Export:

```
Router(config)# mls flow ip full
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls ip nat netflow-frag-l4-zero

To zero out the Layer 4 information in the NetFlow lookup table for fragmented packets, use the **mls ip nat netflow-frag-l4-zero** command in global configuration mode. To restore the default settings, use the **no** form of this command.

mls ip nat netflow-frag-l4-zero

no mls ip nat netflow-frag-l4-zero

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is supported in PFC3BXL or PFC3B mode only.

Use the **mls ip nat netflow-frag-l4-zero** command to prevent matching the first fragment to the NetFlow shortcut (normal operation) that is sent to the software. The next fragments that are sent to the software are translated based on the Layer 4 port information from the first fragment. The translation based on the Layer 4 port information from the first fragment occurs because there are no fragment bits for matching in the NetFlow key.

When there is a large feature configuration on an interface that requires a large number of ACL TCAM entries/masks that are programmed in TCAM, if the interface is configured as a NAT-inside interface, the feature configuration may not fit in the ACL TCAM and the traffic on the interface may get switched in the software.

Examples

This example shows how to zero out the Layer 4 information in the NetFlow lookup table for fragmented packets:

```
Router (config)# mls ip nat netflow-frag-l4-zero
Router (config)#
```

mls nde flow

To specify the filter options for NDE, use the **mls nde flow** command in global configuration mode. To clear the NDE flow filter and reset the filter to the default settings, use the **no** form of this command.

mls nde flow {**include** | **exclude**} {{**dest-port** *port-num*} | {**destination** *ip-addr ip-mask*} | {**protocol** {**tcp** | **udp**}} | {**source** *ip-addr ip-mask*} | {**src-port** *port-num*}}

no mls nde flow {**include** | **exclude**}

Syntax Description

include	Allows exporting of all flows except the flows matching the given filter.
exclude	Allows exporting of all flows matching the given filter.
dest-port *port-num*	Specifies the destination port to filter; valid values are from 1 to 100.
destination *ip-addr ip-mask*	Specifies a destination IP address and mask to filter.
protocol	Specifies the protocol to include or exclude.
tcp	Includes or excludes TCP.
udp	Includes or excludes UDP.
source *ip-addr ip-mask*	Specifies a source IP address and subnet mask bit to filter.
src-port *port-num*	Specifies the source port to filter.

Defaults

The defaults are as follows:

- All expired flows are exported until the filter is specified explicitly.
- Interface export is disabled (**no mls nde interface**).

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **mls nde flow** command adds filtering to the NDE. The expired flows matching the specified criteria are exported. These values are stored in NVRAM and do not clear when NDE is disabled. If any option is not specified in this command, it is treated as a wildcard. The NDE filter in NVRAM does not clear when you disable NDE.

Only one filter can be active at a time. If you do not enter the **exclude** or **include** keyword, the filter is assumed to be an inclusion filter.

The include and exclude filters are stored in NVRAM and are not removed if you disable NDE.

ip-addr maskbits is the simplified long subnet address format. The mask bits specify the number of bits of the network masks. For example, 172.22.252.00/22 indicates a 22-bit subnet address. The *ip-addr* is a full host address, such as 193.22.253.1/22.

Examples

This example shows how to specify an interface flow filter so that only expired flows to destination port 23 are exported (assuming that the flow mask is set to ip-flow):

```
Router(config)# mls nde flow include dest-port 35
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls nde interface

To populate the additional fields in the NDE packets, use the **mls nde interface** command in interface configuration mode. To disable the population of the additional fields, use the **no** form of this command.

mls nde interface

no mls nde interface

Syntax Description

This command has no arguments or keywords.

Defaults

The defaults are as follows:

- Supervisor Engine 2—Disabled
- Supervisor Engine 720—Enabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

You can configure NDE to populate the following additional fields in the NDE packets:

- Egress interface SNMP index
- Source-autonomous system number
- Destination-autonomous system number
- IP address of the next-hop router

The ingress-interface SNMP index is always populated if the flow mask is interface-full or interface-src-dst.

For detailed information, refer to the "Configuring NDE" chapter of the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide*.

Examples

This example shows how to populate the additional fields in the NDE packets:

```
Router(config)# mls nde interface
Router(config)#
```

This example shows how to disable the population of the additional fields:

```
Router(config)# no mls nde interface
Router(config)#
```

Related Commands

Command	Description
mls netflow	Enables NetFlow to gather statistics.
mls netflow sampling	Enables the sampled NetFlow on an interface.

mls nde sender

To enable MLS NDE export, use the **mls nde sender** command in global configuration mode. To disable MLS NDE export, use the **no** form of this command.

mls nde sender [**version** *version*]

no mls nde sender

Syntax Description

version *version*	(Optional) Specifies the NDE version; valid values are **5** and **7**.

Defaults

The defaults are as follows:

- MLS NDE export is disabled.
- *version* is **7**.

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to enable MLS NDE export:

```
Router(config)# mls nde sender
Router(config)#
```

This example shows how to disable MLS NDE export:

```
Router(config)# no mls nde sender
Router(config)#
```

Related Commands

Command	Description
show mls nde	Displays information about the NDE hardware-switched flow.

mls netflow

To enable NetFlow to gather the statistics, use the **mls netflow** command in global configuration mode. To disable NetFlow from gathering the statistics, use the **no** form of this command.

mls netflow

no mls netflow

Syntax Description

interface	(Optional) Specifies statistics gathering per interface.

Defaults

Enabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

NetFlow gathers the statistics from traffic that flows through the Cisco 7600 series router and stores the statistics in the NetFlow table. You can gather the statistics globally based on a protocol or optionally per interface.

If you are not using NDE or the Cisco IOS features that use the hardware NetFlow table (micro-flow QoS, WCCP, TCP Intercept, or Reflexive ACLs), you may safely disable the use and maintenance of the hardware NetFlow table using the **no mls netflow** command in global configuration mode.

Examples

This example shows how to gather the statistics:

```
Router(config)# mls netflow
Router(config)#
```

This example shows how to disable NetFlow from gathering the statistics:

```
Router(config)# no mls netflow
Disabling MLS netflow entry creation.
Router(config)#
```

Related Commands

Command	Description
show mls netflow	Displays configuration information about the NetFlow hardware.

mls netflow interface

To enable the creation of NetFlow entries on a per-VLAN basis, use the **mls netflow interface** command in global configuration mode. To disable the creation of NetFlow entries, use the **no** form of this command.

mls netflow interface

no mls netflow interface

Syntax Description

This command has no arguments or keywords.

Command Default

Creation of NetFlow entries on a per-VLAN basis disabled.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(33)SXH	This command was introduced on the Catalyst 6500 series switches.

Usage Guidelines

Entering the **mls netflow interface** command creates NetFlow entries for all VLANs. NetFlow entries are created both for VLANs on which bridged-flow statistics is enabled and for VLANs on which NetFlow entry creation is enabled.

For example, if you enable Layer 3 per-VLAN entry creation on VLANs 100 and 200 and at the same time you want to enable bridged-flow statistics on VLANs 150 and 250, NetFlow entry creation and bridged-flow statistics are both enabled on all four VLANs. To collect only bridged-flow statistics for VLAN 150 and 250, you must disable the per-VLAN entry creation feature.

Examples

This example shows how to create NetFlow entries on a per-VLAN basis:

```
Router(config)# mls netflow interface
```

mls netflow maximum-flows

To configure the maximum flow allocation in the NetFlow table, use the **mls netflow maximum-flows** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls netflow maximum-flows [*maximum-flows*]

no mls netflow maximum-flows

Syntax Description

maximum-flows	(Optional) Maximum number of flows; valid values are **16**, **32**, **64**, **80**, **96**, and **128**. See the "Usage Guidelines" section for additional information.

Defaults

128

Command Modes

Global configuration

Command History

Release	Modification
12.2(18)SXD	Support for this command was introduced on the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 720.

The value that you specify for the maximum number of flows is that value times 1000. For example, if you enter 32, you specify that 32,000 is the maximum number of permitted flows.

Examples

This example shows how to configure the maximum flow allocation in the NetFlow table:

```
Router(config)# mls netflow maximum-flows 96
Router(config)#
```

This example shows how to return to the default setting:

```
Router(config)# no mls netflow maximum-flows
Router(config)#
```

Related Commands

Command	Description
show mls netflow table-contention	Displays configuration information at the table contention level for the NetFlow hardware.

mls netflow sampling

To enable sampled NetFlow on an interface, use the **mls netflow sampling** command in interface configuration mode. To disable sampled NetFlow on an interface, use the **no** form of this command.

mls netflow sampling

no mls netflow sampling

Syntax Description

This command has no arguments or keywords.

Defaults

Disabled

Command Modes

Interface configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was changed to support per-interface NetFlow for IPv4 traffic.

Usage Guidelines

In Cisco IOS Release 12.2SRA and earlier, the sampled NetFlow can be global or per interface, depending on the current flow mask. For interface-full and interface-destination-source flow masks, sampled NetFlow is enabled on a per-interface basis. For all the other flow masks, sampled NetFlow is always global and is turned on or off for all interfaces.

Enter the **mls sampling** command to enable sampled NetFlow globally.

Cisco IOS Release 12.2(33)SRB and later support per-interface NetFlow for IPv4 traffic. Per-interface NetFlow has the following configuration requirements:

- In addition to issuing the **mls sampling** command (to globally enable NetFlow on the router), you must also issue the **ip flow ingress** and **mls netflow sampling** commands on individual interfaces to enable sampled NetFlow on the interface.
- The only flow masks allowed for IPv4 traffic are interface-destination-source and interface-full. If other flow mask values are used, the router upgrades them as follows:
  - Source, destination, and destination-source flow masks are treated as interface-destination-source.
  - Full flow masks are treated as interface-full.

Note In addition to populating the hardware NetFlow cache, the **flow hardware mpls-vpn ip** *vrf-id* command also enables sampled NetFlow for IPv4 traffic flows on an MPLS VPN VRF interface.

Examples

This example shows how to enable sampled NetFlow on an interface:

```
Router(config-if)# mls netflow sampling
Router(config-if)#
```

This example shows how to disable sampled NetFlow on an interface:

```
Router(config-if)# no mls netflow sampling
Router(config-if)#
```

Related Commands

Command	Description
flow hardware mpls-vpn ip	Enables NetFlow to create and export hardware NetFlow cache entries for IPv4 traffic on an MPLS VPN VRF interface.
ip flow ingress	Enables (ingress) NetFlow accounting for traffic arriving on an interface.
mls flow ip	Configures the flow mask to use for NetFlow Data Export.
mls sampling	Enables the sampled NetFlow and specifies the sampling method.
show mls sampling	Displays information about the sampled NDE status.

mls netflow usage notify

To monitor the NetFlow table usage on the switch processor and the DFCs, use the **mls netflow usage notify** command in global configuration mode. To return to the default settings, use the **no** form of this command.

mls netflow usage notify {*threshold interval*}

no mls netflow usage notify

Syntax Description

threshold	Percentage threshold that, if exceeded, displays a warning message; valid values are from 20 to 100 percent.
interval	Frequency that the NetFlow table usage is checked; valid values are from 120 to 1000000 seconds.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(17d)SXB1	Support for this command was introduced on the Supervisor Engine 720 and the Supervisor Engine 2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

If the NetFlow table usage monitoring is enabled and the NetFlow table usage exceeds the percentage threshold, a warning message is displayed.

NetFlow gathers statistics from traffic and stores the statistics in the NetFlow table. You can gather statistics globally based on a protocol or optionally per interface.

If you are not using NDE or the Cisco IOS features that use the hardware NetFlow table (micro-flow QoS, WCCP, TCP Intercept, or Reflexive ACLs), you may safely disable the use and maintenance of the hardware NetFlow table using the **no mls netflow** command in global configuration mode.

Examples

This example shows how to configure the monitoring of the NetFlow table usage on the switch processor and the DFCs:

```
Router(config)# mls netflow usage notify 80 300
Router(config)#
```

Related Commands

Command	Description
show mls netflow usage	Displays configuration information about the NetFlow hardware.

mls sampling

To enable the sampled NetFlow and specify the sampling method, use the **mls sampling** command in global configuration mode. To disable the sampled NetFlow, use the **no** form of this command.

mls sampling {{**time-based** *rate*} | {**packet-based** *rate* [*interval*]}}

no mls sampling

Syntax Description

time-based *rate*	Specifies the time-based sampling rate; valid values are **64**, **128**, **256**, **512**, **1024**, **2046**, **4096**, and **8192**. See the "Usage Guidelines" section for additional information.
packet-based *rate*	Specifies the packet-based sampling rate; valid values are **64**, **128**, **256**, **512**, **1024**, **2046**, **4096**, and **8192**.
interval	(Optional) Sampling interval; valid values are from 8000 to 16000 milliseconds.

Defaults

Disabled

Command Modes

Global configuration

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed as follows: • The minimum sampling interval for each rate and period was changed from 4000 to 8000 milliseconds. • The time pair for each sampling rate of time-based sampling was changed; Table 12 lists the new time pairs.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was changed to support per-interface NetFlow for IPv4 traffic.

Usage Guidelines

The sampled NetFlow is supported on Layer 3 interfaces only.

You can enable the sampled NetFlow even if NDE is disabled, but no flows are exported.

With packet-based sampling, a flow with a packet count of *n* is sampled *n*/*m* times, where *m* is the sampling rate.

Cisco IOS Release 12.2(33)SRB and later support per-interface NetFlow for IPv4 traffic. Per-interface NetFlow has the following configuration requirements:

- In addition to issuing the **mls sampling** command (to globally enable NetFlow on the router), you must also issue the **ip flow ingress** and **mls netflow sampling** commands on individual interfaces to enable sampled NetFlow on the interface.
- The **flow hardware mpls-vpn ip** *vrf-id* command enables sampled NetFlow for IPv4 traffic flows on an MPLS VPN VRF interface.
- The only flow masks allowed for IPv4 traffic are interface-destination-source and interface-full. If other flow mask values are used, the router upgrades them as follows:
  - Source, destination, and destination-source flow masks are treated as interface-destination-source.
  - Full flow masks are treated as interface-full.

The time-based sampling is based on a preset interval for each sampling rate.

Table 12 lists the sample intervals for each rate and period.

Table 12 Time-Based Sampling Intervals

Sampling Rate	Sampling Time (milliseconds)	Export Interval (Milliseconds)
1 in 64	128	8192
1 in 128	64	8192
1 in 256	32	8192
1 in 512	16	8192
1 in 1024	8	8192
1 in 2048	4	8192
1 in 4096	4	16384
1 in 8192	4	32768

Examples

This example shows how to enable the time-based NetFlow sampling and set the sampling rate:

```
Router(config)# mls sampling time-based 1024
Router(config)#
```

This example shows how to enable the packet-based NetFlow sampling and set the sampling rate and interval:

```
Router(config)# mls sampling packet-based 1024 8192
Router(config)#
```

Related Commands

Command	Description
flow hardware mpls-vpn ip	Enables NetFlow to create and export hardware NetFlow cache entries for IPv4 traffic on an MPLS VPN VRF interface.
ip flow ingress	Enables (ingress) NetFlow accounting for traffic arriving on an interface.
mls flow ip	Configures the flow mask to use for NetFlow Data Export.

Command	Description
mls netflow sampling	Enables the sampled NetFlow on an interface.
show mls sampling	Displays information about the sampled NDE status.

mode (flow sampler configuration)

To specify a packet interval for random sampled NetFlow accounting and enable the flow sampler map, use the **mode** command in NetFlow flow sampler configuration mode.

mode random one-out-of *packet-interval*

Syntax Description

random	Specifies that sampling uses the random mode.
one-out-of *packet-interval*	Specifies the packet interval (1 out of every *n* packets). For *n*, you can specify from 1 to 65535 packets.

Command Default

The random sampling mode and packet sampling interval are undefined.

Command Modes

NetFlow flow sampler configuration

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **mode random one-out-of** command does not have a **no** format to remove it from the configuration. To disable NetFlow random sampling and packet interval you must remove the flow sampler map that you enabled with the **mode random one-out-of** command.

If you want to change the value that you entered for the *packet-interval* argument repeat the **mode random one-out-of** *packet-interval* command using the new value for *packet-interval*.

Random sampled NetFlow accounting cannot be run concurrently with (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling on the same interface, or subinterface. In order to run random sampled NetFlow accounting, you must first disable (ingress) NetFlow accounting, egress NetFlow accounting, or NetFlow accounting with input filter sampling.

You must enable either Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this command.

Tip If you disable dCEF globally using the **no ip cef [distributed]** command, the **flow-sampler** *sampler-map-name* command is removed from any interfaces that you previously configured for random sampled NetFlow accounting. You must reenter the **flow-sampler** *sampler-map-name* command after you reenable CEF or dCEF to reactivate random sampled NetFlow accounting.

Tip If your router is running Cisco IOS release 12.2(14)S or a later release, or Cisco IOS Release 12.2(15)T or a later release, NetFlow accounting might be enabled through the use of the **ip flow ingress** command instead of the **ip route-cache flow** command. If your router has NetFlow accounting enabled through the use of **ip flow ingress** command you must disable NetFlow accounting, using the **no** form of this command, before you apply a random sampler map for random sampled NetFlow accounting on an interface otherwise the full, un-sampled traffic will continue to be seen.

