Flexible NetFlow Command Reference

July 2011

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

Flexible NetFlow Command Reference

CONTENTS

About Cisco IOS Software Documentation

Last Updated: July 30, 2010

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

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

Audience

The Cisco IOS 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 commands necessary to perform particular tasks. The Cisco IOS 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 release.

Documentation Conventions

In Cisco IOS 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 contains the following topics:

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.
italic	Italic text indicates arguments for which you supply values.
[x]	Square brackets enclose an optional keyword or argument.
...	An ellipsis (three consecutive nonbolded periods without spaces) after a syntax element indicates that the element can be repeated.
|	A vertical line, called a pipe, that is enclosed within braces or square brackets 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.
< >	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

Cisco IOS documentation 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. It also lists the configuration guides, command references, and supplementary references and resources that comprise the documentation set. It contains the following topics:

Cisco IOS Documentation Set

The Cisco IOS documentation set 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 select severity 3 (moderate) defects in released Cisco IOS software. Review release notes before other documents to learn whether updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
  - Configuration guides—Compilations of documents that provide conceptual and task-oriented descriptions of Cisco IOS features.
  - Command references—Compilations of command pages in alphabetical order that provide detailed information about the commands used in the Cisco IOS features and the processes that comprise the related configuration guides. For each technology, there is a single command reference that supports all Cisco IOS releases and that is updated at each standard release.
- 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. Command pages 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 organization of the Cisco IOS documentation set 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.

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 descriptions of Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are organized by technology. For information about all Cisco IOS commands, use the Command Lookup Tool at http://tools.cisco.com/Support/CLILookup or the *Cisco IOS Master Command List, All Releases*, at http://www.cisco.com/en/US/docs/ios/mcl/allreleasemcl/all_book.html.

Cisco IOS Supplementary Documents and Resources

Supplementary documents and resources are listed in Table 2 on page 19.

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 Cisco IOS command references contain commands for Cisco IOS software for all releases. The configuration guides and command references 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.

For additional information about configuring and operating specific networking devices, and to access Cisco IOS documentation, go to the Product/Technologies Support area of Cisco.com at the following location:

http://www.cisco.com/go/techdocs

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 Access Aggregation and DSL Configuration Guide* • *Cisco IOS Broadband Access Aggregation and DSL Command Reference*	PPP over ATM (PPPoA) and PPP over Ethernet (PPPoE).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Carrier Ethernet Configuration Guide* • *Cisco IOS Carrier Ethernet Command Reference*	Operations, Administration, and Maintenance (OAM); Ethernet connectivity fault management (CFM); ITU-T Y.1731 fault management functions; Ethernet Local Management Interface (ELMI); MAC address support on service instances, bridge domains, and pseudowire; IEEE 802.3ad Link Bundling; Link Aggregation Control Protocol (LACP) support for Ethernet and Gigabit Ethernet links and EtherChannel bundles; LACP support for stateful switchover (SSO), in service software upgrade (ISSU), Cisco nonstop forwarding (NSF), and nonstop routing (NSR) on Gigabit EtherChannel bundles; and Link Layer Discovery Protocol (LLDP) and media endpoint discovery (MED).
• *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.
• *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), dial-on-demand routing, dial-out, ISDN, large scale dial-out, modem and resource pooling, Multilink PPP (MLP), PPP, and virtual private dialup network (VPDN).
• *Cisco IOS Flexible NetFlow Configuration Guide* • *Cisco IOS Flexible NetFlow Command Reference*	Flexible NetFlow.
• *Cisco IOS High Availability Configuration Guide* • *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 Services Gateway Configuration Guide* • *Cisco IOS Intelligent Services Gateway Command Reference*	Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, and 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).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *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.
• *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: BFD Configuration Guide*	Bidirectional forwarding detection (BFD).
• *Cisco IOS IP Routing: BGP Configuration Guide* • *Cisco IOS IP Routing: BGP Command Reference*	Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast.
• *Cisco IOS IP Routing: EIGRP Configuration Guide* • *Cisco IOS IP Routing: EIGRP Command Reference*	Enhanced Interior Gateway Routing Protocol (EIGRP).
• *Cisco IOS IP Routing: ISIS Configuration Guide* • *Cisco IOS IP Routing: ISIS Command Reference*	Intermediate System-to-Intermediate System (IS-IS).
• *Cisco IOS IP Routing: ODR Configuration Guide* • *Cisco IOS IP Routing: ODR Command Reference*	On-Demand Routing (ODR).
• *Cisco IOS IP Routing: OSPF Configuration Guide* • *Cisco IOS IP Routing: OSPF Command Reference*	Open Shortest Path First (OSPF).
• *Cisco IOS IP Routing: Protocol-Independent Configuration Guide* • *Cisco IOS IP Routing: Protocol-Independent Command Reference*	IP routing protocol-independent features and commands. Generic policy-based routing (PBR) features and commands are included.
• *Cisco IOS IP Routing: RIP Configuration Guide* • *Cisco IOS IP Routing: RIP Command Reference*	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.
• *Cisco IOS ISO CLNS Configuration Guide* • *Cisco IOS ISO CLNS Command Reference*	ISO Connectionless Network Service (CLNS).

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *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.
• *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, and 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.

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

Configuration Guide and Command Reference Titles	Features/Protocols/Technologies
• *Cisco IOS Optimized Edge Routing Configuration Guide* • *Cisco IOS Optimized Edge Routing Command Reference*	Optimized edge routing (OER) monitoring and automatic route optimization and load distribution for multiple connections between networks.
• *Cisco IOS Performance Routing Configuration Guide* • *Cisco IOS Performance Routing Command Reference*	Performance Routing (PfR) provides additional intelligence to classic routing technologies to track the performance of, or verify the quality of, a path between two devices over a WAN infrastructure in order to determine the best egress or ingress path for application traffic.
• *Cisco IOS Quality of Service Solutions Configuration Guide* • *Cisco IOS Quality of Service Solutions Command Reference*	Traffic queueing, traffic policing, traffic shaping, Modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), Multilink PPP (MLP) for QoS, header compression, AutoQoS, Resource Reservation Protocol (RSVP), and weighted random early detection (WRED).
• *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 Security Configuration Guide: Securing the Data Plane*	Access Control Lists (ACLs); Firewalls: Context-Based Access Control (CBAC) and Zone-Based Firewall; Cisco IOS Intrusion Prevention System (IPS); Flexible Packet Matching; Unicast Reverse Path Forwarding (uRPF); Threat Information Distribution Protocol (TIDP) and TMS.
• *Cisco IOS Security Configuration Guide: Securing the Control Plane*	Control Plane Policing, Neighborhood Router Authentication.
• *Cisco IOS Security Configuration Guide: Securing User Services*	AAA (includes 802.1x authentication and Network Admission Control [NAC]); Security Server Protocols (RADIUS and TACACS+); Secure Shell (SSH); Secure Access for Networking Devices (includes Autosecure and Role-Based CLI access); Lawful Intercept.
• *Cisco IOS Security Configuration Guide: Secure Connectivity*	Internet Key Exchange (IKE) for IPsec VPNs; IPsec Data Plane features; IPsec Management features; Public Key Infrastructure (PKI); Dynamic Multipoint VPN (DMVPN); Easy VPN; Cisco Group Encrypted Transport VPN (GETVPN); SSL VPN.
• *Cisco IOS Service Advertisement Framework Configuration Guide* • *Cisco IOS Service Advertisement Framework Command Reference*	Cisco Service Advertisement Framework.
• *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 Activation Configuration Guide* • *Cisco IOS Software Activation Command Reference*	An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses.
• *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). **Note** For information about virtual switch configuration, see the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch.
• *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 Tunnel Protocol Version 3 (L2TPv3); L2VPN Pseudowire Redundancy; L2VPN Interworking; Layer 2 Local Switching; Link Access Procedure, Balanced (LAPB); 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 lists documents and resources that supplement the Cisco IOS software configuration guides and command references.

Table 2 Cisco IOS Supplementary Documents and Resources

Document Title or Resource	Description
Cisco IOS Master Command List, All Releases	Alphabetical list of all the commands documented in all Cisco IOS releases.
Cisco IOS New, Modified, Removed, and Replaced Commands	List of all the new, modified, removed, and replaced commands for a Cisco IOS release.
Cisco IOS System Message Guide	List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system, may be informational only, or may help diagnose problems with communications lines, internal hardware, or system software.
Cisco IOS Debug Command Reference	Alphabetical list of **debug** commands including brief descriptions of use, command syntax, and usage guidelines.
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.
RFCs	Standards documents maintained by the Internet Engineering Task Force (IETF) that Cisco IOS documentation references where applicable. The full text of referenced RFCs may be obtained at the following URL: http://www.rfc-editor.org/

Additional Resources and Documentation Feedback

What's New in Cisco Product Documentation is released 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

Last Updated: February 24, 2010

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:

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

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

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/Technologies Support area of Cisco.com at http://www.cisco.com/go/techdocs.

After you have performed the initial configuration and connected the device to your network, you can configure the device by using the console port or a remote access method, such as Telnet or Secure Shell (SSH), to access the 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.