Examples

The following example shows how to create and enable a random sampler map for random sampled (ingress) NetFlow accounting with CEF switching on Ethernet interface 0/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 0/0
Router(config-if)# no ip route-cache flow
Router(config-if)# ip route-cache cef
Router(config-if)# flow-sampler my-map
```

The following example shows how to create and enable a random sampler map for random sampled egress NetFlow accounting with CEF switching on Ethernet interface 1/0:

```
Router(config)# ip cef
Router(config)# flow-sampler-map my-map
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# interface ethernet 1/0
Router(config-if)# no ip flow egress
Router(config-if)# ip route-cache cef
Router(config-if)# flow-sampler my-map egress
```

The following output from the **show flow-sampler** command verifies that random sampled NetFlow accounting is active:

```
Router# show flow-sampler

 Sampler : my-map, id : 1, packets matched : 7, mode : random sampling mode
  sampling interval is : 100
```

Related Commands

Command	Description
flow-sampler	Applies a flow sampler map for random sampled NetFlow accounting to an interface.
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
netflow-sampler	Enables NetFlow accounting with input filter sampling.
show flow-sampler	Displays the status of random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler).
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

netflow-sampler

To enable NetFlow accounting with input filter sampling, use the **netflow-sampler** command in QoS policy-map class configuration mode. To disable NetFlow accounting with input filter sampling, use the **no** form of this command.

netflow-sampler *sampler-map-name*

no netflow-sampler *sampler-map-name*

Syntax Description

sampler-map-name	Name of the NetFlow sampler map to apply to the class.

Defaults

NetFlow accounting with input filter sampling is disabled.

Command Modes

QoS policy-map class configuration

Command History

Release	Modification
12.3(4)T	This command was introduced.
12.2(25)S	This command was integrated into Cisco IOS Release 12.2(25)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

NetFlow accounting with input filter sampling cannot be run concurrently with (ingress) NetFlow accounting, egress NetFlow accounting, or random sampled NetFlow on the same interface, or subinterface. In order to run NetFlow accounting with input filter sampling, you must first disable (ingress) NetFlow accounting, egress NetFlow accounting, or random sampled NetFlow.

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.

Samplers, also known as filters, are based on classes, but they are enabled on interfaces. You assign a NetFlow input filters sampler to a class by using the **netflow-sampler** command in QoS policy-map class configuration. You the use the **service-policy** command to attach the policy map you defined to one or more interfaces.

Tip If your router is running Cisco IOS release 12.2(14)S or a later release, or Cisco IOS Release 12.2(15)T or a later release, NetFlow accounting might be enabled through the use of the **ip flow ingress** command instead of the **ip route-cache flow** command. If your router has NetFlow accounting enabled through the use of **ip flow ingress** command you must disable NetFlow accounting, using the **no** form of this

command, before you apply a random sampler map for random sampled NetFlow accounting on an interface otherwise the full, un-sampled traffic will continue to be seen.

You must enable either Cisco Express Forwarding (CEF) or distributed CEF (dCEF) before using this command.

Examples

The following example shows how to enable NetFlow accounting with input filter sampling for one class of traffic (traffic with 10 as the first octet of the IP source address):

```
Router(config)# ip cef
Router(config)# flow-sampler-map network-10
Router(config-sampler)# mode random one-out-of 100
Router(config-sampler)# exit
Router(config)# class-map match-any network-10
Router(config-cmap)# match access-group 100
Router(config-cmap)# exit
Router(config)# policy-map network-10
Router(config-pmap)# class network-10
Router(config-pmap-c)# netflow-sampler network-10
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface Ethernet0/0
Router(config-if)# no ip route-cache flow
Router(config-if)# ip route-cache cef
Router(config-if)# interface ethernet 0/0.1
Router(config-if)# service-policy input network-10
Router(config-if)# exit
Router(config)# access-list 100 permit ip 10.0.0.0 0.255.255.255 any
```

The following output from the **show flow-sampler** command verifies that the NetFlow accounting with input filter sampling is active:

```
Router# show flow-sampler

 Sampler : network-10, id : 1, packets matched : 546, mode : random sampling mode
  sampling interval is : 100
```

The following output from the **show ip cache verbose flow** command shows that combination of the **access-list 100 permit ip** *10.0.0.0 0.255.255.255* **any** command and the **match access-group** *100* command has filtered out any traffic in which the source IP address does not have 10 as the first octet:

```
Router# show ip cache verbose flow
IP packet size distribution (116 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .155 .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 .258 .586 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  7 active, 4089 inactive, 66 added
  3768 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 120 seconds
IP Sub Flow Cache, 21640 bytes
  6 active, 1018 inactive, 130 added, 62 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            6      0.0         1   940      0.0      8.8      51.6
TCP-FTP               5      0.0         1   640      0.0      6.9      53.4
TCP-SMTP              2      0.0         3  1040      0.0     41.7      18.5
TCP-other            36      0.0         1  1105      0.0     18.8      41.5
UDP-other             6      0.0         3    52      0.0     54.8       5.5
ICMP                  4      0.0         1   628      0.0     11.3      48.8
Total:               59      0.0         1   853      0.1     20.7      39.6
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
Et0/0.1        10.10.10.3      Et1/0.1        172.16.10.3     06 80  00       1
0016 /0  0                     0016 /0  0     0.0.0.0               840     0.0
Sampler: 1  Class: 1
Et0/0.1        10.10.10.3      Et1/0.1*       172.16.10.3     06 80  00       1
0016 /0  0                     0016 /0  0     0.0.0.0               840     0.0
Sampler: 1  Class: 1  FFlags: 01
Et0/0.1        10.10.11.3      Et1/0.1        172.16.10.7     06 80  00       1
0041 /0  0                     0041 /0  0     0.0.0.0              1140     0.0
Sampler: 1  Class: 1
Et0/0.1        10.10.11.1      Et1/0.1        172.16.10.5     06 80  00       3
0019 /0  0                     0019 /0  0     0.0.0.0              1040    36.7
Sampler: 1  Class: 1
Et0/0.1        10.10.11.1      Et1/0.1*       172.16.10.5     06 80  00       1
0019 /0  0                     0019 /0  0     0.0.0.0              1040     0.0
Sampler: 1  Class: 1  FFlags: 01
Et0/0.1        10.1.1.2        Et1/0.1        172.16.10.10    06 80  00       2
0041 /0  0                     0041 /0  0     0.0.0.0              1140    37.8
Sampler: 1  Class: 1
Et0/0.1        10.10.10.1      Et1/0.1        172.16.10.1     01 80  10       1
0000 /0  0                     0000 /0  0     0.0.0.0               628     0.0
Sampler: 1  Class: 1
```

Related Commands

Command	Description
flow-sampler	Applies a flow sampler map for random sampled NetFlow accounting to an interface.
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
mode (flow sampler configuration)	Specifies a packet interval for NetFlow accounting random sampling mode and enables the flow sampler map.
class-map	Creates a class map to be used for matching packets to a specified class.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy
service-policy	Attaches a policy map to an input interface or virtual circuit (VC).
show flow-sampler	Displays the status of random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler).
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

reliability (NetFlow SCTP)

To specify the level of reliability for the reliable export of NetFlow accounting information in NetFlow cache entries, use the **reliability** command in NetFlow ip flow export stream control transmission protocol (SCTP) configuration mode. To return to the default behavior, use the **no** form of this command.

reliability {**full** | **none** | **partial buffer-limit**}

no reliability {**full** | **none** | **partial buffer-limit** *limit*}

Syntax Description

ip-address | *hostname*	IP address or hostname of the workstation to which you want to send the NetFlow information.
full	Configures guaranteed reliable, ordered delivery of messages to a export destination. This is the default behavior.
none	Specifies that each message is sent once. The message is not stored in a buffer and cannot be retransmitted if it is not received by the export destination.
partial	Specifies the limit on the amount of memory the router will use to buffer messages while waiting for them to be acknowledged by the export destination.
buffer-limit *limit*	Specifies the amount of memory that is available for the buffering of messages that have not been acknowledged by the export destination. Range: 1 to 35000 packets.

Command Default

NetFlow reliable export uses full reliability mode by default.

Command Modes

NetFlow ip flow export SCTP (config-flow-export-sctp)

Command History

Release	Modification
12.4(4)T	This command was introduced.

Usage Guidelines

NetFlow Reliable Export Using SCTP with Partial Reliability

If a stream is specified as unreliable, the packet is simply sent once and not buffered on the exporter at all. If the packet is lost en route to the receiver, the exporter is not notified and cannot re-transmit it

When a stream is specified as partially reliable, a limit can be placed on how much memory should be dedicated to storing un-acknowledged packets. The limit is configurable. If the limit is exceeded and the router attempts to buffer another packet, the oldest un-acknowledged packet is discarded. When SCTP discards the oldest unacknowledged packet a message called a forward-tsn (transmit sequence number) is sent to the export destination 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 a large number of packets to be buffered, for example when you are 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 on how much memory should be dedicated to storing unacknowledged packets can be reduced if other processes on the router begin to run out of memory. Deciding on the best value for the limit on how much memory should be dedicated to storing un-acknowledged packets 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 export destination.

NetFlow Reliable Export Using SCTP with Reliability Disabled

When an SCTP connection is specified as unreliable, exported messages are sent once only and are not buffered. If the message is lost en route to the export destination, it cannot be retransmitted. Unreliable SCTP can be used when the export destination 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.

Examples

The following example shows how to configure the networking device to use full SCTP reliability:

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# reliability full
```

The following example shows how to configure the networking device to use partial SCTP reliability, with a maximum value for the buffer limit of 35000 export packets:

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# reliability partial buffer-limit 35000
```

The following example shows how to configure the networking device to use SCTP with no reliability:

```
Router(config)# ip flow-export destination 172.16.10.2 78 sctp
Router(config-flow-export-sctp)# reliability none
```

Related Commands

Command	Description
backup	Configures a backup destination for the reliable export of NetFlow accounting information in NetFlow cache entries
ip flow-export destination sctp	Enables the reliable export of NetFlow accounting information in NetFlow cache entries.
show ip flow export	Displays the status and the statistics for NetFlow accounting data export.

show flow-sampler

To display the status and statistics for random sampled NetFlow (including mode, packet interval, and number of packets matched for each flow sampler), use the **show flow-sampler** command in user EXEC or privileged EXEC mode.

show flow-sampler [*sampler-map-name*]

Syntax Description

sampler-map-name	(Optional) Name of a flow sampler map.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.3(2)T	This command was introduced.
12.2(18)S	This command was integrated into Cisco IOS Release 12.2(18)S.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

The following is sample output from the **show flow-sampler** command for all flow samplers:

```
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
```

The following is sample output from the **show flow-sampler** command for a flow sampler named mysampler1:

```
Router> show flow-sampler mysampler1

Sampler : mysampler1, id : 1, packets matched : 0, mode : random sampling mode
  sampling interval is : 100
```

Table 13 describes the fields shown in the displays.

Table 13 show flow-sampler Field Descriptions

Field	Description
Sampler	Name of the flow sampler
id	Unique ID of the flow sampler
packets matched	Number of packets matched for the flow sampler

Table 13 show flow-sampler Field Descriptions (continued)

Field	Description
mode	Flow sampling mode
sampling interval is	Flow sampling interval (in packets)

Related Commands

Command	Description
flow-sampler	Applies a flow sampler map for random sampled NetFlow accounting to an interface.
flow-sampler-map	Defines a flow sampler map for random sampled NetFlow accounting.
mode (flow sampler configuration)	Specifies a packet interval for NetFlow accounting random sampling mode.
netflow-sampler	Enables NetFlow accounting with input filter sampling.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

show fm nat netflow data

To display the information about the NAT-related NetFlow data, use the **show fm nat netflow data** command in user EXEC or privileged EXEC mode.

show fm nat netflow data

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	The output was changed to display the information about the NetFlow lookup mode state for fragments.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the information about the NAT-related NetFlow data:

```
Router> show fm nat netflow data

FM Pattern with stat push disabled: 1
Default/TCP/UDP Timeouts:
Def s/w timeout: 86400 h/w timeout: 300 Pattern(ingress): 4
Pattern(egress): 4 Push interval: 1333
TCP s/w timeout: 86400 h/w timeout: 300 Pattern(ingress): 4
Pattern(egress): 4 Push interval: 1333
UDP s/w timeout: 300 h/w timeout: 300 Pattern(ingress): 3
Pattern(egress): 3 Push interval: 100
Port Timeouts:
Idle timeout :3600 secs
Fin/Rst timeout :10 secs
Fin/Rst Inband packets sent per timeout :10000
Netflow mode to Zero-out Layer4 information for fragment packet lookup :
Enabled
Router>
```

Related Commands

Command	Description
show fm summary	Displays a summary of FM Information.

show ip cache flow

To display a summary of the NetFlow accounting statistics, use the **show ip cache flow** command in user EXEC or privileged EXEC mode.

show ip cache [*prefix mask*] [*type number*] **flow**

Syntax Description

prefix mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
type number	(Optional) Displays only the entries in the cache that match the interface type and number combination.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
11.1CA	The information display for the command was updated.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the NetFlow Multicast Support feature was added.
12.2(18)S	Support for the NetFlow Multicast Support feature was added.
12.3(4)T, 12.3(6), 12.2(20)S	The **execute-on** command was implemented on the Cisco 7500 platforms to include the remote execution of the **show ip cache flow** command.
12.3(11)T	Support for egress flow accounting was added, and the [*prefix mask*] and [*type number*] arguments were removed.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to include hardware-entry information.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified to show the VPN name and VPN ID in the display output.

Usage Guidelines

Some of the content in the display of the **show ip cache flow** command uses multiline headings and multiline data fields. Figure 1 uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same.

Figure 1 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the show ip cache verbose flow Command

```
Router# 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        10.251.138.2    Et1/0.1        172.16.10.2     06 80  00     65
0015 /0  0                     0015 /0  0     0.0.0.0                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                                                    127034
```

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running distributed Cisco Express Forwarding (dCEF), NetFlow cache information is maintained on each line card or Versatile Interface Processor. To display this information on a distributed platform by use of the **show ip cache flow** command, you must enter the command at a line card prompt.

Cisco 7600 Series Platforms

The **module** *num* keyword and argument are supported on DFC-equipped modules only.

The VPN name and ID are shown in the display output in the format VPN:vpn-id.

Cisco 7500 Series Platform

The Cisco 7500 series platforms are not supported by Cisco IOS Release 12.4T and later. Cisco IOS Release 12.4 is the last Cisco IOS release to support the Cisco 7500 series platforms.

To display NetFlow cache information using the **show ip cache flow** command on a Cisco 7500 series router that is running dCEF, enter the following sequence of commands:

```
Router# if-con slot-number
LC-slot-number# show ip cache 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 NetFlow cache information:

```
Router# execute-on slot-number show ip cache flow
```

Cisco 12000 Series Platform

To display NetFlow cache information using the **show ip cache flow** command on a Cisco 12000 Series Internet Router, enter the following sequence of commands:

```
Router# attach slot-number
LC-slot-number# show ip cache 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 NetFlow cache information:

```
Router# execute-on slot-number show ip cache flow
```

Examples

The following is a sample display of a main cache using the **show ip cache flow** command:

```
Router# show ip cache flow
IP packet size distribution (2381 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .092 .000 .003 .000 .141 .048 .000 .000 .000 .093 .000 .000 .000 .000 .000

    512  544  576 1024 1536 2048 2560 3072 3584 4096 4608
   .000 .000 .048 .189 .381 .000 .000 .000 .000 .000 .000

IP Flow Switching Cache, 278544 bytes
  22 active, 4074 inactive, 45 added
  2270 ager polls, 0 flow alloc failures
  Active flows timeout in 1 minutes
  Inactive flows timeout in 100 seconds
IP Sub Flow Cache, 25736 bytes
  23 active, 1001 inactive, 47 added, 45 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              4       0.0        67   840      2.6      59.4       0.7
TCP-SMTP             1       0.0        67   168      0.6      59.4       0.5
TCP-BGP              1       0.0        68  1140      0.6      60.3       0.4
TCP-NNTP             1       0.0        68  1340      0.6      60.2       0.2
TCP-other            7       0.0        68   913      4.7      60.3       0.4
UDP-TFTP             1       0.0        68   156      0.6      60.2       0.1
UDP-other            4       0.0        36   151      1.4      45.6      14.7
ICMP                 4       0.0        67   529      2.7      60.0       0.2
Total:              23       0.2        62   710     14.3      57.5       2.9

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Et2/0         192.168.137.78  Et3/0*        192.168.10.67   06 0041 0041    39
Et2/0         172.19.216.196  Et3/0*        192.168.10.38   06 0077 0077    39
Et0/0.1       10.56.78.128    Et1/0.1       172.16.30.231   06 00B3 00B3    48
Et0/0.1       10.10.18.1      Et1/0.1       172.16.30.112   11 0043 0043    47
Et0/0.1       10.162.37.71    Et1/0.1       172.16.30.218   06 027C 027C    48
Et0/0.1       172.16.6.1      Null          224.0.0.9       11 0208 0208     1
```

```
Et0/0.1       10.231.159.251  Et1/0.1       172.16.10.2     06 00DC 00DC    48
Et2/0         10.234.53.1     Et3/0*        192.168.10.32   06 0016 0015    39
Et2/0         10.210.211.213  Et3/0*        192.168.10.127  06 006E 006E    38
Et0/0.1       10.234.53.1     Et1/0.1       172.16.30.222   01 0000 0000    47
Et0/0.1       10.90.34.193    Et1/0.1       172.16.10.2     06 0016 0015    48
Et0/0.1       10.10.10.2      Et1/0.1       172.16.10.2     06 0016 0015    48
Et2/0         10.10.18.1      Et3/0*        192.168.10.162  11 0045 0045    39
Et0/0.1       192.168.3.185   Et1/0.1       172.16.10.2     06 0089 0089    48
Et0/0.1       10.10.11.1      Et1/0.1       172.16.30.51    06 0019 0019    49
Et0/0.1       10.254.254.235  Et1/0.1       172.16.10.2     11 00A1 00A1    48
Et2/0         192.168.23.2    Et3/0*        192.168.10.2    01 0000 0000    39
Et0/0.1       10.251.10.1     Et1/0.1       172.16.10.2     01 0000 0800    47
R3#
```

Note The asterisk (*) immediately following the "DstIf" field indicates that the flow being shown is an egress flow.

The following output of the **show ip cache flow** command on a Cisco 7600 series router shows the source interface some of the traffic in the NetFlow hardware cache on the PFC is VPN Red.

```
PE1# show ip cache flow

------------------------------------------------------------------------------
MSFC:
IP packet size distribution (3139 total packets):
   1-32   64   96  128  160  192  224  256  288  320  352  384  416  448  480
   .000 .685 .309 .000 .000 .000 .000 .003 .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, 56 added
  20904 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 33992 bytes
  0 active, 1024 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added
  last clearing of statistics never
Protocol         Total    Flows   Packets Bytes  Packets Active(Sec) Idle(Sec)
--------         Flows     /Sec     /Flow  /Pkt     /Sec     /Flow     /Flow
TCP-BGP             10      0.0         1    49      0.0       0.0      15.3
TCP-other            6      0.0         2    49      0.0       4.5      15.5
UDP-other           28      0.0        74    63      0.1     320.5      12.7
IP-other             6      0.0       153    80      0.0    1488.3       1.7
Total:              50      0.0        60    68      0.2     358.6      12.2

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP  Pkts
Fa1/1         172.16.1.1      Null          224.0.0.2       11 0286 0286    74
Fa1/1         172.16.1.1      Null          224.0.0.5       59 0000 0000    33

------------------------------------------------------------------------------
PFC:

Displaying Hardware entries in Module 5
 SrcIf            SrcIPaddress          DstIPaddress      Pr       SrcP      Dss
 Fa1/1            172.20.1.2            172.20.1.3        0        0         0
 Fa1/1            172.20.1.3            172.20.1.2        0        0         0
 Fa1/1            172.16.1.2            172.16.2.6        0        0         0
```

```
Fa1/1              172.16.1.1          224.0.0.2         udp      646      64
vpn:red            10.2.0.2            10.1.1.1          0        0        0
.
.
.
PE1#
```

Table 14 describes the significant fields shown in the flow switching cache lines of the display.

Table 14 show ip cache flow Field Descriptions in Flow Switching Cache Display

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 were not currently 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 looked at the cache to cause entries to expire (used by Cisco for diagnostics only).
flow alloc failures	Number of times the NetFlow code tried to allocate a flow but could not.
last clearing of statistics	Standard time output (hh:mm:ss) since the **clear ip flow stats** privileged EXEC command was executed. This time output changes to hours and days after the time exceeds 24 hours.

Table 15 describes the significant fields shown in the activity by protocol lines of the display.

Table 15 show ip cache flow Field Descriptions in Activity by Protocol Display

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 in the cache for this protocol since the last time the statistics were cleared.
Flows/Sec	Average number of flows for this protocol per second; 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; 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; 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; equal to the total packets for this protocol divided by the total number of seconds for this summary period.

Table 15 show ip cache flow Field Descriptions in Activity by Protocol Display (continued)

Field	Description
Active(Sec)/Flow	Number of seconds from the first packet to 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 16 describes the significant fields in the NetFlow record lines of the display.

Table 16 show ip cache flow Field Descriptions in NetFlow Record Display

Field	Description
SrcIf	Interface on which the packet was received.
SrcIPaddress	IP address of the device that transmitted the packet.
DstIf	Interface from which the packet was transmitted. **Note** If an asterisk (*) immediately follows the DstIf field, the flow being shown is an egress flow.
DstIPaddress	IP address of the destination device.
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.)
SrcP	The source protocol port number in hexadecimal.
DstP	The destination protocol port number in hexadecimal.
Pkts	Number of packets switched through this flow.

Related Commands

Command	Description
clear ip flow stats	Clears the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.

show ip cache flow aggregation

To display the NetFlow accounting aggregation cache statistics, use the **show ip cache flow aggregation** command in user EXEC or privileged EXEC mode.

show ip cache [*prefix mask*] [*interface-type interface-number*] [**verbose**] **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**}

Syntax Description

prefix mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
interface-type interface-number	(Optional) Displays only the entries in the cache that match the interface type and interface number combination.
verbose	(Optional) Displays additional information from the aggregation cache.
as	Displays the configuration of the autonomous system aggregation cache scheme.
as-tos	Displays the configuration of the autonomous system type of service (ToS) aggregation cache scheme.
bgp-nexthop-tos	Displays the BGP next hop and ToS aggregation cache scheme.
destination-prefix	Displays the configuration of the destination prefix aggregation cache scheme.
destination-prefix-tos	Displays the configuration of the destination prefix ToS aggregation cache scheme.
prefix	Displays the configuration of the prefix aggregation cache scheme.
prefix-port	Displays the configuration of the prefix port aggregation cache scheme.
prefix-tos	Displays the configuration of the prefix ToS aggregation cache scheme.
protocol-port	Displays the configuration of the protocol port aggregation cache scheme.
protocol-port-tos	Displays the configuration of the protocol port ToS aggregation cache scheme.
source-prefix	Displays the configuration of the source prefix aggregation cache scheme.
source-prefix-tos	Displays the configuration of the source prefix ToS aggregation cache scheme.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(15)S	This command was modified to include new **show** output for ToS aggregation schemes.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the BGP Next Hop Support feature was added.
12.2(18)S	Support for the BGP Next Hop Support feature was added.
12.0(26)S	Support for the BGP Next Hop Support feature was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to include hardware-entry information.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRB	This command was modified to show the VPN name and VPN ID in the display output.

Usage Guidelines

Some of the content in the display of the **show ip cache flow aggregation** command uses multiline headings and multiline data fields. Figure 2 uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same.

Figure 2 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the show ip cache verbose flow Command

```
Router# 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        10.251.138.2    Et1/0.1        172.16.10.2     06 80  00    65
0015 /0  0                     0015 /0  0     0.0.0.0                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
                                                                        127034
```

Cisco 7600 Series Platforms

If you enter the **show ip cache flow aggregation** command without the **module** *num*, the software-switched aggregation cache on the RP is displayed.

The **module** *num* keyword and argument are supported on DFC-equipped modules only.

The VPN name and ID are shown in the display output in the format VPN:vpn-id.

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running Distributed Cisco Express Forwarding (dCEF), NetFlow cache information is maintained on each line card or Versatile Interface Processor. To display this information on a distributed platform by use of the **show ip cache flow** command, you must enter the command at a line card prompt.

Cisco 7500 Series Platform

The Cisco 7500 series platforms are not supported by Cisco IOS Release 12.4T and later. Cisco IOS Release 12.4 is the last Cisco IOS release to support the Cisco 7500 series platforms.

To display NetFlow cache information using the **show ip cache flow** command on a Cisco 7500 series router that is running dCEF, enter the following sequence of commands:

```
Router# if-con slot-number
LC-slot-number# show ip cache 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 NetFlow cache information:

```
Router# execute-on slot-number show ip cache flow
```

Cisco 12000 Series Platform

To display NetFlow cache information using the **show ip cache flow** command on a Cisco 12000 Series Internet Router, enter the following sequence of commands:

```
Router# attach slot-number
LC-slot-number# show ip cache 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 NetFlow cache information:

```
Router# execute-on slot-number show ip cache flow
```

Examples

The following is a sample display of an autonomous system aggregation cache with the **show ip cache flow aggregation as** command:

```
Router# show ip cache flow aggregation as

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If       Src AS  Dst If       Dst AS  Flows   Pkts  B/Pk  Active
Fa1/0         0      Null          0         1      2     49    10.2
Fa1/0         0      Se2/0         20        1      5    100     0.0
```

The following is a sample display of an autonomous system aggregation cache for the prefix mask 10.0.0.0 255.0.0.0 with the **show ip cache flow aggregation as** command:

```
Router# show ip cache 10.0.0.0 255.0.0.0 flow aggregation as

IP Flow Switching Cache, 278544 bytes
  2 active, 4094 inactive, 13 added
  178 ager polls, 0 flow alloc failures

Src If        Src AS  Dst If         Dst AS     Flows    Pkts  B/Pk  Active
e1/2           0      Null           0            1     2       49    10.2
e1/2           0      e1/2           20           1     5      100     0.0
```

The following is a sample display of an destination prefix TOS cache with the **show ip cache flow aggregation destination-prefix-tos** command:

```
Router# show ip cache flow aggregation destination-prefix-tos

IP Flow Switching Cache, 278544 bytes
  7 active, 4089 inactive, 21 added
  5970 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  7 active, 1017 inactive, 21 added, 21 added to flow
```

```
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

Dst If         Dst Prefix      Msk  AS    TOS Flows  Pkts B/Pk  Active
Null           224.0.0.0       /24  0     C0      2     6    72   132.1
Et1/0.1        172.16.30.0     /24  0     00      2   134    28   121.1
Et1/0.1        172.16.30.0     /24  0     80     12   804   780   124.6
Et1/0.1        172.16.10.0     /24  0     00      4   268  1027   121.1
Et1/0.1        172.16.10.0     /24  0     80     12   804   735   123.6
Et3/0          192.168.10.0    /24  0     80     10   669   755   121.8
Et3/0          192.168.10.0    /24  0     00      2   134    28   121.2
Router#
```

The following is a sample display of an prefix port aggregation cache with the **show ip cache flow aggregation prefix-port** command:

```
Router# show ip cache flow aggregation prefix-port

IP Flow Switching Cache, 278544 bytes
  21 active, 4075 inactive, 84 added
  26596 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

Src If         Src Prefix      Msk  Dst If         Dst Prefix      Msk Flows  Pkts
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    2    132
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     67
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     67
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     66
Et2/0          0.0.0.0         /0   Et3/0          192.168.10.0    /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    1     67
Et0/0.1        172.16.6.0      /24  Null           224.0.0.0       /24    1      3
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    1     66
Et2/0          0.0.0.0         /0   Et3/0          192.168.10.0    /24    1     66
Et2/0          0.0.0.0         /0   Et3/0          192.168.10.0    /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     66
Et2/0          0.0.0.0         /0   Et3/0          192.168.10.0    /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.30.0     /24    1     67
Et2/0          0.0.0.0         /0   Et3/0          192.168.10.0    /24    1     67
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    1     66
Et0/0.1        0.0.0.0         /0   Et1/0.1        172.16.10.0     /24    1     66
Et2/0          0.0.0.0         /0   Et3/0          192.168.10.0    /24    1     67
Router#
```

The following is a sample display of an prefix port aggregation cache for the prefix mask 172.16.0.0 255.255.0.0 with the **show ip cache 172.16.0.0 255.255.0.0 flow aggregation prefix-port** command:

```
Router# show ip cache 172.16.0.0 255.255.0.0 flow aggregation prefix-port

IP Flow Switching Cache, 278544 bytes
  21 active, 4075 inactive, 105 added
  33939 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
```

```
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

Src If         Src Prefix     Msk  Dst If         Dst Prefix     Msk Flows  Pkts
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    6    404
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    203
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    203
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    202
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    3    203
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    201
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    202
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    3    202
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    3    202
Et0/0.1        172.16.6.0     /24  Null           224.0.0.0      /24    2      6
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    3    203
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    203
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.30.0    /24    3    203
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    3    202
Et0/0.1        0.0.0.0        /0   Et1/0.1        172.16.10.0    /24    3    203
Router#
```

The following is a sample display of an protocol port aggregation cache with the **show ip cache flow aggregation protocol-port** command:

```
Router# show ip cache flow aggregation protocol-port

IP Flow Switching Cache, 278544 bytes
  19 active, 4077 inactive, 627 added
  150070 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 300 seconds
IP Sub Flow Cache, 25736 bytes
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 2 chunks added

Protocol  Source Port  Dest Port  Flows  Packets  Bytes/Packet  Active
  0x01       0x0000      0x0000      4      270        28        242.4
  0x01       0x0000      0x0000      8      541       290        244.4
  0x06       0x0041      0x0041      4      271      1140        243.3
  0x06       0x0041      0x0041      4      271      1140        243.4
  0x11       0x00A1      0x00A1      4      271       156        243.4
  0x11       0x0043      0x0043      4      271       156        243.4
  0x06       0x00B3      0x00B3      4      271      1140        243.4
  0x06       0x0035      0x0035      4      270      1140        242.5
  0x11       0x0045      0x0045      4      271       156        243.3
  0x06       0x0016      0x0015      4      270       840        242.5
  0x06       0x0016      0x0015     12      810       840        244.5
  0x06       0x0077      0x0077      4      271      1340        243.3
  0x01       0x0000      0x0800      4      270      1500        242.5
  0x06       0x0019      0x0019      4      271       168        243.4
  0x06       0x0089      0x0089      4      271       296        243.4
  0x11       0x0208      0x0208      3        9        72        222.1
  0x06       0x00DC      0x00DC      4      271      1140        243.4
  0x06       0x006E      0x006E      4      271       296        243.4
  0x06       0x027C      0x027C      4      271      1240        243.4
Router#
```

Table 17 describes the significant fields shown in the output of the **show ip cache flow aggregation** command.

Table 17 Field Descriptions for the show ip cache flow aggregation command

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 are not currently assigned to a specific flow at the time this command is entered.
added	Number of flows created since the start of the summary period.
ager polls	Number of times the NetFlow code looked at the cache to cause entries to expire. (Used by Cisco for diagnostics only.)
Src If	Specifies the source interface.
Src AS	Specifies the source autonomous system.
Src Prefix	The prefix for the source IP addresses.
Msk	The numbers of bits in the source or destination prefix mask.
Dst If	Specifies the destination interface.
AS	Autonomous system. This is the source or destination AS number as appropriate for the keyword used. For example, if you enter the **show ip cache flow aggregation destination-prefix-tos** command, this is the destination AS number.
TOS	The value in the type of service (ToS) field in the packets.
Dst AS	Specifies the destination autonomous system.
Dst Prefix	The prefix for the destination IP addresses
Flows	Number of flows.
Pkts	Number of packets.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	The time in seconds that this flow has been active at the time this command was entered.
Protocol	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.)
Source Port	The source port value in hexadecimal.
Dest Port	The destination port value in hexadecimal.
Packets	The number of packets sene in the aggregated flow.
Bytes/Packet	The average size of packets sene in the aggregated flow.

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays a summary of the NetFlow aggregation cache accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow export	Displays the statistics for the data export.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

show ip cache verbose flow

To display a detailed summary of the NetFlow accounting statistics, use the **show ip cache verbose flow** command in user EXEC or privileged EXEC mode.

show ip cache [*prefix mask*] [*type number*] **verbose flow**

Syntax Description

prefix mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
type number	(Optional) Displays only the entries in the cache that match the interface type and number combination.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1	This command was introduced.
11.1CA	The information display for the command was updated.
12.3(1)	Support for the NetFlow Multicast Support feature was added.
12.0(24)S	Multiprotocol Label Switching (MPLS) flow records were added to the command output.
12.3(4)T	The **execute-on** command was implemented on the Cisco 7500 platforms to include the remote execution of the **show ip cache verbose flow** command.
12.3(6)	The command was integrated into Cisco IOS Release 12.3(6).
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)S	Support for the NetFlow Multicast Support feature was added.
12.3(8)T	MPLS flow records were added to the command output for Cisco IOS Release 12.3(8)T.
12.3(11)T	Support for egress flow accounting was added, and the [*prefix mask*] and [*type number*] arguments were removed.
12.3(14)T	Support for NetFlow Layer 2 and Security Monitoring Exports was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to include hardware-entry information.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXE	The output was changed to add fragment offset (FO) information on the Supervisor Engine 720 only.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Usage Guidelines

Use the **show ip cache verbose flow** command to display flow record fields in the NetFlow cache in addition to the fields that are displayed with the **show ip cache flow** command. The values in the additional fields that are shown depend on the NetFlow features that are enabled and the flags that are set in the flow.

Note The flags, and therefore the fields, might vary from flow to flow.

Some of the content in the display of the **show ip cache verbose flow** command uses multiline headings and multiline data fields. Figure 3 uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same

Figure 3 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the show ip cache verbose flow Command

```
Router# 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        10.251.138.2    Et1/0.1        172.16.10.2     06 80  00     65
0015 /0  0                     0015 /0  0     0.0.0.0                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                                                    127034
```

NetFlow Multicast Support

When the NetFlow Multicast Support feature is enabled, the **show ip cache verbose flow** command displays the number of replicated packets and the packet byte count for NetFlow multicast accounting. When you configure the NetFlow Version 9 Export Format feature, this command displays additional NetFlow fields in the header.

MPLS-aware NetFlow

When you configure the MPLS-aware NetFlow feature, you can use the **show ip cache verbose flow** command to display both the IP and MPLS portions of MPLS flows in the NetFlow cache on a router line card. To display only the IP portion of the flow record in the NetFlow cache when MPLS-aware NetFlow is configured, use the **show ip cache flow** command.

NetFlow BGP Nexthop

The NetFlow **bgp-nexthop** command can be configured when either the Version 5 export format or the Version 9 export format is configured. The following caveats apply to the **bgp-nexthop** command:

- The values for the BGP nexthop IP address are exported to a NetFlow collector only when the Version 9 export format is configured.
- In order for the BGP information to be populated in the main cache you must either have a NetFlow export destination configured or NetFlow aggregation configured.

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running distributed Cisco Express Forwarding, 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 7600 Series Platforms

The **module** *num* keyword and argument are supported on DFC-equipped modules only.

Cisco 7500 Series Platform

The Cisco 7500 series platforms are not supported by Cisco IOS Release 12.4T and later. Cisco IOS Release 12.4 is the last Cisco IOS release to support the Cisco 7500 series platforms.

To display detailed NetFlow cache information on a Cisco 7500 series router that is running distributed Cisco Express Forwarding, 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
```

Examples

The following example shows output from the **show ip cache verbose flow** command:

```
Router# 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
```

The preceding output shows the percentage distribution of packets by size. In this display, 20.6 percent of the packets fall in the 1024-byte size range and 79.3 percent fall in the 1536-byte range.

The next section of the output can be divided into three sections. The section and the table corresponding to each are as follows:

- Field Descriptions in the NetFlow Cache Section of the Output (Table 18 on page 144)
- Field Descriptions in the Activity by Protocol Section of the Output (Table 19 on page 144)
- Field Descriptions in the NetFlow Record Section of the Output (Table 20 on page 145)

```
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     0.0.0.0               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

Et0/0.1        172.16.6.1      Et1/0.1        172.16.10.2     01 00  00    4880
0000 /0  0                     0000 /0  0     0.0.0.0              1354    20.1
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      772                            Max plen:       1500
Min TTL:       255                            Max TTL:        255
ICMP type:       0                            ICMP code:        0
IP id:        2943                            FO:             185

Et2/0          192.168.137.78  Et3/0*         192.168.10.67   06 80  00       3
0041 /0  0                     0041 /24 0     172.17.7.2           1140     1.8
FFlags: 01
MAC: (VLAN id) aabb.cc00.2002  (000)          aabb.cc00.2201  (000)
Min TTL:        59                            Max TTL:         59
IP id:           0

Et0/0.1        10.10.13.1      Et1/0.1        172.16.10.2     06 80  00      65
0017 /0  0                     0017 /0  0     0.0.0.0               940    10.8
MAC: (VLAN id) aaaa.bbbb.cc03  (005)          aaaa.bbbb.cc06  (006)
Min plen:      940                            Max plen:       940
Min TTL:        59                            Max TTL:         59
IP id:           0

Et2/0          10.234.53.1     Et3/0*         192.168.10.32   06 80  00       3
0016 /0  0                     0015 /24 0     172.17.7.2           840      1.7
```

```
FFlags: 01
MAC: (VLAN id) aabb.cc00.2002  (000)          aabb.cc00.2201  (000)
Min TTL:        59                            Max TTL:         59
IP id:           0

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

Et2/0          10.10.18.1      Et3/0*         192.168.10.162  11 80  10       4
0045 /0  0                     0045 /24 0     172.17.7.2            156     2.7
FFlags: 01
MAC: (VLAN id) aabb.cc00.2002  (000)          aabb.cc00.2201  (000)
Min TTL:        59                            Max TTL:         59
IP id:           0
```

Note The asterisk (*) immediately following the "DstIf" field indicates that the flow being shown is an egress flow.

Table 18 describes the significant fields shown in the NetFlow cache section of the output.

Table 18 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 for diagnostics only).
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** privileged EXEC 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 changes to hours and days after the time exceeds 24 hours.

Table 19 describes the significant fields shown in the activity by protocol section of the output.

Table 19 Field Descriptions in the Activity by Protocol Section of the Output

Field	Description
Protocol	The types of IP protocols that are in the flows.
Total Flows	Number of flows in the cache for this protocol since the last time the statistics were cleared.

Table 19 Field Descriptions in the Activity by Protocol Section of the Output (continued)

Field	Description
Flows/Sec	Average number of flows for this protocol per second; 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; 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; 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; 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 from the first packet to 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 20 describes the significant fields in the NetFlow record section of the output.

Table 20 Field Descriptions for 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. The value of this field is always set to 0 in MPLS flows.
SrcIPaddress	IP address of the device that transmitted the packet.
DstIf	Interface from which the packet was transmitted. **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 protocol.
Flgs	TCP flags, shown in hexadecimal format (result of bitwise OR of TCP flags from all packets in the flow).