Note The AUX port on the Route Processor (RP) installed in a Cisco ASR 1000 series router does not serve any useful customer purpose and should be accessed only under the advisement of a customer support representative.

Using the CLI

This section describes the following topics:

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.
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.

Table 3 CLI Command Modes (continued)

Command Mode	Access Method	Prompt	Exit Method	Mode Usage
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 # >` The # symbol represents the line number and increments at each prompt.	Issue the **continue** command.	• Run as the default operating mode when a valid image cannot be loaded. • Access the fall-back procedure for loading an image when the device lacks a valid 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.
Diagnostic (available only on Cisco ASR 1000 series routers)	The router boots or enters diagnostic mode in the following scenarios. When a Cisco IOS process or processes fail, in most scenarios the router will reload. • A user-configured access policy was configured using the **transport-map** command, which directed the user into diagnostic mode. • The router was accessed using an RP auxiliary port. • A break signal (**Ctrl-C**, **Ctrl-Shift-6**, or the **send break** command) was entered, and the router was configured to enter diagnostic mode when the break signal was received.	`Router(diag)#`	If a Cisco IOS process failure is the reason for entering diagnostic mode, the failure must be resolved and the router must be rebooted to exit diagnostic mode. If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or use a method that is configured to connect to the Cisco IOS CLI. If the RP auxiliary port was used to access the router, use another port for access. Accessing the router through the auxiliary port is not useful for customer purposes.	• Inspect various states on the router, including the Cisco IOS state. • Replace or roll back the configuration. • Provide methods of restarting the Cisco IOS software or other processes. • Reboot hardware (such as the entire router, an RP, an ESP, a SIP, a SPA) or other hardware components. • Transfer files into or off of the router using remote access methods such as FTP, TFTP, and SCP.

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 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 CLI includes an interactive Help feature. Table 4 describes the purpose of the CLI interactive Help commands.

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.
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
```

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 numeral. 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 numeral 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 the following:

http://www.cisco.com/en/US/products/sw/iosswrel/ps1831/products_tech_note09186a00801746e6.shtml

Using the Command History Feature

The command history feature saves, in a command history buffer, the commands that you enter during a session. The default number of saved commands 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 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 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 are 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 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 the following:

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_a1.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 to 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. To see what **default** commands are available on your system, enter **default ?** in the appropriate command mode of the command-line interface.

The **no** form is documented in the command pages of Cisco IOS command references. The **default** form is generally documented in the command pages only when the **default** form performs a function different than that of the plain and **no** forms of the command.

Command pages often include a "Command Default" section as well. The "Command Default" section documents the state of the configuration if the command is not used (for configuration commands) or the outcome of using the command if none of the optional keywords or arguments is specified (for EXEC commands).

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*:

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 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.

The following three output modifiers are available:

- **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.	Reenter 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 *Cisco IOS Release 12.4T System Message Guide*.

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" 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/Technology Support

  http://www.cisco.com/go/techdocs
- Support area on Cisco.com (also search for documentation by task or product)

  http://www.cisco.com/en/US/support/index.html
- 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
- Output Interpreter, a troubleshooting tool that analyzes command output of supported **show** commands

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

Cisco IOS Flexible NetFlow Commands

cache (Flexible NetFlow)

To configure a flow cache parameter for a Flexible NetFlow flow monitor, use the **cache** command in Flexible NetFlow flow monitor configuration mode. To remove a flow cache parameter for a Flexible NetFlow flow monitor, use the **no** form of this command.

cache {**entries** *number* | **timeout** {**active** *seconds* | **inactive** *seconds* | **update** *seconds* | **event transaction-end**} | **type** {**immediate** | **normal** | **permanent**}}

no cache {**entries** | **timeout** {**active** | **inactive** | **update** | **event transaction-end**} | **type**}

Syntax Description

entries *number*	Specifies the maximum number of entries in the flow monitor cache. Range: 16 to 1048576. Default: 4096.
timeout active *seconds*	Specifies the active flow timeout in seconds. Range: 1 to 604800 (7 days). Default: 1800.
timeout inactive *seconds*	Specifies the inactive flow timeout in seconds. Range: 1 to 604800 (7 days). Default: 15.
timeout update *seconds*	Specifies the update timeout, in seconds, for a permanent flow cache. Range: 1 to 604800 (7 days). Default: 1800.
timeout event transaction-end	Specifies that the record is generated and exported in the NetFlow cache at the end of a transaction.
type	Specifies the type of the flow cache.
immediate	Configures an immediate cache type. This cache type will age out every record as soon as it is created.
normal	Configures a normal cache type. The entries in the flow cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. This is the default cache type.
permanent	Configures a permanent cache type. This cache type disables flow removal from the flow cache.

Command Default

The default Flexible NetFlow flow monitor flow cache parameters are used.

The following flow cache parameters for a Flexible NetFlow flow monitor are enabled:

- Cache type: normal
- Maximum number of entries in the flow monitor cache: 4096
- Active flow timeout: 1800 seconds
- Inactive flow timeout: 15 seconds
- Update timeout for a permanent flow cache: 1800 seconds

Command Modes

Flexible NetFlow flow monitor configuration (config-flow-monitor)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was modified. Support for this command was added for Cisco 7200 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
Cisco IOS XE Release 3.4S	This command was modified. The **event transaction-end** keyword was added.

Usage Guidelines

Each flow monitor has a cache that it uses to store all the flows it monitors. Each cache has various configurable elements, such as the number of entries and the time that a flow is allowed to remain in it. When a flow times out, it is removed from the cache and sent to any exporters that are configured for the corresponding flow monitor.

If a cache is already active (that is, you have applied the flow monitor to at least one interface in the router), your changes to the record, cache type, and cache size parameters will not take effect until you either reboot the router or remove the flow monitor from every interface and then reapply it. Therefore whenever possible you should customize the record, cache type, and cache size parameters for the cache before you apply the flow monitor to an interface. You can modify the timers, flow exporters, and statistics parameters for a cache while the cache is active.

cache entries

This command controls the size of the cache. Cache size should be based on a number of factors, including the number of flows expected, the time the flows are expected to last (based on the configured key fields and the traffic), and the timeout values configured for the cache. The size should be large enough to minimize emergency expiry.

Emergency expiry is caused by the Flexible NetFlow cache becoming full. When the Flexible NetFlow cache becomes full, the router performs “emergency expiry” where a number of flows are immediately aged, expired from the Flexible NetFlow cache, and exported in order to free up space for more flows.

For a permanent cache (flows never expire), the number of entries should be large enough to accommodate the number of flows expected for the entire duration of the cache entries. If more flows occur than there are cache entries, the excess flows are not recorded in the cache.

For an immediate cache (flows expire immediately), the number of entries simply controls the amount of history that is available for previously seen packets.

cache timeout active

This command controls the aging behavior of the normal type of cache. If a flow has been active for a long time, it is usually desirable to age it out (starting a new flow for any subsequent packets in the flow). This age out process allows the monitoring application that is receiving the exports to remain up to date. By default this timeout is 1800 seconds (30 minutes), but it can be adjusted according to system requirements. A larger value ensures that long-lived flows are accounted for in a single flow record; a smaller value results in a shorter delay between starting a new long-lived flow and exporting some data for it.

cache timeout inactive

This command controls the aging behavior of the normal type of cache. If a flow has not seen any activity for a specified amount of time, that flow will be aged out. By default, this timeout is 15 seconds, but this value can be adjusted depending on the type of traffic expected.

If a large number of short-lived flows is consuming many cache entries, reducing the inactive timeout can reduce this overhead. If a large number of flows frequently get aged out before they have finished collecting their data, increasing this timeout can result in better flow correlation.

cache timeout update

This command controls the periodic updates sent by the permanent type of cache. This behavior is similar to the active timeout, except that it does not result in the removal of the cache entry from the cache. By default this timer value is 1800 seconds (30 minutes).

cache timeout event transaction-end

To use this command, you must configure the **match connection transaction id** command and the **match application name** command for the flow record. This command causes the record to be generated and exported in the NetFlow cache at the end of a transaction. A transaction is a set of logical exchanges between endpoints. There is normally one transaction within a flow.

cache type immediate

This command specifies the immediate cache type. This type of cache will age out every record as soon as it is created, with the result that every flow contains just one packet. The commands that display the cache contents will provide a history of the packets seen.

The use of this cache type is appropriate when very small flows are expected and a minimum amount of latency between analyzing a packet and exporting a report is desired. We recommend using this command when you are sampling packet chunks because the number of packets per flow is typically very low.

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

Note The timeout settings have no effect for the immediate cache type.

cache type normal

This command specifies the normal cache type. This is the default cache type. The entries in the cache will be aged out according to the **timeout active** *seconds* and **timeout inactive** *seconds* settings. When a cache entry is aged out, it is removed from the cache and exported via any exporters configured for the monitor associated with the cache.

cache type permanent

This command specifies the permanent cache type. This type of cache never ages out any flows. This cache type is useful when the number of flows you expect to see has a limit and there is a need to keep long-term statistics on the router. For example, if the only key field is IP TOS, a limit of 256 flows can be seen, so to monitor the long-term usage of the IP TOS field, a permanent cache can be used. Update messages are exported via any exporters configured for the monitor associated with this cache in accordance with the **timeout update** *seconds* setting.

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

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

Examples

The following example shows how to configure the number of entries for the flow monitor cache:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache entries 16
```