Table 20 Field Descriptions for the NetFlow Record Section of the Output (continued)

Field	Description
Pkts	Number of packets in this flow.
Active	The time in seconds that this flow has been active at the time this command was entered.
MAC	Source and destination MAC addresses from the Layer 2 frames in the flow.
VLAN id	Source and destination VLAN IDs from the Layer 2 frames in the flow.
Min plen	Minimum packet length for the packets in the flows. **Note** This value is updated when a datagram with a lower value is received.
Max plen	Maximum packet length for the packets in the flows. **Note** This value is updated when a datagram with a higher value is received.
Min TTL	Minimum Time-To-Live (TTL) for the packets in the flows. **Note** This value is updated when a datagram with a lower value is received.
Max TTL	Maximum TTL for the packets in the flows. **Note** This value is updated when a datagram with a higher value is received.
IP id	IP identifier field for the packets in the flow.
ICMP type	Internet Control Message Protocol (ICMP) type field from the ICMP datagram in the flow.
ICMP code	ICMP code field from the ICMP datagram in the flow.
FO	This is the value of the fragment offset field from the first fragmented datagram in the second flow. The value is: 185

The following 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 Modular QoS CLI (MQC), the display includes the class ID. If any general flags are set, the output includes the flags.

```
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          10.8.8.8         Et0/0*         10.9.9.9         01 00  10       3
0000 /8  302                   0800 /8  300   10.3.3.3               100     0.1
BGP: 2.2.2.2         Sampler: 1  Class: 1  FFlags: 01
```

Table 21 describes the significant fields shown in the NetFlow output for a sampler, for an MQC policy class, and for general flags.

Table 21 show ip cache verbose flow Field Descriptions for a NetFlow Sampler, an MCQ Policy Class, and General Flags

Field (with Sample Values)	Description
Sampler: 1	Shows the ID of the sampler that captured the flow. The sampler ID in this example is 1.
Class: 1	Shows the ID of the Modular QoS CLI (MQC) traffic class. The class ID in this example is 1.
FFlags: 01	Shows the general flow flag (shown in hexadecimal format), which is the bitwise OR of one or more of the following: • 01 indicates an output (or egress) flow. (If this bit is not set, the flow is an input [or ingress] flow.) • 02 indicates a flow that was dropped (for example, by an access control list [ACL]). • 04 indicates a Multiprotocol Label Switching (MPLS) flow. • 08 indicates an IP version 6 (IPv6) flow. The flow flag in this example is 01 (an egress flow).

The following example shows the NetFlow output for the **show ip cache verbose flow** command when NetFlow BGP next-hop accounting is enabled:

```
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
Et0/0/2        10.0.0.2        Et0/0/4        10.0.0.5        01 00  10      20
0000 /8  0                     0800 /8  0     10.0.0.6             100     0.0
BGP:26.0.0.6
Et0/0/2        10.0.0.2        Et0/0/4        10.0.0.7        01 00  10      20
0000 /8  0                     0800 /8  0     10.0.0.6             100     0.0
BGP:26.0.0.6
Et0/0/2        10.0.0.2        Et0/0/4        10.0.0.7        01 00  10      20
0000 /8  0                     0000 /8  0     10.0.0.6             100     0.0
BGP:26.0.0.6
```

Table 22 describes the significant fields shown in the NetFlow BGP next-hop accounting lines of the output.

Table 22 show ip cache verbose flow Field Descriptions in NetFlow BGP Next-Hop Accounting Output

Field	Description
BGP:BGP_NextHop	Destination address for the BGP next hop

The following example shows the NetFlow output for the **show ip cache verbose flow** command when NetFlow multicast accounting is configured:

```
Router# show ip cache verbose flow
.
.
.
SrcIf          SrcIPaddress    DstIf          DstIPaddress    Pr TOS Flgs  Pkts
Port Msk AS                    Port Msk AS    NextHop              B/Pk  Active
IPM:OPkts    OBytes
IPM:    0       0
Et1/1/1        10.0.0.1        Null           192.168.1.1       01 55  10     100
0000 /8  0                     0000 /0  0     0.0.0.0                28     0.0
IPM:  100    2800
Et1/1/1        10.0.0.1        Se2/1/1.16     192.168.1.1       01 55  10     100
0000 /8  0                     0000 /0  0     0.0.0.0                28     0.0
IPM:    0       0
Et1/1/2        10.0.0.1        Et1/1/4        192.168.2.2       01 55  10     100
0000 /8  0                     0000 /0  0     0.0.0.0                28     0.1
Et1/1/2        10.0.0.1        Null           192.168.2.2       01 55  10     100
0000 /8  0                     0000 /0  0     0.0.0.0                28     0.1
IPM:  100    2800
```

Table 23 describes the significant fields shown in the NetFlow multicast accounting lines of the output.

Table 23 show ip cache verbose flow Field Descriptions in NetFlow Multicast Accounting Output

Field	Description
OPkts	Displays the number of IP multicast (IPM) output packets
OBytes	Displays the number of IPM output bytes
DstIPaddress	Displays the destination IP address for the IPM output packets

The following example shows the output for both the IP and MPLS sections of the flow record in the NetFlow cache when MPLS-aware NetFlow is enabled:

```
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
```

Table 24 describes the significant fields for the IP and MPLS sections of the flow record in the output.

Table 24 show ip cache verbose flow Field Descriptions for the IP and MPLS Sections of the Flow Record in the Output

Field	Description
Pos	Position of the MPLS label in the label stack, starting with 1 as the top label.
Lbl	Value given to the MPLS label by the router.
Exp	Value of the experimental bit.

Table 24 show ip cache verbose flow Field Descriptions for the IP and MPLS Sections of the Flow Record in the Output (continued)

Field	Description
S	Value of the end-of-stack bit. Set to 1 for the oldest entry in the stack and to 0 for all other entries.
LDP/10.10.10.10	Type of MPLS label and associated IP address for the top label in the MPLS label stack.

Related Commands

Command	Description
attach	Connects to a specific line card for the purpose of executing monitoring and maintenance commands on that line card only.
clear ip flow stats	Clears the NetFlow accounting statistics.
execute-on	Executes commands on a line card.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip interface	Displays the usability status of interfaces configured for IP.

show ip cache verbose flow aggregation

To display the aggregation cache configuration, use the **show ip cache verbose flow aggregation** command in user EXEC and privileged EXEC mode.

show ip cache [*prefix mask*] [*interface-type interface-number*] [**verbose**] **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** | **exp-bgp-prefix**}

Syntax Description

prefix mask	(Optional) Displays only the entries in the cache that match the prefix and mask combination.
interface-type interface-number	(Optional) Displays only the entries in the cache that match the interface type and interface number combination.
verbose	(Optional) Displays additional information from the aggregation cache.
as	Displays the configuration of the autonomous system aggregation cache scheme.
as-tos	Displays the configuration of the autonomous system type of service (ToS) aggregation cache scheme.
bgp-nexthop-tos	Displays the BGP next hop and ToS aggregation cache scheme.
destination-prefix	Displays the configuration of the destination prefix aggregation cache scheme.
destination-prefix-tos	Displays the configuration of the destination prefix ToS aggregation cache scheme.
prefix	Displays the configuration of the prefix aggregation cache scheme.
prefix-port	Displays the configuration of the prefix port aggregation cache scheme.
prefix-tos	Displays the configuration of the prefix ToS aggregation cache scheme.
protocol-port	Displays the configuration of the protocol port aggregation cache scheme.
protocol-port-tos	Displays the configuration of the protocol port ToS aggregation cache scheme.
source-prefix	Displays the configuration of the source prefix aggregation cache scheme.
source-prefix-tos	Displays the configuration of the source prefix ToS aggregation cache scheme.
exp-bgp-prefix	Displays the configuration of the exp-bgp-prefix aggregation cache scheme.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.0(3)T	This command was introduced.
12.0(15)S	This command was modified to include new **show** output for ToS aggregation schemes.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.3(1)	Support for the BGP Next Hop Support feature was added.
12.2(18)S	Support for the BGP Next Hop Support feature was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17b)SXA	The output was changed to include hardware-entry information.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXE	The output was changed to add fragment offset (FO) information on the Supervisor Engine 720 only.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2. The **exp-bgp-prefix** aggregation cache was added.

Usage Guidelines

Use the **show ip cache verbose flow aggregation** command to display flow record fields in the NetFlow aggregation cache in addition to the fields that are displayed with the **show ip cache flow aggregation** command. The values in the additional fields that are shown depend on the NetFlow features that are enabled and the flags that are set in the flow.

Note The flags, and therefore the fields, might vary from flow to flow.

Some of the content in the display of the **show ip cache verbose flow aggregation** command uses multiline headings and multiline data fields. Figure 4 uses an example of the output from the **show ip cache verbose flow** to show how to associate the headings with the correct data fields when there are two or more lines of headings and two or more lines of data fields. The first line of the headings is associated with the first line of data fields. The second line of the headings is associated with the second line of data fields, and so on.

When other features such as IP Multicast are configured, the number of lines in the headings and data fields increases. The method for associating the headings with the correct data fields remains the same

Figure 4 How to Use the Multiline Headings and Multiline Data Fields in the Display Output of the show ip cache verbose flow Command

```
Router# 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        10.251.138.2    Et1/0.1        172.16.10.2     06 80  00     65
0015 /0  0                     0015 /0  0     0.0.0.0                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                                                    127034
```

NetFlow Multicast Support

When the NetFlow Multicast Support feature is enabled, the **show ip cache verbose flow** command displays the number of replicated packets and the packet byte count for NetFlow multicast accounting. When you configure the NetFlow Version 9 Export Format feature, this command displays additional NetFlow fields in the header.

MPLS-aware NetFlow

When you configure the MPLS-aware NetFlow feature, you can use the **show ip cache verbose flow** command to display both the IP and MPLS portions of MPLS flows in the NetFlow cache on a router line card. To display only the IP portion of the flow record in the NetFlow cache when MPLS-aware NetFlow is configured, use the **show ip cache flow** command.

NetFlow BGP Nexthop

The NetFlow **bgp-nexthop** command can be configured when either the Version 5 export format or the Version 9 export format is configured. The following caveats apply to the **bgp-nexthop** command:

- The values for the BGP nexthop IP address are exported to a NetFlow collector only when the Version 9 export format is configured.
- In order for the BGP information to be populated in the main cache you must either have a NetFlow export destination configured or NetFlow aggregation configured.

Displaying Detailed NetFlow Cache Information on Platforms Running Distributed Cisco Express Forwarding

On platforms running distributed Cisco Express Forwarding, 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 7600 Series Platforms

The **module** *num* keyword and argument are supported on DFC-equipped modules only.

Cisco 7500 Series Platform

The Cisco 7500 series platforms are not supported by Cisco IOS Release 12.4T and later. Cisco IOS Release 12.4 is the last Cisco IOS release to support the Cisco 7500 series platforms.

To display detailed NetFlow cache information on a Cisco 7500 series router that is running distributed Cisco Express Forwarding, 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
```

Examples

The following is a sample display of an prefix port aggregation cache with the **show ip cache verbose flow aggregation prefix-port** command:

```
Router# show ip cache verbose flow aggregation prefix-port

IP Flow Switching Cache, 278544 bytes
  20 active, 4076 inactive, 377 added
  98254 ager polls, 0 flow alloc failures
  Active flows timeout in 5 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 25736 bytes
```

```
  0 active, 1024 inactive, 0 added, 0 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

Src If         Src Prefix      Dst If         Dst Prefix      TOS Flows    Pkts
               Port Msk                       Port Msk        Pr  B/Pk   Active
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     80     2     136
               0016 /0                        0015 /24        06   840    62.2
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     80     1      68
               00B3 /0                        00B3 /24        06  1140    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     80     1      68
               0043 /0                        0043 /24        11   156    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     00     1      68
               0000 /0                        0000 /24        01    28    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     80     1      68
               0035 /0                        0035 /24        06  1140    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     80     1      68
               0041 /0                        0041 /24        06  1140    60.3
Et2/0          0.0.0.0         Et3/0          192.168.10.0    80     1      68
               006E /0                        006E /24        06   296    60.3
FFlags: 01
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     80     1      68
               0016 /0                        0015 /24        06   840    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     00     1      68
               0000 /0                        0000 /24        01   554    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     80     1      68
               00A1 /0                        00A1 /24        11   156    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     80     1      67
               00DC /0                        00DC /24        06  1140    59.4
Et2/0          0.0.0.0         Et3/0          192.168.10.0    00     1      68
               0000 /0                        0000 /24        01    28    60.2
FFlags: 01
Et2/0          0.0.0.0         Et3/0          192.168.10.0    80     1      67
               0041 /0                        0041 /24        06  1140    59.4
FFlags: 01
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     80     1      68
               0019 /0                        0019 /24        06   168    60.3
Et2/0          0.0.0.0         Et3/0          192.168.10.0    80     1      68
               0016 /0                        0015 /24        06   840    60.3
FFlags: 01
Et0/0.1        0.0.0.0         Et1/0.1        172.16.30.0     80     1      67
               027C /0                        027C /24        06  1240    59.4
Et2/0          0.0.0.0         Et3/0          192.168.10.0    80     1      68
               0077 /0                        0077 /24        06  1340    60.2
FFlags: 01
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     00     1      68
               0000 /0                        0800 /24        01  1500    60.3
Et0/0.1        0.0.0.0         Et1/0.1        172.16.10.0     80     1      68
               0089 /0                        0089 /24        06   296    60.3
Et2/0          0.0.0.0         Et3/0          192.168.10.0    80     1      68
               0045 /0                        0045 /24        11   156    60.2
FFlags: 01
Router#
```

Table 25 describes the significant fields shown in the output of the **show ip cache verbose flow aggregation prefix-port** command.

Table 25 show ip cache verbose flow aggregation Field Descriptions

Field	Description
Src If	Specifies the source interface.
Src AS	Specifies the source autonomous system.
Src Prefix	The prefix for the source IP addresses.
Msk	The numbers of bits in the source or destination prefix mask.
Dst If	Specifies the destination interface.
AS	Autonomous system. This is the source or destination AS number as appropriate for the keyword used. For example, if you enter the **show ip cache flow aggregation destination-prefix-tos** command, this is the destination AS number.
TOS	The value in the type of service (ToS) field in the packets.
Dst AS	Specifies the destination autonomous system.
Dst Prefix	The prefix for the destination IP addresses
Flows	Number of flows.
Pkts	Number of packets.
Port	The source or destination port number.
Msk	The source or destination prefix mask.
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.)
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	The time in seconds that this flow has been active at the time this command was entered.

The following is a sample display of an exp-bgp-prefix aggregation cache with the **show ip cache verbose flow aggregation exp-bgp-prefix** command:

```
Router# show ip cache verbose flow aggregation exp-bgp-prefix

IP Flow Switching Cache, 278544 bytes
  1 active, 4095 inactive, 4 added
  97 ager polls, 0 flow alloc failures
  Active flows timeout in 30 minutes
  Inactive flows timeout in 15 seconds
IP Sub Flow Cache, 17032 bytes
  1 active, 1023 inactive, 4 added, 4 added to flow
  0 alloc failures, 0 force free
  1 chunk, 1 chunk added

Src If         BGP Nexthop     Label  MPLS EXP    Flows    Pkts   B/Pk    Active
Gi4/0/0.102    10.40.40.40     0      0           1        5      100     0.0
```

Table 26 describes the significant fields shown in the output of the **show ip cache verbose flow aggregation exp-bgp-prefix** command.

Table 26 show ip cache verbose flow aggregation Field Descriptions

Field	Description
Src If	Specifies the source interface.
Flows	Number of flows.
Pkts	Number of packets.
B/Pk	Average number of bytes observed for the packets seen for this protocol (total bytes for this protocol or the total number of flows for this protocol for this summary period).
Active	Number of active flows in the NetFlow cache at the time this command was entered.
BGP Nexthop	The exit point from the MPLS cloud.
Label	The MPLS label value. **Note** This value is set to zero on the Cisco 10000.
MPLS EXP	The 3–bit value of the MPLS labels EXP field.

Related Commands

Command	Description
cache	Defines operational parameters for NetFlow accounting aggregation caches.
enabled (aggregation cache)	Enables a NetFlow accounting aggregation cache.
export destination (aggregation cache)	Enables the exporting of NetFlow accounting information from NetFlow aggregation caches.
ip flow-aggregation cache	Enables NetFlow accounting aggregation cache schemes.
mask (IPv4)	Specifies the source or destination prefix mask for a NetFlow accounting prefix aggregation cache.
show ip cache flow aggregation	Displays a summary of the NetFlow aggregation cache accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow export	Displays the statistics for the data export.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

show ip flow export

To display the status and the statistics for NetFlow accounting data export, including the main cache and all other enabled caches, use the **show ip flow export** command in user EXEC or privileged EXEC mode.

show ip flow export [**sctp**] [**verbose**] | [**template**]

Syntax Description

sctp	(Optional) Displays the status and statistics for export destinations that are configured to use the Stream Control Transmission Protocol (SCTP).
verbose	(Optional) Displays the current values for the SCTP fail-over and restore-time timers in addition to the status and statistics that are displayed by the **show ip flow export sctp** command. For a Multiprotocol Label Switching (MPLS) Prefix/Application/Label (PAL) record, displays additional export information, such as the number of MPLS PAL records exported to a NetFlow collector.
template	(Optional) Displays the data export statistics (such as template timeout and refresh rate) for the template-specific configurations.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
11.1CC	This command was introduced.
12.2(2)T	This command was modified to display multiple NetFlow export destinations.
12.0(24)S	The **template** keyword was added.
12.3(1)	Support for the NetFlow v9 Export Format feature was added.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(18)S	Support for the NetFlow v9 Export Format, and Multiple Export Destination features was added.
12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(18)SXD	The output was changed to include information about NDE for hardware-switched flows.
12.2(18)SXF	This command was integrated into Cisco IOS Release 12.2(18)SXF.
12.4(4)T	The **sctp** and **verbose** keywords were added.
12.2(28)SB	The number of MPLS PAL records exported by NetFlow was added to the verbose keyword output.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.

Examples

The following is sample output from the **show ip flow export** command with NetFlow export over User Datagram Protocol (UDP) (the default NetFlow export transport protocol) configured on the networking device:

Note No NetFlow export over SCTP destinations are configured:

```
Router# show ip flow export

Flow export v9 is enabled for main cache
  Exporting flows to 172.17.10.2 (100)
  Exporting using source interface Loopback0
  Version 9 flow records
  62 flows exported in 17 udp datagrams
  0 flows failed due to lack of export packet
  8 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
  0 export packets were dropped enqueuing for the RP
  0 export packets were dropped due to IPC rate limiting
  0 export packets were dropped due to output drops
```

The following is sample output from the **show ip flow export** command with NetFlow export over UDP and NetFlow SCTP export destinations configured:

```
Router# show ip flow export

Flow export v9 is enabled for main cache
  Exporting flows to 172.17.10.2 (100)
  Exporting flows to 172.16.45.57 (100) via SCTP
  Exporting using source interface Loopback0
  Version 9 flow records
  Cache for destination-prefix aggregation:
    Exporting flows to 192.168.247.198 (200) via SCTP
    Exporting using source IP address 172.16.254.254
  479 flows exported in 318 udp datagrams
  467 flows exported in 315 sctp messages
  0 flows failed due to lack of export packet
  159 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
```

Table 27 describes the significant fields shown in the display of the **show ip flow export** command.

Table 27 show ip flow export Field Descriptions

Field	Description
Exporting flows to	Indicates the export destinations and ports. The ports are in parentheses. **Note** When the export destination is configured with the NetFlow Reliable Transport Using SCTP feature the port number is followed by the text "via SCTP" in the display output.
Exporting using source IP address or Exporting using source interface	Indicates the source IP address or source interface. **Note** The source interface is used when you have configured the **ip flow-export source** *interface-type interface-number* command.
Version flow records	Displays the version of the flow records.
Cache for destination-prefix aggregation	Indicates the type of NetFlow aggregation caches that are configured. **Note** The indented lines below the name of the NetFlow aggregation cache indicate the export parameters that are configured for this cache.
flows exported in udp datagrams	Indicates the total number of export packets (datagrams) sent over UDP, and the total number of flows contained within them.
flows exported in sctp messages	Displays the total number of export packets (messages) sent over SCTP, and the total number of flows contained within them. **Note** SCTP is a message-oriented transport protocol. Therefore SCTP traffic is referred to as messages instead of datagrams.
flows failed due to lack of export packet	Indicates the number of flows that failed because no memory was available to create an export packet.
159 export packets were sent up to process level	The packet could not be processed by Cisco Express Forwarding or by fast switching.
export packets were dropped due to no fib export packets were dropped due to adjacency issues	Indicates the number of packets that Cisco Express Forwarding was unable to switch, or forward to the process level.
0 export packets were dropped due to fragmentation failures 0 export packets were dropped due to encapsulation fixup failures	Indicates the number of packets that were dropped because of problems constructing the IP packet.

Table 27 show ip flow export Field Descriptions (continued)

Field	Description
0 export packets were dropped enqueuing for the RP 0 export packets were dropped due to IPC rate limiting	Indicates the number of times that there was a problem transferring the export packet between the RP and the line card.
0 export packets were dropped due to output drops	Indicates the number of times that the send queue was full while the packet was being sent.

The following is sample output from the **show ip flow export sctp** command with NetFlow SCTP export primary and backup SCTP export destinations configured for the NetFlow main cache and the NetFlow destination-prefix aggregation cache. The primary SCTP export destinations are active:

```
Router# show ip flow export sctp

IPv4 main cache exporting to 172.16.45.57, port 100, none
status: connected
backup mode: fail-over
912 flows exported in 619 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: not connected
   fail-overs: 2
   9 flows exported in 3 sctp messages.
   0 packets dropped due to lack of SCTP resources
destination-prefix cache exporting to 172.16.12.200, port 100, full
status: connected
backup mode: redundant
682 flows exported in 611 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: 8
   2 flows exported in 2 sctp messages.
   0 packets dropped due to lack of SCTP resources
```

The following is sample output from the **show ip flow export sctp** command with NetFlow SCTP export primary and backup SCTP export destinations configured for the NetFlow main cache and the NetFlow destination-prefix aggregation cache. The backup SCTP export destinations are active because the primary SCTP export destinations are unavailable.

```
Router# show ip flow export sctp

IPv4 main cache exporting to 172.16.45.57, port 100, none
status: fail-over
backup mode: fail-over
922 flows exported in 625 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, active for 00:00:24
```

```
   fail-overs: 3
   11 flows exported in 4 sctp messages.
   0 packets dropped due to lack of SCTP resources
destination-prefix cache exporting to 172.16.12.200, port 100, full
status: fail-over
backup mode: redundant
688 flows exported in 617 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, active for 00:00:00
   fail-overs: 13
   2 flows exported in 2 sctp messages.
   0 packets dropped due to lack of SCTP resources
Router#
```

Table 28 describes the significant fields shown in the display of the **show ip flow export sctp** and the **show ip flow export sctp verbose** commands.

Table 28 show ip flow export sctp Field Descriptions

Field	Description
IPv4 main cache exporting to 172.16.45.57, port 100, none	Indicates the type of cache, the IP address and port number used to reach the destination, and the level of reliability for the association: • IPv4 main cache—The type of NetFlow cache to which the display output applies. • 172.16.45.57—The IP address used for the SCTP export destination. • port 100—The SCTP port used for the SCTP export destination. • none—The level of reliability for this association. **Note** The reliability options are full and none.
status	The current state of each association. The states are: • initializing—The association is being established. • connected—The association is established. **Note** If this is a backup SCTP export destination configured for fail-over mode, you see an additional message indicating how long the association has been active. For example, active for 00:00:01. • not connected—The association will be established when the primary SCTP export backup destination is no longer available. • fail-over—The primary SCTP export destination is no longer available. The backup SCTP export destination is being used. • re-establishing—An association that has been active before is being reestablished.

Table 28 show ip flow export sctp Field Descriptions (continued)

Field	Description
backup mode	The backup mode of each association. The modes are: • redundant—The association is established (connected). **Note** The fact that the association is established does not mean that it is being used to export NetFlow data. • fail-over—The association will be established after the primary association fails.
flows exported in sctp messages	Indicates the total number of export packets (messages) sent over SCTP, and the total number of flows contained within them. **Note** SCTP is a message-oriented transport protocol. Therefore, SCTP traffic is referred to as messages instead of datagrams.
packets dropped due to lack of SCTP resources	The number of packets that were dropped due to lack of SCTP resources.
fail-over time: milli-seconds	The period of time that the networking device waits after losing connectivity to the primary SCTP export destination before attempting to use a backup SCTP export destination. **Note** This field is displayed when you use the **verbose** keyword after the **show ip flow export sctp** command.
restore time: seconds	The period of time that the networking device waits before reverting to the primary SCTP export destination after connectivity to it has been restored. **Note** This field is displayed when you use the **verbose** keyword after the **show ip flow export sctp** command.
backup: 192.168.247.198 port 200	The IP address and SCTP port used for the SCTP export backup destination. • 192.168.247.198—The IP address of the SCTP backup association. • port 200—The SCTP port used for the SCTP backup association.
fail-overs	The number of times that fail-over has occurred.
destination-prefix cache exporting to 172.16.12.200, port 100, full	Indicates the type of cache configures, the destination address and port number for the SCTP export, and the level of reliability for the association: • destination-prefix cache—The type of NetFlow aggregation cache configured. • 172.16.12.200—The IP address used for the SCTP export destination. • port 100—Indicates the SCTP port used for the SCTP export destination. • full—The level of reliability for this association,

The following is sample output from the **show ip flow export template** command:

```
Router# show ip flow export template

   Template Options Flag = 1
   Total number of Templates added = 4
   Total active Templates = 4
   Flow Templates active = 3
   Flow Templates added = 3
   Option Templates active = 1
   Option  Templates added = 1
   Template ager polls = 2344
   Option Template ager polls = 34
Main cache version 9 export is enabled
 Template export information
   Template timeout = 30
   Template refresh rate = 20
 Option export information
   Option timeout = 800
   Option refresh rate = 300
Aggregation cache destination-prefix 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
```

Table 29 describes the significant fields shown in the display of the **show ip flow export template** command.

Table 29 show ip flow export template Field Descriptions

Field	Description
Template Options Flag	Identifies which options are enabled. The values are: • *0—No o*ption template configured. • 1—Version 9 option export statistics configured. • 2—Random sampler option template configured. • 4—Version 9 option export statistics for IPv6 configured.
Total number of Templates added	Indicates the number of Flow Templates and Option Templates that have been added since Version 9 export was first configured. This value in this field is the sum of the “Flow Templates added” and the “Option Templates added” fields. The value is incremented when a new template is created, because each template requires a unique ID.
Total active Templates	This is the sum of the values in the “Flow Templates active” and “Option Templates” active fields. The value in this field is incremented when a new data template or option template is created.

Table 29 show ip flow export template Field Descriptions (continued)

Field	Description
Flow Templates active	Indicates the number of (data) templates in use for Version 9 data export. When a new data template is created, this count, the "Total active Templates," the "Flow Templates added," and the "Total number of Templates added" counts are all incremented. **Note** When a data template is removed, only the "Flow Templates active" count and the "Total active Templates" count are decremented.
Flow Templates added	Indicates the number of Flow Templates and Option Templates that have been added since Version 9 export was first configured. The value is incremented when a new flow template is created, because each template requires a unique ID.
Option Templates active	Indicates the number of option templates which are currently in use for Version 9 options export. Configuring a new option increments this count and also the "Total active Templates," the "Option Templates added," and the "Total number of Templates added" counts. Removing (unconfiguring) an option decrements only the "Option Templates active" count and the "Total active Templates" count.
Option Templates added	Indicates the number of Option Templates that have been added since Version 9 export was first configured. The count is incremented when a new option template is created, because each template requires a unique ID.
Template ager polls	The number of times, since Version 9 export was configured, that the (data) template ager has run. The template ager checks up to 20 templates per invocation, resending any that need refreshed.
Option Template ager polls	The number of times, since Version 9 export was configured, that the option template ager has run. The template ager checks up to 20 templates per invocation, resending any that need refreshed.
Main cache version 9 export is enabled	NetFlow export Version 9 is enabled for the main NetFlow cache.
Template export information	Template timeout—The interval (in minutes) that the router waits after sending the templates (flow and options) before they are sent again. You can specify from 1 to 3600 minutes. The default is 30 minutes. • Template refresh rate—The number of export packets that are sent before the options and flow templates are sent again. You can specify from 1 to 600 packets. The default is 20 packets.

Table 29 show ip flow export template Field Descriptions (continued)

Field	Description
Option export information	• Option timeout—The interval (in minutes) that the router will wait after sending the options records before they are sent again. You can specify from 1 to 3600 minutes. The default is 30 minutes. • Option refresh rate—The number of packets that are sent before the configured options records are sent again. You can specify from 1 to 600 packets. The default is 20 packets.
Aggregation cache destination-prefix version 9 export is enabled	NetFlow export Version 9 is enabled for the NetFlow destination-prefix aggregation cache.

The following example displays the additional line in the **show ip flow export** command output when the **verbose** keyword is specified and MPLS PAL records are being exported to a NetFlow collector:

```
Router# show ip flow export verbose

Flow export v9 is enabled for main cache
  Exporting flows to 10.23.0.5 (4200)
  Exporting using source IP address 10.2.72.35
  Version 9 flow records
  Cache for destination-prefix aggregation:
    Exporting flows to 10.2.0.1 (4200)
    Exporting using source IP address 10.2.72.35
    182128 MPLS PAL records exported
  189305 flows exported in 6823 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 swat72f3#
```

The line of output added for the MPLS PAL records precedes the "*x* flows exported in *y* UDP datagrams" line. In this example, the additional line of output precedes "189305 flows exported in 6823 UDP datagrams."

Related Commands

Command	Description
ip flow-export	Enables export of NetFlow accounting information in NetFlow cache entries.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays the NetFlow accounting configuration on interfaces.
show mpls flow mappings	Displays the full MPLS PAL table.

show ip flow top

The documentation for the **show ip flow top** command was merged with the **show ip flow top-talkers** command in Cisco IOS Release 12.4(9)T.

show ip flow top-talkers

To display the statistics for the NetFlow aggregated top talkers or unaggregated top flows, use the **show ip flow top-talkers** command in user EXEC or privileged EXEC mode.

Cisco IOS Releases 12.4(9)T and Newer

show ip flow top-talkers [**verbose**] | [{*number* [**from-cache main**] **aggregate** *aggregate-field* [**sorted-by** {**aggregate** | **bytes** | **flows** | **packets**} [**ascending** | **descending**]] [**match** *match-field match-value*]}]

Cisco IOS Releases 12.4(4)T and 12.4(6)

show ip flow top {*number* [**from-cache main**] **aggregate** *aggregate-field* [**sorted-by** {**aggregate** | **bytes** | **flows** | **packets**} [**ascending** | **descending**]] [**match** *match-field match-value*]}]

show ip flow top-talkers [**verbose**]

Cisco IOS Releases Prior to 12.4(4)T

show ip flow top-talkers [**verbose**]

Syntax Description

Cisco IOS Releases Prior to 12.4(9)T Syntax	
verbose	(Optional) Displays additional details for the unaggregated top flows.
Cisco IOS Releases 12.4(9)T and Newer Syntax	
verbose	(Optional) Displays additional details for the unaggregated top flows.
number	(Optional) Specifies the number of top talkers to show in the display. The range is 1 to 100.
from-cache	(Optional) Specifies the cache that the display output is generated from.
main	Display output is generated from the main cache.
aggregate *aggregate-field*	(Optional) The combination of the **aggregate** and the *aggregate-field* keywords and arguments specifies which field to aggregate for the display output. See Table 30.
sorted-by	(Optional) Specifies which field to sort by. If this keyword is specified, you must select one of the following keywords: • **aggregate**—Sort by the aggregated field in the display data. • **bytes**—Sort by the number of bytes in the display data. • **flows**—Sort by the number of flows in the display data. • **packets**—Sort by number of packets in the display data.
ascending	(Optional) Arranges the display output in ascending order.
descending	(Optional) Arranges the display output in descending order.
match *match-field match-value*	(Optional) The combination of the **match**, *match-field*, and *match-value* keywords and arguments specifies the field from the flows – and the value in the field – to match. See Table 31.

Defaults

The **show ip flow top-talkers** *number* command string displays output in descending order based on the value in the **sorted-by** field.

The **show ip flow top-talkers** *number* command string displays data from the main NetFlow cache.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
Original version of the show ip flow top-talkers command (unaggregated top flows)	
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This feature was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
Original version of the show ip flow top command (aggregated top talkers)	
12.4(4)T	This command was introduced.
Merged show ip flow top-talkers and show ip flow top commands	
12.4(9)T	The **show ip flow top** command was merged into the **show ip flow top-talkers** command.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

You must have NetFlow configured before you can use the **show ip flow top-talkers** command.

The **show ip flow top-talkers** command can be used to display statistics for unaggregated top flows or aggregated top talkers. Prior to Cisco IOS release 12.4(9)T the **show ip flow top-talkers** command could only be used to display statistics for unaggregated top flows. In Cisco IOS release 12.4(9)T and newer releases, the **show ip flow top-talkers** command can be used to display statistics for both unaggregated top flows and aggregated top talkers.

Refer to the following sections for more information on using either of these methods:

- Unaggregated Top Flows—All Cisco IOS Releases Prior to 12.4(9)T, page 168
- Aggregated Top Talkers—Cisco IOS Releases 12.4(9)T and Newer, page 169

Unaggregated Top Flows—All Cisco IOS Releases Prior to 12.4(9)T

When you use the **show ip flow top-talkers** command in releases prior to Cisco IOS release 12.4(9)T, the display output shows only separate (unaggregated) statistics for the number of top flows that you specified with the **top** command.

Note The **sort-by** and **top** commands must be configured before you enter the **show ip flow top-talkers** [**verbose**] command. Optionally, the **match** command can be configured to specify additional matching criteria. Refer to the configuration documentation for the "NetFlow MIB and Top Talkers" feature for more information on using the **top**, **sort-by**, and **match** commands.

This method of viewing flow statistics is useful for identifying the unique flows that are responsible for the highest traffic utilization in your network. For example, if you have a centralized WEB server farm and you want to see statistics for the top 50 flows between your servers and your users regardless of the network protocol or application in use, you can configure **top** *50* and use the **show ip flow top-talkers verbose** command to view the statistics from the 50 top flows.

Tip If you want to limit the flows that are displayed to specific protocols or IP addresses, you can configure match criteria with the **match** command.

Displaying information on individual top flows will not provide you with a true map of your network utilization when the highest volume application or protocol traffic on your network is being generated by a large number of users who are sending small amounts of traffic. For example, if you configure **top** *10* and there are ten or more users generating more FTP traffic than any other type of traffic in your network, you will see the FTP traffic as the top flows even though there might be 10,000 users using HTTP to access web sites at much lower individual levels of network utilization that account for a much larger aggregated traffic volume. In this situation you need to aggregate the traffic patterns across flows using the **show ip flow top-talkers** [*number*] command string as explained in the "Aggregated Top Talkers—Cisco IOS Releases 12.4(9)T and Newer" section on page 169 instead.

The timeout period as specified by the **cache-timeout** command does not start until the **show ip flow top-talkers** command is entered. From that time, the same top talkers are displayed until the timeout period expires. To recalculate a new list of top talkers before the timeout period expires, you can change the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers** command.

A long timeout period for the **cache-timeout** command limits the system resources that are used by the NetFlow MIB and Top Talkers feature. However, the list of top talkers is calculated only once during the timeout period. If a request to display the top talkers is made more than once during the timeout period, the same results are displayed for each request, and the list of top talkers is not recalculated until the timeout period expires.

A short timeout period ensures that the latest list of top talkers is retrieved; however too short a period can have undesired effects:

- 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.
- The list of top talkers is updated every time the top talkers information is requested, possibly causing unnecessary usage of system resources.

A good method to ensure that the latest information is displayed, while also conserving system resources, is to configure a large value for the timeout period, but cause the list of top talkers to be recalculated by changing the parameters of the **cache-timeout**, **top**, or **sort-by** command prior to entering the **show ip flow top-talkers** command to display the top talkers. Changing the parameters of the **cache-timeout**, **top**, or **sort-by** command causes the list of top talkers to be recalculated upon receipt of the next command line interface (CLI) or MIB request.

Aggregated Top Talkers—Cisco IOS Releases 12.4(9)T and Newer

The **show ip flow top** command was merged with the **show ip flow top-talkers** command in Cisco IOS release 12.4(9)T. The two commands were merged to make it easier for you to display cache information on either unaggregated top flows, or aggregated top talkers, using the same root command.

The CLI help for the **show ip flow top-talkers** command was modified to help you differentiate between the two command formats.