The following example shows how to configure the active timeout for the flow monitor cache:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache timeout active 4800
```

The following example shows how to configure the inactive timer for the flow monitor cache:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache timeout inactive 3000
```

The following example shows how to configure the permanent cache update timeout:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache timeout update 5000
```

The following example shows how to configure a normal cache:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache type normal
```

The following example shows how to configure a permanent cache:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache type permanent
```

The following example shows how to configure an immediate cache:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# cache type immediate
```

Related Commands

Command	Description
flow monitor	Creates a flow monitor, and enters Flexible NetFlow flow monitor configuration mode.

clear flow exporter

To clear the statistics for a Flexible NetFlow flow exporter, use the **clear flow exporter** command in privileged EXEC mode.

clear flow exporter [[**name**] *exporter-name*] **statistics**

Syntax Description

name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) Name of a flow exporter that was previously configured.
statistics	Clears the flow exporter statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example clears the statistics for all of the flow exporters configured on the router:

```
Router# clear flow exporter statistics
```

The following example clears the statistics for the flow exporter named FLOW-EXPORTER-1:

```
Router# clear flow exporter name FLOW-EXPORTER-1 statistics
```

Related Commands

Command	Description
debug flow exporter	Enables debugging output for flow exporters.

clear flow monitor

To clear a Flexible NetFlow flow monitor, flow monitor cache, or flow monitor statistics and to force the export of the data in the flow monitor cache, use the **clear flow monitor** command in privileged EXEC mode.

clear flow monitor name *monitor-name* [**cache** [**force-export**] | **force-export** | **statistics**]

Syntax Description

name	Specifies the name of a flow monitor.
monitor-name	Name of a flow monitor that was previously configured.
cache	(Optional) Clears the flow monitor cache information.
force-export	(Optional) Forces the export of the flow monitor cache statistics.
statistics	(Optional) Clears the flow monitor statistics.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

cache

This keyword removes all entries from the flow monitor cache. These entries will not be exported and the data gathered in the cache will be lost.

Note The statistics for the cleared cache entries are maintained.

force-export

This keyword removes all entries from the flow monitor cache and exports them via all flow exporters assigned to the flow monitor. This action can result in a short-term increase in CPU usage. Use with caution.

Note The statistics for the cleared cache entries are maintained.

statistics

This keyword clears the statistics for this flow monitor.

Note The "Current entries" statistic will not be cleared because this is an indicator of how many entries are in the cache and the cache is not cleared with this command.

Examples

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1:

```
Router# clear flow monitor name FLOW-MONITOR-1
```

The following example clears the statistics and cache entries for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Router# clear flow monitor name FLOW-MONITOR-1 force-export
```

The following example clears the cache for the flow monitor named FLOW-MONITOR-1 and forces an export:

```
Router# clear flow monitor name FLOW-MONITOR-1 cache force-export
```

The following example clears the statistics for the flow monitor named FLOW-MONITOR-1:

```
Router# clear flow monitor name FLOW-MONITOR-1 statistics
```

Related Commands

Command	Description
debug flow monitor	Enables debugging output for flow monitors.

clear sampler

To clear the statistics for a Flexible NetFlow flow sampler, use the **clear sampler** command in privileged EXEC mode.

clear sampler [**name**] *sampler-name*

Syntax Description

name	(Optional) Specifies the name of a flow sampler.
sampler-name	(Optional) Name of a flow sampler that was previously configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example clears the sampler statistics for all flow samplers configured on the router:

```
Router# clear sampler
```

The following example clears the sampler statistics for the flow sampler named SAMPLER-1:

```
Router# clear sampler name SAMPLER-1
```

Related Commands

Command	Description
debug sampler	Enables debugging output for flow samplers.

collect application name

To configure the use of the application name as a nonkey field for a Flexible NetFlow flow record, use the **collect application name** command in Flexible NetFlow flow record configuration mode. To disable the use of the application name as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect application name

no collect application name

Syntax Description

This command has no arguments or keywords.

Command Default

The application name is not configured as a non-key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
15.0(1)M	This command was introduced.

Examples

The following example configures the application name as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect application name
```

Related Commands

Command	Description
flow record	Creates a flow record.
match application name	Configures the use of application name as a key field for a Flexible NetFlow flow record.

collect connection

To configure various connection information fields as a nonkey field for a Flexible NetFlow flow record, use the **collect connection** command in Flexible NetFlow flow record configuration mode. To disable the use of the connection information fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect connection {**initiator** | **new-translations** | **sum-duration**}

no collect connection {**initiator** | **new-translations** | **sum-duration**}

Syntax Description

initiator	Configures information about the direction of the flow as a nonkey field.
new-translations	Configures the number of TCP or UDP connections that were opened during an observation period as a nonkey field.
sum-duration	Configures the total time in seconds for all of the TCP or UDP connections that were in use during an observation period as a nonkey field.

Command Default

Connection information fields are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

To use this command, you must configure the **match application name** command for the flow record.

The **initiator** keyword provides the following information about the direction of the flow.

- 0x00=undefined
- 0x01=initiator—The flow source is initiator of the connection.
- 0x02=reverseInitiator—The flow destination is the initiator of the connection.

For the **new-translations** and **sum-duration** keywords, the observation period can be specified by the start and end time stamps for the flow.

The Flexible NetFlow **collect** commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example shows how to configure information about the direction of the flow as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect connections initiator
```

Related Commands

Command	Description
flow record	Creates a flow record for Flexible NetFlow, and enters Flexible NetFlow flow record configuration mode.

collect counter

To configure the number of bytes or packets in a flow as a nonkey field for a Flexible NetFlow flow record, use the **collect counter** command in Flexible NetFlow flow record configuration mode. To disable the use of the number of bytes or packets in a flow (counters) as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect counter {**bytes** [**long** | **replicated** [**long**] | **squared long**] | **packets** [**long** | **replicated** [**long**]]}

no collect counter {**bytes** [**long** | **replicated** [**long**] | **squared long**] | **packets** [**long** | **replicated** [**long**]]}

Syntax Description

bytes	Configures the number of bytes seen in a flow as a nonkey field and enables collecting the total number of bytes from the flow.
long	(Optional) Enables collecting the total number of bytes or packets from the flow using a 64-bit counter rather than a 32-bit counter.
replicated	Total number of replicated (multicast) IPv4 packets.
squared long	(Optional) Enables collecting the total of the square of the number of bytes from the flow.
packets	Configures the number of packets seen in a flow as a nonkey field and enables collecting the total number of packets from the flow.

Command Default

The number of bytes or packets in a flow is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(22)T	The **replicated** keyword was added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow **collect** commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect counter bytes

This command configures a 32-bit counter for the number of bytes seen in a flow.

collect counter packets

This command configures a 32-bit counter that is incremented for each packet seen in the flow. For extremely long flows it is possible for this counter to restart at 0 (wrap) when it reaches the limit of approximately 4 billion packets. On detection of a situation that would cause this counter to restart at 0, a flow monitor with a normal cache type exports the flow and starts a new flow.

collect counter packets long

This command configures a 64-bit counter that will be incremented for each packet seen in the flow. It is unlikely that a 64-bit counter will ever restart at 0.

collect counter bytes squared long

This counter can be used in conjunction with the byte and packet counters in order to calculate the variance of the packet sizes. Its value is derived from squaring each of the packet sizes in the flow and adding the results. This value can be used as part of a standard variance function.

The variance and standard deviation of the packet sizes for the flow can be calculated with the following formulas:

cbs: value from the **counter bytes squared** field

pkts: value from the **counter packets** field

bytes: value from the **counter bytes** field

Variance = $(cbs/pkts) – (bytes/pkts)^2$

Standard deviation = square root of Variance

Example 1:

Packet sizes of the flow: 100, 100, 100, 100

Counter packets: 4

Counter bytes: 400, mean packet size = 100

Counter bytes squared: 40,000

Variance = $(40,000/4) – (400/4)^2 = 0$

Standard Deviation = 0

Size = 100 +/– 0

Example 2:

Packet sizes of the flow: 50, 150, 50, 150

Counter packets: 4

Counter bytes: 400, mean packet size = 100

Counter bytes squared: 50,000

Variance = $(50,000/4) – (400/4)^2 = 2500$

Standard deviation = 50

Size = 100 +/– 50

Examples

The following example configures the total number of bytes in the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect counter bytes
```

The following example configures the total number of bytes in the flows as a nonkey field using a 64-bit counter:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect counter bytes long
```

The following example configures the sum of the number of bytes of each packet in the flow squared as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect counter bytes squared long
```