```
Router# show ip flow top-talkers ?
Display aggregated top talkers:
  <1-100>  Number of aggregated top talkers to show

Display unaggregated top flows:
  verbose  Display extra information about unaggregated top flows
  |        Output modifiers
  <cr>

Router#
```

When you use the **show ip flow top-talkers** [*number*] command the display output will consist of aggregated statistics from the flows (aggregated top talkers) for the number of top talkers that you specified with the *number* argument.

Unlike the **show ip flow top-talkers** [**verbose**] command, the **show ip flow top-talkers** [*number*] command string does not require:

- Any pre-configuration of the router for the **show ip flow top-talkers** [*number*] command string itself. You can use the **show ip flow top-talkers** [*number*] command string immediately after enabling NetFlow on at least one interface in the router.
- Manipulating a cache timeout parameter to force a recalculation of the aggregated top talkers. The information in the display output of the **show ip flow top-talkers** [*number*] command string always contains the latest, most up-to-date information because it is not cached.

The arguments that are available with the **show ip flow top-talkers** [*number*] command enable you to quickly modify the criteria to be used for generating the display output. Refer to the configuration documentation for the "NetFlow Dynamic Top Talkers CLI" feature which is included in the Cisco IOS Release 12.4(4)T module "Detecting and Analyzing Network Threats With NetFlow", for additional information using the **show ip flow top-talkers** [*number*] command string.

For additional usage guidelines on displaying statistics for aggregated top talkers using the **show ip flow top-talkers** [*number*] command string, see the following sections:

- Top Traffic Flows
- Data Displayed by the show ip flow top command
- Top Talkers Display Output With Aggregation Only
- Top Talkers Display Output With Aggregation and Match Criteria
- Top Talkers Display Output in Ascending Order With Aggregation and Match Criteria
- Aggregate-field and Match-field Match-value Keywords, Arguments, and Descriptions

Top Traffic Flows

Using the **show ip flow top-talkers** command to display the aggregated statistics from the flows on a router for the highest volume applications and protocols in your network helps you identify, and classify, security problems such as a denial of service (DoS) attacks because DoS attack traffic almost always show up as one of the highest volume protocols in your network when a DoS attack is in progress. Displaying the aggregated statistics from the flows on a router is also useful for traffic engineering, diagnostics and troubleshooting.

Data Displayed by the show ip flow top command

The data in the display output from the **show ip flow top-talkers** command is not flow centric. You cannot identify individual flows with the **show ip flow top-talkers** command.

For example, when you use the **show ip flow top-talkers 5 aggregate destination-address** command:

- If you do not specify any match criteria, the aggregated statistics for the top five destination IP addresses from the flows on a router are displayed.

- If you specify match criteria, the aggregated statistics for the top five destination IP addresses that meet the match criteria that you specified is displayed.

Top Talkers Display Output With Aggregation Only

If you do not use any of the optional parameters the **show ip flow top-talkers** command displays the aggregated statistics from the flows on the router for the aggregation field that you enter. For example, to aggregate the flows based on the destination IP addresses, and display the top five destination IP addresses, you use the **show ip flow top-talkers 5 aggregate destination-address** command.

Top Talkers Display Output With Aggregation and Match Criteria

You can limit the display output by adding an optional match criterion. For example, to aggregate the statistics from the flows based on the destination IP addresses, and display the top five destination IP addresses that contain TCP traffic, you use the **show ip flow top-talkers 5 aggregate destination-address match protocol tcp** command.

Top Talkers Display Output in Ascending Order With Aggregation and Match Criteria

You can change the default sort order of the display output by using the **sorted-by** keyword. For example, to aggregate the statistics from the flows based on the destination IP addresses, and display the top five destination IP addresses that contain TCP traffic sorted on the aggregated field in ascending order, you use the **show ip flow top-talkers 5 aggregate destination-address sorted-by aggregate ascending match protocol tcp** command.

Tip This usage of the **show ip flow top-talkers 5 aggregate destination-address sorted-by aggregate ascending match protocol tcp** command string is useful for capacity planning because it shows the smallest flows first. The smallest flows indicate the minimum amount of capacity that you need to provide.

Aggregate-field and Match-field Match-value Keywords, Arguments, and Descriptions

Table 30 shows the keywords and descriptions for the *aggregate-field* argument of the **show ip flow top-talkers** *number* **aggregate** *aggregate-field* command. You must enter one of the keywords from this table.

Table 30 Keywords and Descriptions for aggregate-field Argument

Keyword	Description
bgp-nexthop	Flows that have the same value in the bgp-nexthop field are aggregated.
bytes	Flows that have the same number of bytes are aggregated.
destination-address	Flows that have the same value in the destination-address field are aggregated.
destination-as	Flows that have the same value in the destination-as field are aggregated.
destination-interface	Flows that have the same value in the destination-interface field are aggregated.
destination-port	Flows that have the same value in the destination-port field are aggregated.

Table 30 Keywords and Descriptions for aggregate-field Argument (continued)

Keyword	Description
destination-vlan	Flows that have the same value in the destination-vlan field are aggregated.
dscp	Flows that have the same value in the dscp field are aggregated.
fragment-offset	Flows that have the same value in the fragment-offset field are aggregated.
icmp	Flows that have the same value in the icmp-type and icmp code fields are aggregated.
icmp-code	Flows that have the same value in the icmp-code field are aggregated.
icmp-type	Flows that have the same value in the icmp-type field are aggregated.
incoming-mac	Flows that have the same value in the incoming-mac address field are aggregated.
ip-id	Flows that have the same value in the ip-id field are aggregated.
ip-nexthop-address	Flows that have the same value in the ip-nexthop-address field are aggregated.
max-packet-length	Flows that have the same value in the max-packet-length field are aggregated.
max-ttl	Flows that have the same value in the max-ttl field are aggregated.
min-packet-length	Flows that have the same value in the min-packet-length field are aggregated.
min-ttl	Flows that have the same value in the min-ttl field are aggregated.
outgoing-mac	Flows that have the same value in the outgoing-mac address field are aggregated.
packets	Flows that have the same number of packets are aggregated.
precedence	Flows that have the same value in the precedence field are aggregated.
protocol	Flows that have the same value in the protocol field are aggregated.
source-address	Flows that have the same value in the source-address field are aggregated.
source-as	Flows that have the same value in the source-as field are aggregated.
source-interface	Flows that have the same value in the source-interface field are aggregated.
source-port	Flows that have the same value in the source-port field are aggregated.

Table 30 Keywords and Descriptions for aggregate-field Argument (continued)

Keyword	Description
source-vlan	Flows that have the same value in the source-vlan field are aggregated.
tcp-flags	Flows that have the same value in the tcp-flags field are aggregated.
tos	Flows that have the same value in the tos field are aggregated.

Table 31 shows the keywords, arguments, and descriptions for the *match-field match-value* arguments for the **show ip flow top-talkers** *number* **aggregate** *aggregate-field* **match** *match-field match-value* command. These keywords are all optional.

Note In Table 31 the match criteria that you select must be available in the cache. For example, if you use the **show ip flow top 20 aggregate destination-address match destination-vlan 1** command, and you have not configured the **ip flow-capture vlan-id** command, the "% VLAN id is not available for this cache" error message is displayed.

Note In Table 31 the *match-field* is the keyword in the keyword column and the *match-value* is the argument(s) for the keyword. For example, for the keyword **bgp-nexthop**, **bgp-nexthop** is the *match-field* and [*ip-address* | *hostname*] is the *match-value*.

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-talkers** 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 0x00DC in the following excerpt 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-talkers** command.

```
R3# show ip cache verbose flow
.
.
.
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
0023 /0  0                     00DC /0  0     0.0.0.0                40   281.4
.
.
.
```

Table 31 Keywords, Arguments, and Descriptions for match-field match-value

Keyword	Description
bgp-nexthop {*ip-address* | *hostname*}	IP address or hostname of the BGP nexthop router to match in the flows.
bytes {[*bytes*] | [**min** *bytes*] [**max** *bytes*]}	Range of bytes to match in the flows. • **min**—Minimum number of bytes to match. • **max**—Maximum number of bytes to match. • Range: 0 to 4294967295 **Note** If you want to use **min** *bytes* you must enter it before **max** *bytes*.
destination-as *as-number*	Destination Autonomous System number to match in the flows. The range is 0 to 65535.
destination-interface *interface-type interface-number*	Destination interface to match in the flows.
destination-port {[*port*] | [**min** *port*] [**max** *port*]}	The range of destination ports to match in the flows. • **min**—Minimum port number to match. • **max**—Maximum port number to match. • Range: 0 to 65535 **Note** If you want to use **min** *port* you must enter it before **max** *port*.
destination-prefix *prefix/mask*	Destination IP address prefix and mask to match in the flows. **Note** Enter the prefix-mask by using the CIDR method of /number-of-bits. For example, 192.0.0.0/8.
destination-vlan *vlan-id*	Destination VLAN ID to match in the flows. • Range: 0 to 4095
dscp *dscp*	Value in the DSCP field to match in the flows. • Range: 0x0 to 0x3F
flows {[*flows*] | [**min** *flows*] [**max** *flows*]}	The range of flows in the aggregated data to match in the flows. • **min**—Minimum number of flows to match. • **max**—Maximum number of flows to match. • Range: 0 to 4294967295 **Note** If you want to use **min** *flows* you must enter it before **max** *flows*.
fragment-offset *fragment-offset*	Value in the fragment offset field to match in the flows. • Range: 0 to 8191

Table 31 Keywords, Arguments, and Descriptions for match-field match-value (continued)

Keyword	Description
icmp type *type* **code** *code*	ICMP type and code values to match in the flows. • Range for *type* and *code*: 0 to 255.
icmp-code *code*	ICMP code value to match in the flows. • Range: 0 to 255
icmp-type *type*	ICMP type value to match in the flows. • Range: 0 to 255
incoming-mac *mac-address*	Incoming MAC address to match in the flows.
ip-id *ip-id*	IP ID value to match in the flows. • Range: 0 to 65535
ip-nexthop-prefix *prefix/mask*	IP nexthop address prefix and mask to match in the flows. **Note** Enter the prefix-mask by using the CIDR method of /number-of-bits. For example, 192.0.0.0/8.
max-packet-length {[*max-packet-length*] | [**min** *max-packet-length*] [**max** *max-packet-length*]}	The range of maximum packet length values to match in the flows. • **min**—Minimum value in the maximum packet length field to match. • **max**—Maximum value in the maximum packet length field to match. • Range: 0 to 65535 **Note** If you want to use **min** *max-packet-length* you must enter it before **max** *max-packet-length*.
max-ttl {[*max-ttl*] | [**min** *max-ttl*] [**max** *max-ttl*]}	The range of maximum TTL values to match in the flows. • **min**—Minimum value in the maximum TTL field to match. • **max**—Maximum value in the maximum TTL field to match. • Range: 0 to 255 **Note** If you want to use **min** *max-ttl* you must enter it before **max** *max-ttl*.

Table 31 Keywords, Arguments, and Descriptions for match-field match-value (continued)

Keyword	Description
min-packet-length {[*min-packet-length*] | [**min** *min-packet-length*] [**max** *min-packet-length*]}	The range of minimum packet length values to match in the flows. • **min**—Minimum value in the minimum packet length field to match. • **max**—Maximum value in the minimum packet length field to match. • Range: 0 to 65535 **Note** If you want to use **min** *min-packet-length* you must enter it before **max** *min-packet-length*.
min-ttl {[*min-ttl*] | [**min** *min-ttl*] [**max** *min-ttl*]}	The range of minimum TTL values to match in the flows. • **min**—Minimum value in the minimum TTL field to match. • **max**—Maximum value in the minimum TTL field to match. • Range: 0 to 255 **Note** If you want to use **min** *min-ttl* you must enter it before **max** *min-ttl*.
outgoing-mac *mac-address*	Outgoing MAC address to match in the flows.
packets {[*packet-size*] | [**min** *packet-size*] [**max** *packet-size*]}	The range of packet sizes to match in the flows. • **min**—Minimum size of packets to match. • **max**—Maximum size of packets to match. • Range: 0 to 4294967295 **Note** If you want to use **min** *packet-size* you must enter it before **max** *packet-size*.
precedence *precedence*	Precedence value to match in the flows. • Range: 0 to 7
protocol {[*protocol-number*] | [**tcp** | **udp** | **icmp** | **igmp** | **ip-in-ip** | **gre** | i**pv6-in-ipv6**]}	Protocol value to match in the flows. • Range: 0 to 255 **Note** TCP, UDP, ICMP, IGMP, IP-in-IP, GRE, and IPv6-in-IPv6 are the protocols that NetFlow tracks for the protocols summary in the display output of the **show ip cache verbose flow** command. Other protocols can be matched by specifying their numeric values.
source-as *source-as*	Source autonomous system value to match in the flows. • Range: 0 to 65535

Table 31 Keywords, Arguments, and Descriptions for match-field match-value (continued)

Keyword	Description
source-interface *interface-type interface-number*	Source interface to match in the flows.
source-port {[*port*] | [[**min** *port*] [**max** *port*]]}	The range of source port values to match in the flows. • **min**—Source port value to match. • **max**—Source port value to match. • Range: 0 to 65535 **Note** If you want to use **min** *port* you must enter it before **max** *port*.
source-prefix *prefix/mask*	Source address prefix and mask to match in the flows. **Note** Enter the prefix-mask by using the CIDR method of /number-of-bits. For example, 192.0.0.0/8.
source-vlan *vlan-id*	Source VLAN ID to match in the flows. • Range: 0 to 4095
tcp-flags *flag*	Value in the TCP flag field to match in the flows. • Range: 0x0 to 0xFF
tos *tos*	Value in the TOS flag field to match in the flows. • Range: 0x0 to 0xFF

The Order That Aggregation Occurs in

With the exception of the **flows** keyword in Table 31, all matches made with the *match-field match-value* arguments are performed prior to aggregation, and only matching flows are aggregated. For example, the **show ip flow top-talkers** *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 flows** *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 are flows in the cache that include 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-talkers 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 20 flows matched. For example, if your router has 20 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-talkers 10 aggregate destination-address match destination-prefix** *224.0.0.0/3* command, the display will indicate that 1 of 20 flows matched.

If the total number of top talkers is less than the number of top talkers that were requested in the command, the available 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-talkers** command, the display output will indicate "N of M flows matched" where N is the number of matched flows, M is the total number of flows seen, and N is less than or equal to M. 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 expired from the cache and new flows were created, as the top talkers feature scans through the cache. Therefore, M is NOT the total number of flows in the cache, but rather, the number of flows observed in the cache by the top talkers feature.

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 source-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.

TCP-Flags

If you want to use the **tcp-flags** *flag* match criteria you must enter the hexadecimal values for the type of TCP flag that you want to match.

The TCP flags as used in the **tcp-flags** *flag* match criteria are provided in Table 32.

Table 32 Values for the tcp-flags flag match criteria

Hexadecimal Value	Field Name
0x01	FIN–Finish; end of session
0x02	SYN–Synchronize; indicates request to start session
0x04	RST–Reset; drop a connection
0x08	PUSH–Push; packet is sent immediately
0x10	ACK–Acknowledgement
0x20	URG–Urgent
0x40	ECE–Explicit Congestion Notification Echo
0x80	CWR–Congestion Window Reduced

For more information on TCP and TCP flags, refer to RFC 3168 at the following URL: http://www.ietf.org/rfc/rfc3168.txt.

Examples

The **show ip flow top-talkers** command can be used to display information for unaggregated top flows or aggregated top talkers. Refer to the following sections for examples on using either of these methods:

- Examples for Unaggregated Top Flows—All Cisco IOS releases that Support the NetFlow MIB and Top Talkers Feature, page 179
- Examples for Aggregated Top Talkers—All Cisco IOS releases that Support the NetFlow Dynamic Top Talkers CLI Feature, page 180

Examples for Unaggregated Top Flows—All Cisco IOS releases that Support the NetFlow MIB and Top Talkers Feature

The following example shows the output of the **show ip flow top-talkers** command.

In the example, the NetFlow MIB and Top Talkers feature has been configured to allow a maximum of five top talkers to be viewed. The display output is configured to be sorted by the total number of bytes in each top talker, and the list of top talkers is configured to be retained for 2 seconds (2000 milliseconds).

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 5
Router(config-flow-top-talkers)# sort-by bytes
Router(config-flow-top-talkers)# cache-timeout 2000

Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   144K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   144K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   135K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   125K
Et0/0.1       10.92.231.235   Et1/0.1       172.16.10.2     06 0041 0041   115K
5 of 5 top talkers shown. 11 flows processed
```

Table 33 describes the significant fields shown in the display.

Table 33 show ip flow top-talkers Field Descriptions

Field	Description
SrcIf	Source interface
SrcIPaddress	Source IP address
DstIf	Destination interface
DstIPaddress	Destination IP address
Pr	Protocol number
SrcP	Source port
DstP	Destination port
Bytes	Total number of bytes in each top talker
X of Y top talkers shown	Y–The number of Top Talkers specified by the **top** command. X–The number of flows displayed. The value for “X” is always <= the value for “Y”. For example, if “Y” = 5 and there are 3 Top Talkers, the display will show 3 of 5 top talkers shown.
flows processed	The number of flows observed in the NetFlow cache.

Table 34 shows messages that could be received in response to the **show ip flow top-talkers** command and their explanations.

Table 34 show ip flow top-talkers Message Descriptions

Message	Description
% Top talkers not configured	The NetFlow MIB and Top Talkers feature has not yet been configured.
% Cache is not enabled	The cache is not enabled
% Cache is empty	There are no flows in the cache to be viewed.
% There are no matching flows to show	The match criteria that were specified do not match any flows in the cache.

Examples for Aggregated Top Talkers—All Cisco IOS releases that Support the NetFlow Dynamic Top Talkers CLI Feature

The following example looks for up to 10 top talkers, aggregates them on the protocol type, sorts them by the number of packets in the flows, and displays the output in descending order:

```
Router# show ip flow top-talkers 10 aggregate protocol sorted-by packets descending

There are 3 top talkers:

IPV4 PROT       bytes        pkts       flows
=========  ==========  ==========  ==========
        1  2009729203     1455464          11
        6    33209300       30690          19
       17          92           1           1


31 of 31 flows matched.
```

Things to note in this display output:

- All 31 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 that is aggregated into the first flow is ICMP traffic (IP protocol type 1). This might indicate an ICMP DoS attack is in progress.

Table 35 describes the significant fields shown in the display.

Table 35 show ip flow top-talkers 10 aggregate protocol sorted-by packets descending Field Descriptions

Field	Description
There are top X talkers	The number of top talkers (X) is displayed.
IPV4 PROT [1]	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.
X of Y flows matched.	Y–Number of flows seen in the cache. X–Number of flows in the cache that matched the criteria you specified.

1. IPV4 is shown in upper-case (capital) letters because it is the field that the display is aggregated on. In this example this is the keyword **protocol** in the **show ip flow top-talkers 10 aggregate protocol sorted-by packets descending** command.

The following example looks for up to five top talkers, aggregates them on the source IP address, sorts them in descending order by the numbers of packets, matches on the ICMP type value of 8, and displays the output in descending order:

```
Router# show ip flow top-talkers 5 aggregate source-address sorted-by packets descending
match icmp-type 8

There are 3 top talkers:

IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
192.168.87.200     23679120       16501           1
10.234.53.1        18849000       12566           1
172.30.231.193     12094620        8778           1


3 of 29 flows matched.
```

The following example looks for up to five top talkers, aggregates them on the destination IP address, sorts them in descending order by the numbers of packets, matches on the ICMP type value of 8, and displays the output in descending order:

```
Router# show ip flow top-talkers 5 aggregate destination-address sorted-by packets
descending match icmp-type 8

There are 2 top talkers:

IPV4 DST-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
172.16.1.2         32104500       21403           2
172.16.10.2         2128620        2134           1

3 of 32 flows matched.
```

Table 36 describes the significant fields shown in the display.

Table 36 show ip flow top-talkers 5 aggregate {source-address | destination-address} sorted-by packets descending match icmp-type 8 Field Descriptions

Field	Description
There are top X talkers	The number of top talkers (X) is displayed.
IPV4 SRC-ADDR [1]	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 IPv4 traffic in the flows based on the source IPv4 IP address. In this example there are 3 IP source addresses in the flows: • 192.168.87.200 • 10.234.53.1 • 172.30.231.193
IPV4 DST-ADDR [2]	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 IPv4 traffic in the flows based on the destination IPv4 IP address. In this example there are 2 IP destination addresses in the flows: • 172.16.1.2 • 172.16.10.2
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.
X of Y flows matched.	Y–Number of flows seen in the cache. X–Number of flows in the cache that matched the criteria you specified.