The following example configures the total number of packets from the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect counter packets
```

The following example configures the total number of packets from the flows as a nonkey field using a 64-bit counter:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect counter packets long
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect datalink dot1q vlan

To configure the 802.1Q (dot1q) VLAN ID as a non-key field for a Flexible NetFlow flow record, use the **collect datalink dot1q vlan** command in Flexible NetFlow flow record configuration mode. To disable the use of the 802.1Q VLAN ID value as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect datalink dot1q vlan {**input** | **output**}

no collect datalink dot1q vlan {**input** | **output**}

Syntax Description

input	Configures the VLAN ID of traffic being received by the router as a nonkey field.
output	Configures the VLAN ID of traffic being transmitted by the router as a nonkey field.

Command Default

The 802.1Q VLAN ID is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

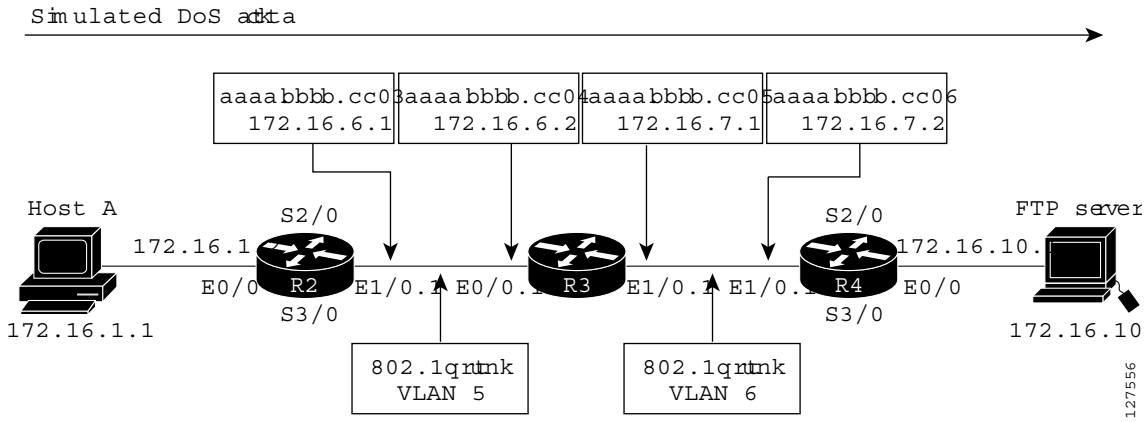
Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The **input** and **output** keywords of the **collect datalink dot1q vlan** command are used to specify the observation point that is used by the **collect datalink dot1q vlan** command to capture the 802.1q VLAN IDs from network traffic. For example, when you configure a flow record with the **collect datalink dot1q vlan input** command to monitor the simulated denial of service (DoS) attack in Figure 1 and apply the flow monitor to which the flow record is assigned in either input (ingress) mode on interface Ethernet 0/0.1 on R3 or output (egress) mode on interface Ethernet 1/0.1 on R3, the observation point is always Ethernet 0/0.1 on R3. The 802.1q VLAN ID that is collected is 5.

Figure 1 Simulated DoS Attack



The observation point of **collect** commands that do not have the input and/or output keywords is always the interface to which the flow monitor that contains the flow record with the **collect** commands is applied.

Examples

The following example configures the 802.1Q VLAN ID of traffic being received by the router as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect datalink dot1q vlan input
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect datalink mac

To configure the use of MAC addresses as a nonkey field for a Flexible NetFlow flow record, use the **collect datalink mac** command in Flexible NetFlow flow record configuration mode. To disable the use of Layer 2 MAC addresses as a non-key field for a Flexible NetFlow flow record, use the **no** form of this command.

collect datalink mac {**destination** | **source**} **address** {**input** | **output**}}

no collect datalink mac {**destination** | **source**} **address** {**input** | **output**}}

Syntax Description

destination address	Configures the use of the destination MAC address as a non-key field.
source address	Configures the use of the source MAC address as a non-key field.
input	Packets received by the router.
output	Packets transmitted by the router.

Command Default

MAC addresses are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

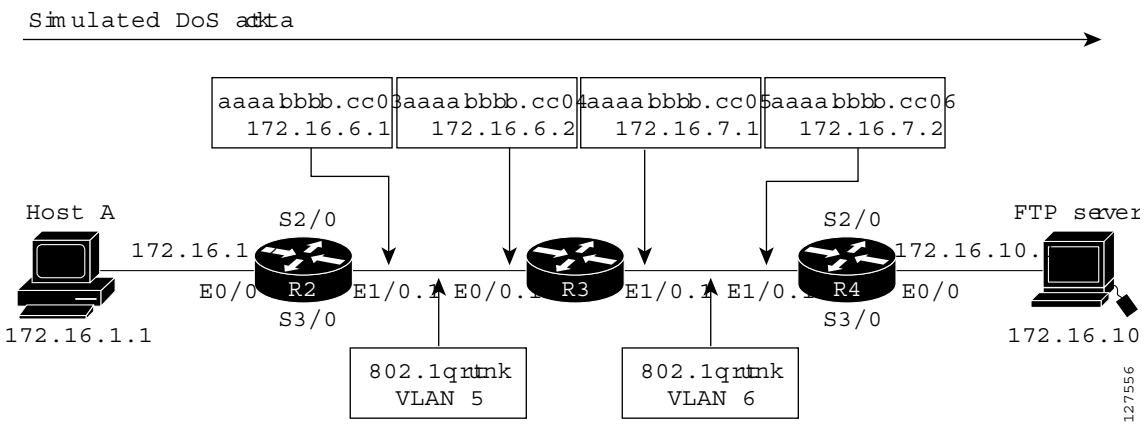
Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The **input** and **output** keywords of the **collect datalink mac** command are used to specify the observation point that is used by the **collect datalink mac** command to capture the MAC addressees from network traffic. For example, when you configure a flow record with the **collect datalink mac destination address input** command to monitor the simulated denial of service (DoS) attack in Figure 2 and apply the flow monitor to which the flow record is assigned in either input (ingress) mode on interface Ethernet 0/0.1 on R3 or output (egress) mode on interface Ethernet 1/0.1 on R3, the observation point is always Ethernet 0/0.1 on R3. The destination MAC address that is collected is aaaa.bbbb.cc04.

Figure 2 Simulated DoS Attack



When the destination output mac address is configured, the value is the destination mac address of the output packet, even if the monitor the flow record is applied to is input only.

When the destination input mac address is configured, the value is the destination mac address of the input packet, even if the monitor the flow record is applied to is output only.

When the source output mac address is configured, the value is the source mac address of the output packet, even if the monitor the flow record is applied to is input only.

When the source input mac address is configured, the value is the source mac address of the input packet, even if the monitor the flow record is applied to is output only.

Examples

The following example configures the use of the destination MAC address of packets that are received by the router as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect datalink mac destination address input
```

The following example configures the use of the source MAC addresses of packets that are transmitted by the router as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect datalink mac source address output
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect flow

To configure the flow direction, the flow sampler ID number, or reason why the flow ended as a nonkey field for a flow record, use the **collect flow** command in flow record configuration mode. To disable the use of the flow direction and the flow sampler ID number as a nonkey field for a flow record, use the **no** form of this command.

Flexible Netflow

collect flow {**direction** | **sampler** | **end-reason**}

no collect flow {**direction** | **sampler** | **end-reason**}

Cisco Performance Monitor in Cisco IOS Release 15.1(4)M1

collect flow direction

no collect flow direction

Syntax Description

direction	Configures the flow direction as a nonkey field and enables the collection of the direction in which the flow was monitored.
sampler	Configures the flow sampler ID as a nonkey field and enables the collection of the ID of the sampler that is assigned to the flow monitor.
end-reason	Configures the reason why the flow ended and was exported as a nonkey field. Also enables the collection of the reason.

Command Default

The flow direction and the flow sampler ID number are not configured as nonkey fields.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was modified. Support for this command was added for Cisco 7200 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
15.1(4)M1	This command was integrated into Cisco IOS Release 15.1(4)M1 with only the **direction** keyword.
Cisco IOS XE Release 3.4S	This command was modified. The **end-reason** keyword was added.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Flexible NetFlow, the mode is also known as Flexible NetFlow flow record configuration mode. For Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode. Here we refer to them both as flow record configuration mode.

The Flexible NetFlow and Performance Monitor **collect** commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect flow direction

This field indicates the direction of the flow. This is of most use when a single flow monitor is configured for input and output flows. It can be used to find and eliminate flows that are being monitored twice: once on input and once on output. This field may also be used to match up pairs of flows in the exported data when the two flows are flowing in opposite directions.

collect flow sampler

This field contains the ID of the flow sampler used to monitor the flow. This is useful when more than one flow sampler is being used with different sampling rates. The flow exporter **option sampler-table** command exports options records with mappings of the flow sampler ID to sampling rate so the collector can calculate the scaled counters for each flow.

collect flow end-reason

This field contains information about the reason why the flow ended and was exported. This information can be useful when troubleshooting issues with flows ending unexpectedly. The values for this field are:

- 0x00—Not determined. The reason for the termination of the flow could not be determined.
- 0x01—Idle timeout. The flow was terminated because it was considered to be idle.
- 0x02—Active timeout. The flow was terminated for reporting purposes while it was still active. For example, the flow was terminated after the maximum lifetime of unreported flows was reached.
- 0x03—End of flow detected. The flow was terminated because the Metering Process detected signals indicating the end of the flow. For example, the TCP FIN flag was detected.
- 0x04—Forced end. The flow was terminated because of some external event. For example, a shutdown of the Metering Process was initiated by a network management application.
- 0x05—Lack of resources. The flow was terminated because of a lack of resources available to the Metering Process and/or the Exporting Process.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **flow record type performance-monitor** command.