1. IPV4 SRC-ADDR is shown in upper-case (capital) letters because it is the field that the display is aggregated on. In this example this is the keyword **source-address** in the **show ip flow top-talkers 5 aggregate source-address sorted-by packets descending match icmp-type 8** command.

2. IPV4 DST-ADDR is shown in upper-case (capital) letters because it is the field that the display is aggregated on. In this example this is the keyword **destination-address** in the **show ip flow top-talkers 5 aggregate destination-address sorted-by packets descending match icmp-type 8** command.

The following example looks for up to five top talkers, aggregates them on the source IP address, sorts them in descending order by the number of bytes in the flow, matches on the port range of 20 to 21 (FTP Data and control ports, respectively), and displays the output in descending order:

```
Router# show ip flow top-talkers 5 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           920          23           2
10.10.12.1               480          12           2
10.251.138.218           400          10           2
10.132.221.111           400          10           2
10.71.200.138            280           7           1


9 of 34 flows matched.
```

Tip You can enter the port numbers in their decimal values as shown (20 and 21), or in their hexadecimal equivalents of 0x14 and 0x15.

Table 37 describes the significant fields shown in the display.

Table 37 show ip flow top-talkers 5 aggregate source-address sorted-by packets descending match icmp-type 8 Field Descriptions

Field	Description
There are top X talkers	The number of top talkers (X) is displayed.
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 IPv4 traffic in the flows based on the source IPv4 IP address. In this example there are 5 IP source addresses in the flows: • 10.231.185.254 • 10.10.12.1 • 10.251.138.218 • 10.132.221.111 • 10.71.200.138
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.

Table 37 show ip flow top-talkers 5 aggregate source-address sorted-by packets descending match icmp-type 8 Field Descriptions (continued)

Field	Description
flows	Displays the numbers of aggregated flows for each top talker.
X of Y flows matched.	Y–Number of flows seen in the cache. X–Number of flows in the cache that matched the criteria you specified.

The following example looks for up to five top talkers, aggregates them on the source IP address, sorts them in descending order by the aggregated field (source IP address), and displays the output in descending order:

```
Router# show ip flow top-talkers 5 aggregate source-address sorted-by aggregate descending

There are 5 top talkers:

IPV4 SRC-ADDR         bytes        pkts       flows
===============  ==========  ==========  ==========
172.16.1.85           97360        2434           2
172.16.1.84           97320        2433           2
10.251.138.218        34048        1216           1
10.231.185.254        34048        1216           1
10.132.221.111        34076        1217           1


7 of 18 flows matched.
```

Table 38 describes the significant fields shown in the display.

Table 38 show ip flow top-talkers 5 aggregate source-address sorted-by aggregate descending Field Descriptions

Field	Description
There are top X talkers	The number of top talkers (X) is displayed.
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 IPv4 traffic in the flows based on the source IPv4 IP address. In this example there are 5 IP source addresses in the flows: • 172.16.1.85 • 172.16.1.84 • 10.251.138.218 • 10.231.185.254 • 10.132.221.111
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.

Table 38 show ip flow top-talkers 5 aggregate source-address sorted-by aggregate descending Field Descriptions (continued)

Field	Description
flows	Displays the numbers of aggregated flows for each top talker.
X of Y flows matched.	Y–Number of flows seen in the cache. X–Number of flows in the cache that matched the criteria you specified.

Related Commands

Command	Description
cache-timeout	Specifies the length of time for which the list of top talkers (heaviest traffic patterns and most-used applications in the network) for the NetFlow MIB and Top Talkers feature is retained.
ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and Top Talkers (heaviest traffic patterns and most-used applications in the network) feature.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and Top Talkers (heaviest traffic patterns and most-used applications in the network) feature.
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and Top Talkers feature.
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and Top Talkers feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.

show mls ip non-static

To display information for the software-installed nonstatic entries, use the **show mls ip non-static** command in user EXEC or privileged in the EXEC mode.

show mls ip non-static [**count** [**module** *number*] | **detail** [**module** *number*] | **module** *number*]

Syntax Description

count	(Optional) Displays the total number of nonstatic entries.
module *number*	(Optional) Designates the module number.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip** command.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the software-installed nonstatic entries:

```
Router> show mls ip non-static

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed nonstatic entries:

```
Router> show mls ip non-static detail

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
Router>
```

This example shows how to display the total number of software-installed nonstatic entries:

```
Router> show mls ip non-static count

Displaying Netflow entries in Supervisor Earl

 Number of shortcuts = 0
Router>
```

show mls ip routes

To display the NetFlow routing entries, use the **show mls ip routes** command in user EXEC or privileged EXEC mode.

show mls ip routes [**non-static** | **static**] [**count** [**module** *number*] | **detail** [**module** *number*] | **module** *number*]

Syntax Description

non-static	(Optional) Displays the software-installed nonstatic entries.
static	(Optional) Displays the software-installed static entries.
count	(Optional) Displays the total number of NetFlow routing entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip sw-installed** command

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the software-installed nonstatic routing entries:

```
Router> show mls ip routes non-static

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed nonstatic routing entries:

```
Router> show mls ip routes non-static detail

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+-----------+

Router>
```

This example shows how to display the total number of software-installed routing entries:

```
Router> show mls ip routes count
Displaying Netflow entries in Supervisor Earl

 Number of shortcuts = 0
Router>
```

Related Commands

Command	Description
show mls netflow ip sw-installed	Displays information for the software-installed IP entries.

show mls ip static

To display the information for the software-installed static IP entries, use the **show mls ip static** command in user EXEC or privileged EXEC mode.

show mls ip static [**count** [**module** *number*] | **detail** [**module** *number*] | **module** *number*]

Syntax Description

count	(Optional) Displays the total number of static entries.
module *number*	(Optional) Designates the module number.
detail	(Optional) Specifies a detailed per-flow output.

Command Modes

User EXEC
Privileged ECEX

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command is supported on releases prior to Release 12.2(17a)SX only.
12.2(17b)SXA	This command is replaced by the **show mls netflow ip sw-installed** command.

Usage Guidelines

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the software-installed static entries:

```
Router> show mls ip static

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed static entries:

```
Router> show mls ip static detail

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
Router>
```

This example shows how to display the total number of software-installed static entries:

```
Router> show mls ip static count

Displaying Netflow entries in Supervisor Earl

 Number of shortcuts = 0
Router>
```

show mls nde

To display information about the NDE hardware-switched flow, use the **show mls nde** command in user EXEC or privileged EXEC mode.

show mls nde

Syntax Description

This command has no arguments or keywords.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(18)SXD	The output for Cisco 7600 series routers that are configured with a Supervisor Engine 720 was changed to include the current NDE mode.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The output for Cisco 7600 series routers that are configured with a Supervisor Engine 720 includes the current NDE mode.

Examples

Supervisor Engine 2 Examples

This example shows the output from Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This example shows how to display information about the NDE status on a Cisco 7600 series router that is configured with a Supervisor Engine 2:

```
Router# show mls nde
 Netflow Data Export is Enabled
Router#
```

Supervisor Engine 720 Examples

This example shows how to display information about the NDE hardware-switched flow on a Cisco 7600 series router that is configured with a Supervisor Engine 720:

```
Router# show mls nde
 Netflow Data Export enabled (Interface Mode)
 Exporting flows to 172.20.55.71 (9991)
 Exporting flows from 10.6.60.120 (59020)
 Version: 7
```

```
 Include Filter not configured
 Exclude Filter not configured
 Total Netflow Data Export Packets are:
    0 packets, 0 no packets, 0 records
Router#
```

Related Commands

Command	Description
mls nde sender	Enables MLS NDE export.
show ip flow-export	Displays the information about the hardware-switched and software-switched flows for the data export, including the main cache and all other enabled caches.
show mls netflow	Displays configuration information about the NetFlow hardware.

show mls netflow

To display configuration information about the NetFlow hardware, use the **show mls netflow** command in user EXEC or privileged EXEC mode.

show mls netflow {**aging** | **aggregation flowmask** | **creation** | **flowmask** | {**table-contention** {**detailed** | **summary**}}}

show mls netflow [**ip** | **ipv6** | **mpls**] [**any** | **count** | **destination** {*hostname* | *ip-address*} | **detail** | **dynamic** | **flow** {**tcp** | **udp**} | **module** *number* | **nowrap** | **source** {*hostname* | *ip-address*} | **sw-installed** [**non-static** | **static**]]

Syntax Description

aging	Displays the NetFlow-aging information.
aggregation flowmask	Displays the flow mask that is set for the current NetFlow aggregations.
creation	Displays the configured protocol-creation filters.
flowmask	Displays the current NetFlow IP and IPX flow mask.
table-contention	Displays the NetFlow table-contention level information.
detailed	Displays detailed NetFlow table-contention level information.
summary	Displays a summary of NetFlow table-contention levels.
ip	(Optional) Displays information about the NetFlow IP table; see the **show mls netflow ip** command.
ipv6	(Optional) Displays information about the NetFlow IPv6 table; see the **show mls netflow ipv6** command.
mpls	(Optional) Displays information about the NetFlow MPLS table.
any	(Optional) Displays detailed NetFlow table-entry information with no test wrap.
count	(Optional) Displays the total number of MLS NetFlow IP entries.
destination *hostname*	(Optional) Displays the entries for a specific destination hostname.
destination *ip-address*	(Optional) Displays the entries for a specific destination IP address.
detail	(Optional) Specifies a detailed output.
dynamic	(Optional) Displays the hardware-created dynamic entries; see the **show mls netflow ip dynamic** command.
flow tcp	(Optional) Displays information about the TCP flows.
flow udp	(Optional) Displays information about the UDP flows.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
nowrap	(Optional) Displays information without text wrap.
source *hostname*	(Optional) Displays the entries for a specific source address.
source *ip-address*	(Optional) Displays the entries for a specific source IP address.
sw-installed	(Optional) Displays the routing NetFlow entries; see the **show mls netflow ip sw-installed** command.

non-static	(Optional) Displays information for software-installed static IP entries; see the **show mls netflow ip sw-installed** command.
static	(Optional) Displays information for the software-installed nonstatic IP entries; see the **show mls netflow ip sw-installed** command.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed as follows: • Enhanced the **show mls netflow aggregation flowmask** command output to include a list of aggregation caches with minimum flow mask and NetFlow-aggregation schemes such as destination-prefix, source-prefix, protocol-port, and prefix. • Included support for the **ipv6** option.
12.2(17b)SXA	This command was changed to add the following keywords and arguments: • **details** • **nowrap** • **module** *num* • Changed the syntax from **show mls** [**ip** | **ipv6** | **mpls**] to **show mls netflow** [**ip** | **ipv6** | **mpls**].
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX train.
12.2(18)SXD	This command was changed to support the **creation** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Note The **creation** keyword is not supported in releases prior to Release 12.2(18)SXD.

The **ipv6**, and **mpls** keywords are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

The **interface**, **macd**, and **macs** keywords are not supported.

If you enter the **show mls netflow ip** command with no argument, the output of the **show mls netflow ip routes** and **show mls netflow ip dynamic** commands are displayed.

When you view the output, note that a colon (:) is used to separate the fields.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module that are used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module that is installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. These valid values also apply when entering the **module** *number* keyword and argument.

Examples

This example shows how to display the NetFlow-aging configuration:

```
Router# show mls netflow aging
             enable timeout  packet threshold
             ------ -------  ----------------
normal aging true       300        N/A
fast aging   true       32         100
long aging   true       900        N/A
Router#
```

This example shows how to display the configured protocol-creation filters:

```
Router# show mls netflow creation
Excluded protocols:
port protocol
-------+----------
10     tcp
8      udp/tcp
Router#
```

Supervisor Engine 720 Examples

These examples show the output from Cisco 7600 series routers that are configured with a Supervisor Engine 720.

This example shows how to display the flow mask that is set for the current NetFlow aggregation:

```
Router# show mls netflow aggregation flowmask
Current flowmask set for netflow aggregation : Dest only
Minimum flowmask required for netflow aggregation schemes
----------------------+------------------+-----------------
Aggregation Scheme Min. Flowmask Status
----------------------+------------------+-----------------
as Intf Src Dest disabled
protocol-port Full Flow disabled
source-prefix Intf Src Dest disabled
destination-prefix Dest only enabled
prefix Intf Src Dest disabled
Router#
```

This example shows how to display detailed information about the NetFlow table-contention level:

```
Router# show mls netflow table-contention detailed
Earl in Module 2
Detailed Netflow CAM (TCAM and ICAM) Utilization
================================================
TCAM Utilization   :     0%
ICAM Utilization   :     0%
Netflow TCAM count :     0
Netflow ICAM count :     0
Router#
```

This example shows how to display a summary of the NetFlow table-contention level:

```
Router# show mls netflow table summary
Earl in Module 2
Summary of Netflow CAM Utilization (as a percentage)
================================================
TCAM Utilization   :     0%
ICAM Utilization   :     0%
Router#
```

Supervisor Engine 2 Examples

These examples show the output from Cisco 7600 series routers that are configured with a Supervisor Engine 2.

This example shows how to display the flow mask that is set for the current NetFlow aggregations:

```
Router# show mls netflow aggregation flowmask
Current flowmask set for netflow aggregation : interface and full flow
Minimum flowmask required for netflow aggregation schemes
---------------------+------------------+-----------------
Aggregation Scheme Min. Flowmask Status
---------------------+------------------+-----------------
as if-dst-src enabled
protocol-port full enabled
source-prefix if-dst-src enabled
destination-prefix dst enabled
prefix if-dst-src enabled
Router#
```

This example shows how to display detailed information about the NetFlow table-contention level:

```
Router# show mls netflow table-contention detailed
Earl in Module 1
Detailed Table Contention Level Information
==========================================
Layer 3
-------
L3 Contention Level:     0
Page Hits Requiring 1 Lookup    =        0
Page Hits Requiring 2 Lookups   =        0
Page Hits Requiring 3 Lookups   =        0
Page Hits Requiring 4 Lookups   =        0
Page Hits Requiring 5 Lookups   =        0
Page Hits Requiring 6 Lookups   =        0
Page Hits Requiring 7 Lookups   =        0
Page Hits Requiring 8 Lookups   =        0
Page Misses                     =        0
Router#
```

This example shows how to display a summary of the NetFlow table-contention level:

```
Router# show mls netflow table summary
Earl in Module 1
Summary of Table Contention Levels (on a scale of 0 (lowest) to 5 (highest))
================================================================================
L3 Contention Level: 0
Router#
```

Related Commands

Command	Description
ip flow-aggregation cache	Creates a flow-aggregation cache and enters the aggregation cache configuration mode.
mls netflow usage notify	Monitors the NetFlow table usage on the switch processor and the DFCs.
show ip cache flow	Displays a summary of the NetFlow cache-flow entries.

show mls netflow ip

To display information about MLS NetFlow IP traffic, use the **show mls netflow ip** command in user EXEC or privileged EXEC mode.

show mls netflow ip any

show mls netflow ip count [**module** *number*]

show mls netflow ip destination {*hostname* | *ip-address*}[*/ip-mask*] [**count** [**module** *number*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **source** {*hostname* | *ip-address*}[*/ip-mask*] | **sw-installed** [**non-static** | **static**]]

show mls netflow ip detail [**module** *number* | **nowrap** [**module** *number*]]

show mls netflow ip dynamic [**count** [**module** *number*]] [**detail**] [**module** *number*] [**nowrap** [**module** *number*] [**qos** [**module** *number*]] [**nowrap** [**module** *number*]]]

show mls netflow ip flow {**icmp** | **tcp** | **udp**} [**count** [**module** *number*] | **destination** {*hostname* | *ip-address*}[*/ip-mask*] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **source** {*hostname* | *ip-address*} | s**w-installed** [**non-static** | **static**]]

show mls netflow ip module *number*

show mls netflow ip qos [**module** *number* | **nowrap** [**module** *number*]]

show mls netflow ip source {*hostname* | *ip-address*}[*/ip-mask*] [**count** [**module** *number*]] | **detail** | **dynamic** | **flow** {**icmp** | **tcp** | **udp**} | **module** *number* | **nowrap** | **qos** | **sw-installed** [**non-static** | **static**]

Syntax Description

any	Displays detailed NetFlow table-entry information with no test wrap.
count	Displays the total number of MLS NetFlow IP entries.
destination *hostname*	Displays the entries for a specific destination hostname.
destination *ip-address*	Displays the entries for a specific destination IP address.
detail	(Optional) Specifies a detailed output.
dynamic	Displays the hardware-created dynamic entries; see the **show mls netflow ip dynamic** command.
flow icmp	Displays information about the ICMP flows.
flow tcp	Displays information about the TCP flows.
flow udp	Displays information about the UDP flows.
/ip-mask	Masks the IP address.
module *number*	Displays the entries on the specified module; see the "Usage Guidelines" section for valid values.
nowrap	Displays information without text wrap.
qos	Displays QoS microflow policing information.
source *hostname*	Displays the entries for a specific source address.

source *ip-address*	Displays the entries for a specific source IP address.
sw-installed	(Optional) Displays the routing NetFlow entries; see the **show mls netflow ip sw-installed** command.
non-static	(Optional) Displays information for software-installed static IP entries; see the **show mls netflow ip sw-installed** command.
static	(Optional) Displays information for the software-installed nonstatic IP entries; see the **show mls netflow ip sw-installed** command.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed as follows: • Enhanced the **show mls netflow aggregation flowmask** command output to include a list of aggregation caches with minimum flow mask and NetFlow-aggregation schemes such as destination-prefix, source-prefix, protocol-port, and prefix. • Included support for the **ipv6** option.
12.2(17b)SXA	Changed the syntax from **show mls** [**ip** | **ipv6** | **mpls**] to **show mls netflow** [**ip** | **ipv6** | **mpls**] and added the **nowrap** keyword.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.
12.2(18)SXD	This command was changed to include the following keywords: • The **icmp** keyword to display information about ICMP flows. • The **qos** keyword to display QoS microflow policing information.
12.2(18)SXF	This command was changed to remove support for the **any** keyword.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(33)SRB	This command was modified to show the VPN name and VPN ID in the display output. In addition, the command was modified to support per-interface NetFlow.

Usage Guidelines

If you enter the **show mls netflow ip** command with no arguments, the output of the **show mls netflow ip sw-installed** and **show mls netflow ip dynamic** commands are displayed.

When you view the output, note that a colon (:) is used to separate the fields.

The **multicast** keyword appears on systems that are not configured with a Supervisor Engine 720.

In Cisco IOS Release 12.2SR and later, the NetFlow cache might contain null entries (with an IP source and destination address of 0.0.0.0). This behavior is the result of changes made to support per-interface NetFlow, which allows you to enable NetFlow for IPv4 traffic on individual interfaces. By default, the

hardware cache is populated with information about packets received on all IP interfaces. However, if NetFlow is not enabled on an IP interface, a null flowmask is used, which results in a null cache entry being created for the interface.

Examples

This example shows how to display information about any MLS NetFlow IP:

```
Router# show mls netflow ip

Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f:AdjPtr
------------------------------------------------------------------------------
Pkts Bytes Age LastSeen Attributes
--------------------------------------------------
10.1.1.2 11.1.1.2 tcp :3 :5 Fa5/11 :0x0
459983 21159218 6 07:45:13 L3 - Dynamic
10.1.1.2 11.1.1.3 tcp :3 :5 Fa5/11 :0x0
459984 21159264 6 07:45:13 L3 - Dynamic
Router#
```

This example shows how to display detailed NetFlow table-entry information:

```
Router# show mls netflow ip detail

Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f:AdjPtr
------------------------------------------------------------------
Pkts Bytes Age LastSeen Attributes
--------------------------------------------------
Mask Pi R CR Xt Prio Dsc IP_EN OP_EN Pattern Rpf FIN_RDT FIN/RST
----+--+-+--+--+----+---+-----+-----+-------+---+-------+-------
Ig/acli Ig/aclo Ig/qosi Ig/qoso Fpkt Gemini MC-hit Dirty Diags
-------+-------+-------+-------+----+------+------+-----+------
QoS Police Count Threshold Leak Drop Bucket Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
172.30.46.2 172.30.45.2 4 :0 :0 Gi7/1: 0x0
140063 6442898 15 01:42:52 L3 - Dynamic
1 1 0 0 1 0 0 1 1 0 0 0 0
0 0 0 0 0 0 0 0 0 0
0x0 672645504 0 0 NO 31784 NO NO
Router#
```

This example shows how to display NetFlow table-entry information with no test wrap:

```
Router# show mls netflow ip nowrap

 Displaying Netflow entries in Supervisor Earl
 DstIP SrcIP Prot:SrcPort:DstPort Src i/f
 :AdjPtr Pkts Bytes Age LastSeen Attributes
 ------------------------------------------------------------------------------
 -
 ------------------------------------------------------------------
 10.1.1.2 11.1.1.92 udp :63 :63 Fa5/11
 :0x0 176339 8111594 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.93 udp :63 :63 Fa5/11
 :0x0 176338 8111548 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.94 udp :63 :63 Fa5/11
 :0x0 176338 8111548 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.95 udp :63 :63 Fa5/11
 :0x0 176338 8111548 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.96 udp :63 :63 Fa5/11
 :0x0 176338 8111548 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.97 udp :63 :63 Fa5/11
```

```
 :0x0 176337 8111502 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.98 udp :63 :63 Fa5/11
 :0x0 176337 8111502 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.99 udp :63 :63 Fa5/11
 :0x0 176337 8111502 912 22:31:15 L3 - Dynamic
 10.1.1.2 11.1.1.100 udp :63 :63 Fa5/11
 :0x0 176337 8111502 912 22:31:15 L3 - Dynamic
Router#
```

This example shows how to display information about the MLS NetFlow on a specific interface:

```
Router# show mls netflow ip interface FastEthernet 3/1

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts          Bytes       Age   LastSeen  Attributes
-------------------------------------------------
172.20.52.19    0.0.0.0         0   :0      :0        0   : 0
0             0           1635  11:05:26   L3 - Dynamic
Router#
```

This example shows how to display information about the MLS NetFlow on a specific IP address:

```
Router# show mls netflow ip destination 172.20.52.122

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts          Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router#
```

This example shows how to display information about the MLS NetFlow on a specific flow:

```
Router# show mls netflow ip flow udp

Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts          Bytes       Age   LastSeen  Attributes
-------------------------------------------------
172.20.52.19    0.0.0.0         0   :0      :0        0   : 0
0             0           1407  11:01:32   L3 - Dynamic
Router#
```

This example shows how to display detailed information about the MLS NetFlow on a full-flow mask:

```
Router# show mls netflow ip detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts          Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
172.20.52.19    0.0.0.0         0   :0      :0        0   : 0
0             0           1464  11:02:31   L3 - Dynamic
  0x0           0               0        0       NO   64        NO       NO
Router#
```

This example shows how to display detailed information about a specific flow type:

```
Router# show mls netflow ip flow icmp

Displaying Netflow entries in Supervisor Earl
DstIP SrcIP Prot:SrcPort:DstPort Src i/f
:AdjPtr
>
>------------------------------------------------------------------------------
-
-
Pkts Bytes Age LastSeen Attributes
--------------------------------------------------
10.1.1.2 11.1.10.151 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
10.1.1.2 11.1.10.153 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
10.1.1.2 11.1.10.155 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
10.1.1.2 11.1.10.157 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
10.1.1.2 11.1.10.159 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
10.1.1.2 11.1.10.161 icmp:0 :0 Fa5/11
:0x0
1945 89470 1062 08:45:15 L3 - Dynamic
10.1.1.2 11.1.10.163 icmp:0 :0 Fa5/11
:0x0
Router#
```

This example shows how to display QoS information:

```
Router# show mls netflow ip qos

Displaying netflow qos information in Supervisor Earl
DstIP            SrcIP           Prot:SrcPort:DstPort Src i/f:AdjPtr
------------------------------------------------------------------------------
Pkts         Bytes        LastSeen   QoS   PoliceCount Threshold  Leak
------------------------------------------------------------------------------
Drop  Bucket
------------
xxx.xxxx.xxx.xxx xxx.xxx.xxx.xxx xxxx:63     :63      Fa5/11 :0x0
772357       35528422     17:59:01   xxx   xxx         xxx        xxx
xxx   xxx
Router#
```

This example shows how to display VPN information on a Cisco 7600 series router:

```
Router# show mls netflow ip module 5
Displaying Netflow entries in module 5
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f          :AdjPtr
------------------------------------------------------------------------------
Pkts         Bytes         Age   LastSeen  Attributes
----------------------------------------------
10.1.1.1        10.2.0.2        0   :0      :0        vpn:red          :0x0
504          398020        1     23:20:48   L3 - Dynamic
224.0.0.5       172.16.1.1      89  :0      :0        Fa1/1            :0x0
1            84            7     23:20:42   L2 - Dynamic
0.0.0.0         0.0.0.0         0   :0      :0        --               :0x0
2238         1582910       33    23:20:48   L3 - Dynamic
```

```
224.0.0.2       172.16.1.1      udp :646    :646      Fa1/1           :0x0
5           310           21    23:20:46   L2 - Dynamic
172.16.2.6      172.16.1.2      0   :0      :0        Fa1/1           :0x0
1           140           22    23:20:27   L2 - Dynamic

Router#
```

Related Commands

Command	Description
flow hardware mpls-vpn ip	Enables NetFlow to create and export hardware cache entries for traffic entering the router on the last MPLS hop of an IPv4 MPLS VPN network.
ip flow ingress	Enables (ingress) NetFlow accounting for traffic arriving on an interface.
mls flow ip	Configures the flow mask to use for NetFlow Data Export.
show mls netflow ip dynamic	Displays the statistics for NetFlow IP entries.
show mls netflow ip sw-installed	Displays information for the software-installed IP entries.
show mls netflow ip routes	Displays the NetFlow IP routing entries.

show mls netflow ip dynamic

To display the statistics for NetFlow IP entries, use the **show mls netflow ip dynamic** command in user EXEC or privileged EXEC mode.

show mls netflow ip dynamic [**count** [**module** *number*] | **detail** [**module** *number*] | **module** *number*]

Syntax Description

count	(Optional) Displays the total number of NetFlow entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
detail	(Optional) Specifies a detailed per-flow output.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command replaced the **show mls netflow ip statistics** command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

The **show mls netflow ip statistics** command is supported on releases prior to Release 12.2(17a)SX. For Release 12.2(17a)SX and later releases, use the **show mls netflow ip dynamic** command.

Examples

This example shows how to display the statistics for the NetFlow IP entries:

```
Router> show mls netflow ip dynamic
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display the statistics for the NetFlow IP entries:

```
Router> show mls netflow ip dynamic detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
Router>
```

Related Commands

Command	Description
show mls netflow ip	Displays information about MLS NetFlow IP traffic.
show mls netflow ip dynamic	Displays the statistics for NetFlow IP entries.
show mls netflow ip sw-installed	Displays information for the software-installed IP entries.
show mls netflow ip routes	Displays the NetFlow IP routing entries.

show mls netflow ip routes

To display the NetFlow IP routing entries, use the **show mls netflow ip routes** command in user EXEC or privileged EXEC mode.

show mls netflow ip routes [**non-static** | **static**] [**count** [**module** *number*] | **detail** [**module** *number*] | **module** *number*]

Syntax Description

non-static	(Optional) Displays the software-installed routing entries.
static	(Optional) Displays the software-installed static routing entries.
count	(Optional) Displays the total number of NetFlow IP routing entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
detail	(Optional) Specifies a detailed per-flow output.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17a)SX	This command was changed to the **show mls netflow ip sw-installed** command.

Usage Guidelines

The **show mls netflow ip routes** command is supported on releases prior to Release 12.2(17a)SX. For Release 12.2(17a)SX and later releases, use the **show mls netflow ip sw-installed** command.

This command is not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 2.

Examples

This example shows how to display the software-installed nonstatic routing entries:

```
Router> show mls netflow ip routes non-static
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
-----------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed nonstatic routing entries:

```
Router> show mls netflow ip routes non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+

Router>
```

This example shows how to display the total number of software-installed routing entries:

```
Router> show mls netflow ip routes count
Displaying Netflow entries in Supervisor Earl

 Number of shortcuts = 0
Router>
```

Related Commands

Command	Description
show mls netflow ip	Displays information about MLS NetFlow IP traffic.
show mls netflow ip dynamic	Displays the statistics for NetFlow IP entries.
show mls netflow ip sw-installed	Displays information for the software-installed IP entries.

show mls netflow ip sw-installed

To display information for the software-installed IP entries, use the **show mls netflow ip sw-installed** command in user EXEC or privileged EXEC mode.

show mls netflow ip sw-installed {**non-static** | **static**} [**count** [**module** *number*] | **detail** [**module** *number*] | **module** *number*]

Syntax Description

non-static	Displays the software-installed routing entries.
static	Displays the software-installed static routing entries.
count	(Optional) Displays the total number of nonstatic entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
detail	(Optional) Specifies a detailed per-flow output.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(17a)SX	The *show mls netflow ip routes* command was changed to the **show mls netflow ip sw-installed** command.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Examples

This example shows how to display the software-installed nonstatic entries:

```
Router> show mls netflow ip sw-installed non-static
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------
Router>
```

This example shows how to display detailed information for the software-installed nonstatic entries:

```
Router> show mls netflow ip sw-installed non-static detail
Displaying Netflow entries in Supervisor Earl
DstIP           SrcIP           Prot:SrcPort:DstPort  Src i/f:AdjPtr
---------------------------------------------------------------------
Pkts         Bytes       Age   LastSeen  Attributes
-------------------------------------------------

    QoS     Police Count Threshold    Leak     Drop Bucket  Use-Tbl Use-Enable
-----------+------------+---------+-----------+----+-------+-------+----------+
Router>
```

This example shows how to display the total number of software-installed nonstatic entries:

```
Router> show mls netflow ip sw-installed non-static count
Displaying Netflow entries in Supervisor Earl

 Number of shortcuts = 0
Router>
```

Related Commands

Command	Description
show mls netflow ip	Displays information about MLS NetFlow IP traffic.
show mls netflow ip dynamic	Displays the statistics for NetFlow IP entries.
show mls netflow ip routes	Displays the NetFlow IP routing entries.

show mls netflow ipx

To display MLS NetFlow IPX information in the EXEC command mode, use the **show mls netflow ipx** command.

show mls netflow ipx [**count** | **destination** {*hostname* | *ipx-address*} | **detail** | **flow** {**tcp** | **udp**} | {**interface** *interface interface-number* | **vlan** *vlan-id* | **macd** *destination-mac-address* | **macs** *source-mac-address* | **routes** *num* | **module** *number* | **source** {*hostname* | *ipx-address*} | **statistics**]

Syntax Description

count	(Optional) Displays the total number of MLS NetFlow IPX entries.
destination *hostname*	(Optional) Displays the entries for a specific destination IPX hostname.
destination *ipx-address*	(Optional) Displays the entries for a specific destination IPX address.
detail	(Optional) Specifies a detailed output.
flow	(Optional) Changes the flow type.
tcp | **udp**	Specifies the flow type.
interface	(Optional) Specifies the interface.
interface	(Optional) Interface type; possible valid values are **ethernet**, **fastethernet**, **gigabitethernet**, **tengigabitethernet**, **pos**, **atm**, and **ge-wan**.
interface-number	(Optional) Module and port number; see the "Usage Guidelines" section for valid values.
vlan *vlan-id*	(Optional) Specifies the VLAN ID; valid values are from 1 to 4094.
macd *destination -mac-address*	(Optional) Specifies the destination MAC address.
macs *source-mac-address*	(Optional) Specifies the source MAC address.
routes *num*	(Optional) Displays the routing NetFlow entries.
module *number*	(Optional) Displays the entries that are downloaded on the specified module; see the "Usage Guidelines" section for valid values.
source *hostname*	(Optional) Displays the entries for a specific source address.
source *ipx-address*	(Optional) Displays the entries for a specific destination IPX address.
statistics	(Optional) Displays the statistics for NetFlow entries.

Defaults

This command has no default settings.

Command Modes

EXEC

Command History

Release	Modification
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to Release 12.2(17d)SXB.

Usage Guidelines

The s**how mls netflow ipx** command is only supported on systems that have a version 2 Supervisior Engine.

The **interface**, **macd**, and **macs** keywords are not supported.

When you enter the *ipx-network*, the format is N.H.H.H.

When you enter the *destination-mac-address*, the format for the 48-bit MAC address is H.H.H.

The *interface-number* argument designates the module and port number. Valid values for *interface-number* depend on the specified interface type and the chassis and module used. For example, if you specify a Gigabit Ethernet interface and have a 48-port 10/100BASE-T Ethernet module installed in a 13-slot chassis, valid values for the module number are from 1 to 13 and valid values for the port number are from 1 to 48. These valid values also apply when entering the **module** *number* keyword and argument.

Examples

The output from the **show mls netflow ipx** commands is similar to the **show mls netflow ip** commands.

Related Commands

Command	Description
show mls netflow ip	Displays information about the hardware NetFlow IP.

show mls sampling

To display information about the sampled NDE status, use the **show mls sampling** command in user EXEC or privileged EXEC mode.

show mls sampling

Syntax Description

This command has no keywords or arguments.

Defaults

This command has no default settings.

Command Modes

User EXEC
Privileged EXEC

Command History

Release	Modification
12.2(14)SX	Support for this command was introduced on the Supervisor Engine 720.
12.2(17d)SXB	Support for this command on the Supervisor Engine 2 was extended to the 12.2 SX release.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.

Usage Guidelines

Sampled NetFlow is supported on Layer 3 interfaces only.

Examples

This example shows how to display information about the sampled NDE status:

```
Router# show mls sampling
time-based sampling is enabled
1 out of every 1024 packets is being sampled.
Sampling Interval and Period is 4 millisec per 4096 millisec
Router#
```

Related Commands

Command	Description
mls netflow sampling	Enables the sampled NetFlow on an interface.
mls sampling	Enables the sampled NetFlow and specifies the sampling method.

sort-by

To specify the sorting criterion for the NetFlow top talkers (unaggregated top flows), use the **sort-by** command in NetFlow top talkers configuration mode. To disable NetFlow top talkers, use the **no** form of this command.

sort-by [**bytes** | **packets**]

no sort-by [**bytes** | **packets**]

Syntax Description

bytes	Sorts the list of top talkers by the total number of bytes in each Top Talker.
packets	Sort the list of top talkers by the total number of packets in each Top Talker.

Defaults

No default behavior or values.

Command Modes

NetFlow top talkers configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring NetFlow Top Talkers

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands. Optionally, the **match** command can be configured to specify additional matching criteria.

Examples

In the following example, a maximum of four top talkers is configured. The sort criterion is configured to sort the list of top talkers by the total number of bytes for each top talker.

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command with the configuration from the previous example:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   349K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   349K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   328K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   303K
4 of 4 top talkers shown. 11 flows processed
```

Related Commands

Command	Description
cache-timeout	Specifies the length of time for which the list of top talkers (heaviest traffic patterns and most-used applications in the network) for the NetFlow MIB and top talkers feature is retained.
ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip flow top-talkers	Displays the statistics for the NetFlow accounting top talkers (heaviest traffic patterns and most-used applications in the network).
top	Specifies the maximum number of top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.

top

To specify the maximum number of NetFlow top talkers (unaggregated top flows) to display the statistics for, use the **top** command in NetFlow top talkers configuration mode. To disable NetFlow top talkers, use the **no** form of this command.

top *number*

no top

Syntax Description

number	The maximum number of top talkers that will be displayed. The range is 1 to 200.

Defaults

No default behavior or values.

Command Modes

NetFlow top talkers configuration

Command History

Release	Modification
12.2(25)S	This command was introduced.
12.3(11)T	This feature was integrated into Cisco IOS Release 12.3(11)T.
12.2(27)SBC	This feature was integrated into Cisco IOS Release 12.2(27)SBC.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.

Usage Guidelines

Configuring NetFlow Top Talkers

You must enable NetFlow on at least one interface in the router; and configure NetFlow top talkers before you can use the **show ip flow top-talkers** command to display the traffic statistics for the unaggregated top flows in the network. NetFlow top talkers also requires that you configure the **sort-by** and **top** commands. Optionally, the **match** command can be configured to specify additional matching criteria.

Examples

In the following example, a maximum of four top talkers is configured. The sort criterion is configured to sort the list of top talkers by the total number of bytes for each top talker.

```
Router(config)# ip flow-top-talkers
Router(config-flow-top-talkers)# top 4
Router(config-flow-top-talkers)# sort-by bytes
```

The following example shows the output of the **show ip flow top talkers** command with the configuration from the previous example:

```
Router# show ip flow top-talkers

SrcIf         SrcIPaddress    DstIf         DstIPaddress    Pr SrcP DstP Bytes
Et0/0.1       10.10.18.1      Et1/0.1       172.16.10.232   11 00A1 00A1   349K
Et0/0.1       10.10.19.1      Et1/0.1       172.16.10.2     11 00A2 00A2   349K
Et0/0.1       172.30.216.196  Et1/0.1       172.16.10.2     06 0077 0077   328K
Et0/0.1       10.162.37.71    Et1/0.1       172.16.10.2     06 0050 0050   303K
4 of 4 top talkers shown. 11 flows processed
```

Related Commands

Command	Description
cache-timeout	Specifies the length of time for which the list of top talkers (heaviest traffic patterns and most-used applications in the network) for the NetFlow MIB and top talkers feature is retained.
ip flow-top-talkers	Enters the configuration mode for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
match (NetFlow)	Specifies match criteria for the NetFlow MIB and top talkers (heaviest traffic patterns and most-used applications in the network) feature.
show ip cache flow	Displays a summary of the NetFlow accounting statistics.
show ip cache verbose flow	Displays a detailed summary of the NetFlow accounting statistics.
show ip flow interface	Displays NetFlow accounting configuration for interfaces.
show ip flow top-talkers	Displays the statistics from to the top talkers (heaviest traffic patterns and most-used applications in the network).
sort-by	Specifies the sorting criterion for top talkers (heaviest traffic patterns and most-used applications in the network) to be displayed for the NetFlow MIB and top talkers feature.