Examples

The following example shows how to configure the ID of the flow sampler that is assigned to the flow as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect flow sampler
```

Cisco Performance Monitor in Cisco IOS Release 15.1(4)M1

The following example shows how to configure the direction in which the flow was monitored as a nonkey field:

```
Router(config)# flow record type performance-monitor FLOW-RECORD-1
Router(config-flow-record)# collect flow direction
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter
flow record	Creates a flow record for Flexible NetFlow, and enters Flexible NetFlow flow record configuration mode.
flow record type performance-monitor	Creates a flow record for Performance Monitor, and enters Performance Monitor flow record configuration mode.

collect interface

To configure the input and output interface as a nonkey field for a flow record, use the **collect interface** command in flow record configuration mode. To disable the use of the input and output interface as a nonkey field for a flow record, use the **no** form of this command.

collect interface {**input** | **output**}

no collect interface {**input** | **output**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

collect interface {**input** [**physical**] | **output**} [**snmp**]

no collect interface {**input** [**physical**] | **output**} [**snmp**]

Syntax Description

input	Configures the input interface as a nonkey field and enables collecting the input interface from the flows.
output	Configures the output interface as a nonkey field and enables collecting the output interface from the flows.

Command Default

The input and output interface is not configured as a nonkey field.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and implemented on the Cisco 7200 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(50)SY	This command was modified. The **physical** and **snmp** keywords were added in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command, however the mode prompt is the same for both products. For Flexible NetFlow, the mode is also known as Flexible

NetFlow flow record configuration mode. For Performance Monitor, the mode is also known as Performance Monitor flow record configuration mode. Here we refer to them both as flow record configuration mode.

The Flexible NetFlow and Performance Monitor **collect** commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the **flow record type performance-monitor** command**.**

Examples

The following example configures the input interface as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect interface inpu
```

The following example configures the output interface as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect interface output
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example configures the input interface as a nonkey field:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# collect interface input
```

Related Commands

Command	Description
flow record	Creates a flow record for Flexible NetFlow.
flow record type performance-monitor	Creates a flow record for Performance Monitor.

collect ipv4

To configure one or more of the IPv4 fields as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv4 fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 {**dscp** | **header-length** | **id** | **option map** | **precedence** | **protocol** | **tos** | **version**}

no collect ipv4 {**dscp** | **header-length** | **id** | **option map** | **precedence** | **protocol** | **tos** | **version**}

Syntax Description

dscp	Configures the differentiated services code point (DCSP) field as a nonkey field and enables collecting the value in the IPv4 DSCP type of service (ToS) fields from the flows.
header-length	Configures the IPv4 header length flag as a nonkey field and enables collecting the value in the IPv4 header length (in 32-bit words) field from the flows.
id	Configures the IPv4 ID flag as a nonkey field and enables collecting the value in the IPv4 ID field from the flows.
option map	Configures the IPv4 options flag as a nonkey field and enables collecting the value in the bitmap representing which IPv4 options have been seen in the options field from the flows.
precedence	Configures the IPv4 precedence flag as a nonkey field and enables collecting the value in the IPv4 precedence (part of ToS) field from the flows.
protocol	Configures the IPv4 payload protocol field as a nonkey field and enables collecting the IPv4 value of the payload protocol field for the payload in the flows
tos	Configures the ToS field as a nonkey field and enables collecting the value in the IPv4 ToS field from the flows.
version	Configures the version field as a nonkey field and enables collecting the value in the IPv4 version field from the flows.

Command Default

The IPv4 fields are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Note Some of the keywords of the **collect ipv4** command are documented as separate commands. All of the keywords for the **collect ipv4** command that are documented separately start with **collect ipv4**. For example, for information about configuring the IPv4 time-to-live (TTL) field as a nonkey field and collecting its value for a Flexible NetFlow flow record, refer to the **collect ipv4 ttl** command.

Examples

The following example configures the DSCP field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv4 destination

To configure the IPv4 destination address as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4 destination** command in Flexible NetFlow flow record configuration mode. To disable the use of an IPv4 destination address field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no collect ipv4 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv4 destination address as a nonkey field and enables collecting the value of the IPv4 destination address from the flows.
mask	Configures the IPv4 destination address mask as a nonkey field and enables collecting the value of the IPv4 destination address mask from the flows.
prefix	Configures the prefix for the IPv4 destination address as a nonkey field and enables collecting the value of the IPv4 destination address prefix from the flows.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32.

Command Default

The IPv4 destination address is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the IPv4 destination address prefix from the flows that have a prefix of 16 bits as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
```

```
Router(config-flow-record)# collect ipv4 destination prefix minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv4 fragmentation

To configure the IPv4 fragmentation flags and the IPv4 fragmentation offset as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4 fragmentation** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 fragmentation flags and the IPv4 fragmentation offset as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 fragmentation {**flags** | **offset**}

no collect ipv4 fragmentation {**flags** | **offset**}

Syntax Description

flags	Configures the IPv4 fragmentation flags as a nonkey field and enables collecting the value in the IPv4 fragmentation flag fields from the flows.
offset	Configures the IPv4 fragmentation offset value as a nonkey field and enables collecting the value in the IPv4 fragmentation offset field from the flows.

Command Default

The IPv4 fragmentation flags and the IPv4 fragmentation offset are not configured as nonkey fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect ipv4 fragmentation flags

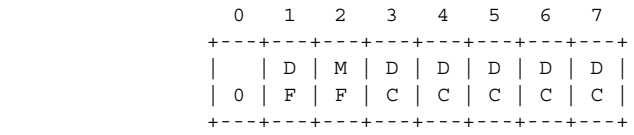
This field collects the “don’t fragment” and “more fragments” flags.

Bit 0: reserved, must be zero.

Bit 1: (DF) 0 = May Fragment, 1 = Don’t Fragment

Bit 2: (MF) 0 = Last Fragment, 1 = More Fragments

Bits 3–7: (DC) Don’t Care, value is irrelevant



For more information on IPv4 fragmentation flags, see RFC 791 *Internet Protocol* at the following URL: http://www.ietf.org/rfc/rfc791.txt.

Examples

The following example configures the IPv4 fragmentation flags as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 fragmentation flags
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv4 section

To configure a section of an IPv4 packet as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4 section** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv4 packet as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 section {**header size** *header-size* | **payload size** *payload-size*}

no collect ipv4 section {**header size** *header-size* | **payload size** *payload-size*}

Syntax Description

header size *header-size*	Configures the number of bytes of raw data starting at the IPv4 header to use as a nonkey field, and enables collecting the value in the raw data from the flows. Range: 1 to 1200.
payload size *payload-size*	Configures the number of bytes of raw data starting at the IPv4 payload to use as a nonkey field, and enables collecting the value in the raw data from the flows. Range: 1 to 1200.

Command Default

A section of an IPv4 packet is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

It is recommended that you configure both **header size** and **payload size** so that you know how much data is going to be captured.

collect ipv4 section header

This command causes the first IPv4 header to be copied into the flow record for this flow. Only the configured size in bytes will be copied and part of the payload will also be captured if the configured size is larger than the size of the header.

Note This command can result in large records which use a lot of router memory and export bandwidth.

collect ipv4 section payload

This command results in a copy of the first IPv4 payload being put into the flow record for this flow. Only the configured size in bytes will be copied and may end in a series of 0's if the configured size is greater than the size of the payload.

Note This command can result in large records which use a lot of router memory and export bandwidth.

Examples

The following example configures the first eight bytes from the IP header of the packets in the flows as a non-key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 section header size 8
```

The following example configures the first 16 bytes from the payload of the packets in the flows as a non-key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 section payload size 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv4 source

To configure the IPv4 source address as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4 source** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 source address field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no collect ipv4 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv4 source address as a nonkey field and enables collecting the value of the IPv4 source address from the flows.
mask	Configures the IPv4 source address mask as a nonkey field and enables collecting the value of the IPv4 source address mask from the flows.
prefix	Configures the prefix for the IPv4 source address as a nonkey field and enables collecting the value of the IPv4 source address prefix from the flows.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32.

Command Default

The IPv4 source address is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was implemented on the Cisco 7200 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect ipv4 source prefix minimum-mask

The source address prefix is the network part of an IPv4 source address. The optional minimum mask allows more information to be gathered about large networks.

collect ipv4 source mask minimum-mask

The source address mask is the number of bits that make up the network part of the source address. The optional minimum mask allows a minimum value to be configured. This command is useful when there is a minimum mask configured for the source prefix field and the mask is to be used with the prefix. In this case, the values configured for the minimum mask should be the same for the prefix and mask fields.

Alternatively, if the collector is aware of the minimum mask configuration of the prefix field, the mask field can be configured without a minimum mask so that the true mask and prefix can be calculated.

Examples

The following example configures the IPv4 source address prefix from the flows that have a prefix of 16 bits as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 source prefix minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv4 total-length

To configure the IPv4 total-length field as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4 total-length** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 total-length field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 total-length [**maximum** | **minimum**]

no collect ipv4 total-length [**maximum** | **minimum**]

Syntax Description

maximum	(Optional) Configures the maximum value of the total length field as a nonkey field and enables collecting the maximum value of the total length field from the flows.
minimum	(Optional) Configures the minimum value of the total length field as a nonkey field and enables collecting the minimum value of the total length field from the flows.

Command Default

The IPv4 total-length field is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect ipv4 total-length [minimum | maximum]

This command is used to collect the lowest and highest IPv4 total length values seen in the lifetime of the flow. Configuring this command results in more processing than is needed to simply collect the first total length value seen using the **collect ipv4 total-length** command.

Examples

The following example configures total-length value as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 total-length
```

The following example configures minimum total-length value seen in the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 total-length minimum
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv4 ttl

To configure the IPv4 time-to-live (TTL) field as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv4 ttl** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 TTL field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv4 ttl [**maximum** | **minimum**]

no collect ipv4 ttl [**maximum** | **minimum**]

Syntax Description

maximum	(Optional) Configures the maximum value of the TTL field as a nonkey field and enables collecting the maximum value of the TTL field from the flows.
minimum	(Optional) Configures the minimum value of the TTL field as a nonkey field and enables collecting the minimum value of the TTL field from the flows.

Command Default

The IPv4 time-to-live (TTL) field is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect ipv4 ttl [minimum | maximum]

This command is used to collect the lowest and highest IPv4 TTL values seen in the lifetime of the flow. Configuring this command results in more processing than is needed to simply collect the first TTL value seen using the **collect ipv4 ttl** command.

Examples

The following example configures the largest value for IPv4 TTL seen in the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 ttl maximum
```

The following example configures the smallest value for IPv4 TTL seen in the flows as a nonkey field

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv4 ttl minimum
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6

To configure one or more of the IPv6 fields as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv6 fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

no collect ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

Syntax Description

dscp	Configures the differentiated services code point (DCSP) field as a nonkey field and enables collecting the value in the IPv6 DSCP type of service (ToS) fields from the flows.
flow-label	Configures the IPv6 flow label as a nonkey field and enables collecting the value in the IPv6 flow label from the flows.
next-header	Configures the next-header field as a nonkey field and enables collecting the value of the next-header field in the IPv6 header from the flows.
payload-length	Configures the length of the IPv6 payload as a nonkey field and enables collecting the number of bytes used for the payload in the flows.
precedence	Configures the IPv6 precedence flag as a nonkey field and enables collecting the value in the IPv6 precedence (part of ToS) field from the flows.
protocol	Configures the IPv6 payload protocol field as a nonkey field and enables collecting the IPv6 value of the payload protocol field for the payload in the flows.
traffic-class	Configures the IPv6 traffic-class field as a nonkey field and enables collecting the value in the IPv6 protocol field from the flows.
version	Configures the IPv6 version field as a nonkey field and enables collecting the value in the IPv6 version field from the flows.

Command Default

The IPv6 fields are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Note Some of the keywords for the **collect ipv6** command are documented as separate commands. All of the keywords for the **collect ipv6** command that are documented separately start with **collect ipv6**. For example, for information about configuring the IPv6 hop limit field as a nonkey field and collecting its value for a Flexible NetFlow flow record, refer to the **collect ipv6 hop-limit command**.

Examples

The following example configures the IPv6 DSCP field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 destination

To configure the IPv6 destination address as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 destination** command in Flexible NetFlow flow record configuration mode. To disable the use of an IPv6 destination address field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no collect ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv6 destination address as a nonkey field and enables collecting the value of the IPv6 destination address from the flows.
mask	Configures the IPv6 destination address mask as a nonkey field and enables collecting the value of the IPv6 destination address mask from the flows.
prefix	Configures the prefix for the IPv6 destination address as a nonkey field and enables collecting the value of the IPv6 destination address prefix from the flows.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 128.

Command Default

TheIPv6 destination address is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the IPv6 destination address prefix from the flows that have a prefix of 16 bits as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 destination prefix minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 extension map

To configure the bitmap of the IPv6 extension header map as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 extension map** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 bitmap of IPv6 extension header map as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 extension map

no collect ipv6 extension map

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the bitmap of the IPv6 extension header map is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

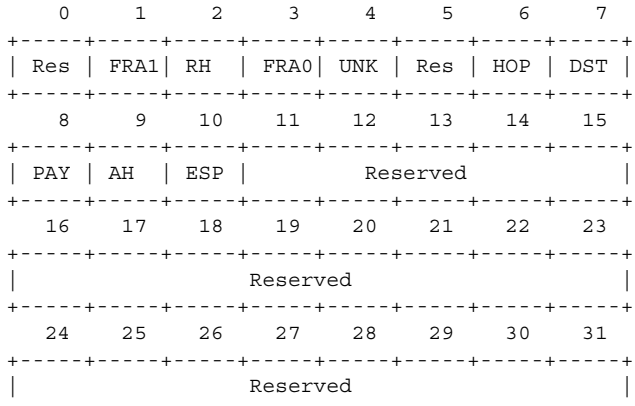
Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Bitmap of the IPv6 Extension Header Map

The bitmap of IPv6 extension header map is made up of 32 bits.



```
+-----+-----+-----+-----+-----+-----+-----+-----+
0  Res  Reserved
1  FRA1 Fragmentation header - not first fragment
2  RH   Routing header
3  FRA0 Fragment header - first fragment
4  UNK  Unknown Layer 4 header
        (compressed, encrypted, not supported)
5  Res  Reserved
6  HOP  Hop-by-hop option header
7  DST  Destination option header
8  PAY Payload compression header
9  AH  Authentication Header
10 ESP Encrypted security payload
11 to 31 Reserved
```

For more information on IPv6 headers, refer to RFC 2460 *Internet Protocol, Version 6 (IPv6)* at the following URL: http://www.ietf.org/rfc/rfc2460.txt.

Examples

The following example configures the bitmap of IPv6 extension header map as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 extension map
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 fragmentation

To configure one or more of the IPv6 fragmentation fields as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 fragmentation** command in Flexible NetFlow flow record configuration mode. To disable the use one or more of the IPv6 fragmentation fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 fragmentation {**flags** | **id** | **offset**}

no collect ipv6 fragmentation {**flags** | **id** | **offset**}

Syntax Description

flags	Configures the IPv6 fragmentation flags as a non-key field and enables collecting the value in the IPv6 fragmentation flag fields from the flows.
id	Configures the IPv6 fragmentation ID as a non-key field and enables collecting the value in the IPv6 fragmentation id fields from the flows
offset	Configures the IPv6 fragmentation offset as a non-key field and enables collecting the value in the IPv6 fragmentation offset field from the flows.

Command Default

The use of one or more of the IPv6 fragmentation fields is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the IPv6 fragmentation flags field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 fragmentation flags
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 hop-limit

To configure the IPv6 hop limit as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 hop-limit** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 hop limit field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 hop-limit [**maximum**] [**minimum**]

no collect ipv6 hop-limit [**maximum**] [**minimum**]

Syntax Description

maximum	(Optional) Configures the IPv6 maximum hop limit as a nonkey field and enables collecting the value of the IPv6 maximum hop limit from the flows.
minimum	(Optional) Configures the IPv6 minimum hop limit as a nonkey field and enables collecting the value of the IPv6 minimum hop limit from the flows.

Command Default

The IPv6 hop limit is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

collect ipv6 hop-limit [minimum | maximum]

This command is used to collect the lowest and highest IPv6 hop limit values seen in the lifetime of the flow. Configuring this command results in more processing than is needed to simply collect the first hop limit value seen using the **collect ipv6 hop-limit** command.

Examples

The following example configures the IPv6 maximum hop limit from the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 hop-limit maximum
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 length

To configure one or more of the IPv6 length fields as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 length** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv6 length fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 length {**header** | **payload** | **total** [**maximum**] [**minimum**]}

no collect ipv6 length {**header** | **payload** | **total** [**maximum**] [**minimum**]}

Syntax Description

header	Configures the length in bytes of the IPv6 header, not including any extension headers, as a nonkey field and collects the value of it for a Flexible NetFlow flow record.
payload	Configures the length in bytes of the IPv6 payload, including any extension headers, as a nonkey field and collects the value of it for a Flexible NetFlow flow record.
total	Configures the total length in bytes of the IPv6 header and payload as a nonkey field and collects the value of it for a Flexible NetFlow flow record.
maximum	(Optional) Configures the maximum total length in bytes of the IPv6 header and payload as a nonkey field and collects the value of it for a Flexible NetFlow flow record.
minimum	(Optional) Configures the minimum total length in bytes of the IPv6 header and payload as a nonkey field and collects the value of it for a Flexible NetFlow flow record.

Command Default

The IPv6 length fields are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

collect ipv6 length [minimum | maximum]

This command is used to collect the lowest and highest IPv6 length values seen in the lifetime of the flow. Configuring this command results in more processing than is needed to simply collect the length value seen using the **collect ipv6 length** command.

Examples

The following example configures the length of the IPv6 header, not including any extension headers, in bytes as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 length header
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 section

To configure a section of an IPv6 packet as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 section** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv6 packet as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 section {**header size** *header-size* | **payload size** *payload-size*}

no collect ipv6 section {**header size** *header-size* | **payload size** *payload-size*}

Syntax Description

header size *header-size*	Configures the number of bytes of raw data, starting at the IPv6 header, to use as a nonkey field, and enables collecting the value in the raw data from the flows. Range: 1 to 1200.
payload size *payload-size*	Configures the number of bytes of raw data, starting at the IPv6 payload, to use as a nonkey field, and enables collecting the value in the raw data from the flows. Range: 1 to 1200.

Command Default

A section of an IPv6 packet is not configured as a non-key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

It is recommended that you configure both **header size** and **payload size** so that you know how much data is going to be captured.

Note The IPv6 payload data is captured only if the first packet in the flow is an IPv6 packet. If the first packet in the flow is not an IPv6 packet, information from other packets in the flow such as packet and byte counters, is still captured.

collect ipv6 section header

This command causes a copy of the first IPv6 header to be put into the flow record for this flow. Only the configured size in bytes will be copied, and part of the payload will also be captured if the configured size is larger than the size of the header.

Note Configuring this command can result in large records that use a lot of router memory and export bandwidth.

collect ipv6 section payload

This command causes a copy of the first IPv6 payload to be put into the flow record for this flow. Only the configured size in bytes will be copied, and it may end in a series of zeros if the configured size is smaller than the size of the payload.

Note Configuring this command can result in large records that use a lot of router memory and export bandwidth.

Examples

The following example configures the first eight bytes from the IPv6 header of the packets in the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 section header size 8
```

The following example configures the first 16 bytes from the payload of the IPv6 packets in the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 section payload size 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect ipv6 source

To configure the IPv6 source address as a nonkey field for a Flexible NetFlow flow record, use the **collect ipv6 source** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 source address field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect ipv6 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no collect ipv6 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv6 source address as a nonkey field and enables collecting the value of the IPv6 source address from the flows.
mask	Configures the IPv6 source address mask as a nonkey field and enables collecting the value of the IPv6 source address mask from the flows.
prefix	Configures the prefix for the IPv6 source address as a nonkey field and enables collecting the value of the IPv6 source address prefix from the flows.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 128.

Command Default

The IPv6 source address is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect IPv6 source prefix minimum mask

The source address prefix field is the network part of the source address. The optional minimum mask allows more information to be gathered about large networks.

collect IPv6 source mask minimum mask

The source address mask is the number of bits that make up the network part of the source address. The optional minimum mask allows a minimum value to be configured. This command is useful when there is a minimum mask configured for the source prefix field and the mask is to be used with the prefix. In this case, the values configured for the minimum mask should be the same for the prefix and mask fields.

Alternatively, if the collector is aware of the minimum mask configuration of the prefix field, the mask field can be configured without a minimum mask so that the true mask and prefix can be calculated.

Examples

The following example configures the IPv6 source address prefix from the flows that have a prefix of 16 bits as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect ipv6 source prefix minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect routing

To configure one or more of the routing attributes as a nonkey field for a Flexible NetFlow flow record, use the **collect routing** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the routing attributes as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect routing {{**destination** | **source**} {**as** [**4-octet**] [**peer** [**4-octet**]] | **traffic-index**} | **forwarding-status** | **next-hop address** {**ipv4** | **ipv6**} [**bgp**] | **vrf input**}

no collect routing {{**destination** | **source**} {**as** [**4-octet**] [**peer** [**4-octet**]] | **traffic-index**} | **forwarding-status** | **next-hop address** {**ipv4** | **ipv6**} [**bgp**] | **vrf input**}

Syntax Description

destination	Configures one or more of the destination routing attributes fields as a nonkey field and enables collecting the values from the flows.
source	Configures one or more of the source routing attributes fields as a nonkey field and enables collecting the values from the flows.
as	Configures the autonomous system field as a nonkey field and enables collecting the value in the autonomous system field from the flows.
4-octet	(Optional) Configures the 32-bit autonomous system number as a key field.
peer	(Optional) Configures the autonomous system number of the peer network as a nonkey field and enables collecting the value of the autonomous system number of the peer network from the flows.
traffic-index	Configures the Border Gateway Protocol (BGP) source or destination traffic index as a nonkey field and enables collecting the value of the BGP destination traffic index from the flows.
forwarding-status	Configures the forwarding status as a nonkey field and enables collecting the value of the forwarding status of the packet from the flows.
next-hop address	Configures the next-hop address value as a nonkey field and enables collecting information regarding the next hop from the flows. The type of address (IPv4 or IPv6) is determined by the next keyword entered.
ipv4	Specifies that the **next-hop address** value is an IPv4 address.
ipv6	Specifies that the **next-hop address** value is an IPv6 address.
bgp	(Optional) Configures the IP address of the next hop BGP network as a nonkey field and enables collecting the value of the IP address of the BGP next hop network from the flows.
vrf input	Configures the Virtual Routing and Forwarding (VRF) ID for incoming packets as a key field.

Command Default

The routing attributes are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	The **ipv6** keyword was added in Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was modified. The **vrf input** keywords were added in Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS Release XE 3.2S	This command was modified. The **4-octet** keyword was added.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect routing source as [peer]

This command collects the 16-bit autonomous system number based on a lookup of the router's routing table using the source IP address. The optional **peer** keyword provides the expected next network, as opposed to the originating network.

collect routing source as 4-octet [peer 4-octet]

This command collects the 32-bit autonomous system number based on a lookup of the router's routing table using the source IP address. The optional peer keyword provides the expected next network, as opposed to the originating network.

collect routing destination as [peer]

This command collects the 16-bit autonomous system number based on a lookup of the router's routing table using the destination IP address. The optional **peer** keyword provides the expected next network as opposed to the destination network.

collect routing destination as 4-octet [peer 4-octet]

This command collects the 32-bit autonomous system number based on a lookup of the router's routing table using the destination IP address. The **peer** keyword will provide the expected next network as opposed to the destination network.

collect routing destination traffic-index

This command collects the traffic-index field based on the destination autonomous system for this flow. The traffic-index field is a value propagated through BGP.

This command is not supported for IPv6.

collect routing source traffic-index

This command collects the traffic-index field based on the source autonomous system for this flow. The traffic-index field is a value propagated through BGP.

This command is not supported for IPv6.

collect routing forwarding-status

This command collects a field to indicate if the packets were successfully forwarded. The field is in two parts and may be up to 4 bytes in length. For the releases specified in the Command History table, only the status field is used:

```
+-+-+-+-+-+-+-+-+
| S | Reason    |
| t | codes     |
| a | or        |
| t | flags     |
| u |           |
| s |           |
+-+-+-+-+-+-+-+-+
 0 1 2 3 4 5 6 7

Status:
00b=Unknown, 01b = Forwarded, 10b = Dropped, 11b = Consumed
```

collect routing vrf input

This command collects the VRF ID from incoming packets on a router. In the case where VRFs are associated with an interface via methods such as VRF Selection Using Policy Based Routing/Source IP Address, a VRF ID of 0 will be recorded. If a packet arrives on an interface that does not belong to a VRF, a VRF ID of 0 is recorded.

Examples

The following example configures the 16-bit autonomous system number based on a lookup of the router's routing table using the source IP address as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing source as
```

The following example configures the 16-bit autonomous system number based on a lookup of the router's routing table using the destination IP address as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing destination as
```

The following example configures the value in the traffic-index field based on the source autonomous system for a flow as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing source traffic-index
```

The following example configures the forwarding status as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing forwarding-status
```

The following example configures the VRF ID for incoming packets as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing vrf input
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.

collect routing is-multicast

To configure the use of the is-multicast field (indicating that the IPv4 traffic is multicast traffic) as a nonkey field, use the **collect routing is-multicast** command in Flexible NetFlow flow record configuration mode. To disable the use of the is-multicast field as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect routing is-multicast

no collect routing is-multicast

Syntax Description

This command has no arguments or keywords

Command Default

The is-multicast field is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example configures the is-multicast field as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing is-multicast
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect routing multicast replication-factor

To configure the multicast replication factor value for IPv4 traffic as a nonkey field for a Flexible NetFlow flow record, use the **collect routing multicast replication-factor** command in Flexible NetFlow flow record configuration mode. To disable the use of the multicast replication factor value as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect routing multicast replication-factor

no collect routing multicast replication-factor

Syntax Description

This command has no arguments or keywords.

Command Default

The multicast replication factor value is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

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

Examples

The following example configures the multicast replication factor value as a nonkey field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect routing multicast replication-factor
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect timestamp sys-uptime

To configure the system uptime of the first seen or last seen packet in a flow as a nonkey field for a Flexible NetFlow flow record, use the **collect timestamp sys-uptime** command in Flexible NetFlow flow record configuration mode. To disable the use of the first seen or last seen packet in a flow as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect timestamp sys-uptime {**first** | **last**}

no collect timestamp sys-uptime {**first** | **last**}

Syntax Description

first	Configures the system uptime for the time the first packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the first packet was seen from the flows.
last	Configures the system uptime for the time the last packet was seen from the flows as a nonkey field and enables collecting time stamps based on the system uptime for the time the most recent packet was seen from the flows.

Command Default

The system uptime field is not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures time stamps based on the system uptime for the time the first packet was seen from the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect timestamp sys-uptime first
```

The following example configures time stamps based on the system uptime for the time the most recent packet was seen from the flows as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect timestamp sys-uptime last
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect transport

To configure one or more of the transport layer fields as a nonkey field for a Flexible NetFlow flow record, use the **collect transport** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the transport layer fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect transport {**destination-port** | **igmp type** | **source-port**}

no collect transport {**destination-port** | **igmp type** | **source-port**}

Syntax Description

destination-port	Configures the destination port as a nonkey field and enables collecting the value of the destination port from the flows.
igmp type	Configures the Internet Group Management Protocol (IGMP) type as a nonkey field and enables collecting the value of the IGMP type from the flows.
source-port	Configures the source port as a nonkey field and enables collecting the value of the source port from the flows.

Command Default

The transport layer fields are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the transport destination port as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport destination-port
```

The following example configures the transport source port as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport source-port
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect transport icmp ipv4

To configure the internet control message protocol (ICMP) IPv4 type field and the code field as nonkey fields for a Flexible NetFlow flow record, use the **collect transport icmp ipv4** command in Flexible NetFlow flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as nonkey fields for a Flexible NetFlow flow record, use the **no** form of this command.

collect transport icmp ipv4 {**code** | **type**}

no collect transport icmp ipv4 {**code** | **type**}

Syntax Description

code	Configures the ICMP code as a nonkey field and enables collecting the value of the ICMP code from the flow.
type	Configures the ICMP type as a nonkey field and enables collecting the value of the ICMP type from the flow.

Command Default

The ICMP IPv4 type field and the code field are not configured as nonkey fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the ICMP IPv4 code field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport icmp ipv4 code
```

The following example configures the ICMP IPv4 type field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport icmp ipv4 type
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect transport icmp ipv6

To configure the Internet Control Message Protocol (ICMP) IPv6 type field and code field as nonkey fields for a Flexible NetFlow flow record, use the **collect transport icmp ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as nonkey fields for a Flexible NetFlow flow record, use the **no** form of this command.

collect transport icmp ipv6 {**code** | **type**}

no collect transport icmp ipv6 {**code** | **type**}

Syntax Description

code	Configures the ICMP code as a nonkey field and enables collecting the value of the ICMP code from the flow.
type	Configures the ICMP type as a nonkey field and enables collecting the value of the ICMP type from the flow.

Command Default

The ICMP IPv6 type field and code field are not configured as nonkey fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the ICMP IPv6 code field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport icmp ipv6 code
```

The following example configures the ICMP IPv6 type field as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport icmp ipv6 type
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect transport tcp

To configure one or more of the TCP fields as a nonkey field for a Flexible NetFlow flow record, use the **collect transport tcp** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the TCP fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect transport tcp {**acknowledgement-number** | **destination-port** | **flags** {[**ack**] | [**cwr**] | [**ece**] | [**fin**] | [**psh**] | [**rst**] | [**syn**] | [**urg**]} | **header-length** | **sequence-number** | **source-port** | **urgent-pointer** | **window-size**}

no collect transport tcp {**acknowledgement-number** | **destination-port** | **flags** {[**ack**] [**cwr**] [**ece**] [**fin**] [**psh**] [**rst**] [**syn**] [**urg**]} | **header-length** | **sequence-number** | **source-port** | **urgent-pointer** | **window-size**}

Syntax Description

acknowledgement-number	Configures the TCP acknowledgement number as a nonkey field and enables collecting the value of the TCP acknowledgement number from the flow.
destination-port	Configures the TCP destination port as a nonkey field and enables collecting the value of the TCP destination port from the flow.
flags	Configures one or more of the TCP flags as a nonkey field and enables collecting the values from the flow.
ack	(Optional) Configures the TCP acknowledgement flag as a nonkey field.
cwr	(Optional) Configures the TCP congestion window reduced flag as a nonkey field.
ece	(Optional) Configures the TCP Explicit Congestion Notification echo (ECE) flag as a nonkey field.
fin	(Optional) Configures the TCP finish flag as a nonkey field.
psh	(Optional) Configures the TCP push flag as a nonkey field.
rst	(Optional) Configures the TCP reset flag as a nonkey field.
syn	(Optional) Configures the TCP synchronize flag as a nonkey field.
urg	(Optional) Configures the TCP urgent flag as a nonkey field.
header-length	Configures the TCP header length (in 32-bit words) as a nonkey field and enables collecting the value of the TCP header length from the flow.
sequence-number	Configures the TCP sequence number as a nonkey field and enables collecting the value of the TCP sequence number from the flow.
source-port	Configures the TCP source port as a nonkey field and enables collecting the value of the TCP source port from the flow.
urgent-pointer	Configures the TCP urgent pointer as a nonkey field and enables collecting the value of the TCP urgent pointer from the flow.
window-size	Configures the TCP window size as a nonkey field and enables collecting the value of the TCP window size from the flow.

Command Default

The TCP fields are not configured as a nonkey field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

collect transport tcp flags ece

For more information about ECN echo, refer to RFC 3168 *The Addition of Explicit Congestion Notification (ECN) to IP*, at the following URL: http://www.rfc.net/rfc3168.html.

Examples

The following example configures the TCP acknowledgement number as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport tcp acknowledgement-number
```

The following example configures the TCP source port as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport tcp source-port
```

The following example configures the TCP acknowledgement flag as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport tcp flags ack
```

The following example configures the TCP finish flag as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport tcp flags fin
```

The following example configures the TCP reset flag as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport tcp flags rst
```

Related Commands

Command	Description
flow record	Creates a flow record.

collect transport udp

To configure one or more of the user datagram protocol UDP fields as a nonkey field for a Flexible NetFlow flow record, use the **collect transport udp** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the UDP fields as a nonkey field for a Flexible NetFlow flow record, use the **no** form of this command.

collect transport udp {**destination-port** | **message-length** | **source-port**}}

no collect transport udp {**destination-port** | **message-length** | **source-port**}}

Syntax Description

destination-port	Configures the UDP destination port as a nonkey field and enables collecting the value of the UDP destination port fields from the flow.
message-length	Configures the UDP message length as a nonkey field and enables collecting the value of the UDP message length fields from the flow.
source-port	Configures the UDP source port as a nonkey field and enables collecting the value of the UDP source port fields from the flow.

Command Default

The UDP fields are not configured as nonkey fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The Flexible NetFlow collect commands are used to configure nonkey fields for the flow monitor record and to enable capturing the values in the fields for the flow created with the record. The values in nonkey fields are added to flows to provide additional information about the traffic in the flows. A change in the value of a nonkey field does not create a new flow. In most cases the values for nonkey fields are taken from only the first packet in the flow.

Examples

The following example configures the UDP destination port as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport udp destination-port
```

The following example configures the UDP message length as a nonkey field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport udp message-length
```

The following example configures the UDP source port as a non-key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# collect transport udp source-port
```

Related Commands

Command	Description
flow record	Creates a flow record.

debug flow exporter

To enable debugging output for Flexible NetFlow flow exporters, use the **debug flow exporter** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug flow exporter [[**name**] *exporter-name*] [**error**] [**event**] [**packets** *number*]

no debug flow exporter [[**name**] *exporter-name*] [**error**] [**event**] [**packets** *number*]

Syntax Description

name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) The name of a flow exporter that was previously configured.
error	(Optional) Enables debugging for flow exporter errors.
event	(Optional) Enables debugging for flow exporter events.
packets	(Optional) Enables packet-level debugging for flow exporters.
number	(Optional) the number of packets to debug for packet-level debugging of flow exporters. Range: 1 to 65535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example indicates that a flow exporter packet has been queued for process send:

```
Router# debug flow exporter

May 21 21:29:12.603: FLOW EXP: Packet queued for process send
```

Related Commands

Command	Description
clear flow exporter	Clears the Flexible NetFlow statistics for exporters.

debug flow monitor

To enable debugging output for Flexible NetFlow flow monitors, use the **debug flow monitor** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug flow monitor [**error**] [[**name**] *monitor-name* [**cache**] [**error**] [**packets** *packets*]]

no debug flow monitor [**error**] [[**name**] *monitor-name* [**cache**] [**error**] [**packets** *packets*]]

Syntax Description

error	(Optional) Enables debugging for flow monitor errors.
name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) The name of a flow monitor that was previously configured.
cache	(Optional) Enables debugging for the flow monitor cache.
packets	(Optional) Enables packet-level debugging for flow monitors.
packets	(Optional) The number of packets to debug for packet-level debugging of flow monitors. Range: 1 to 65535.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example shows that the cache for FLOW-MONITOR-1 was deleted:

```
Router# debug flow monitor FLOW-MONITOR-1 cache

May 21 21:53:02.839: FLOW MON:  'FLOW-MONITOR-1' deleted cache
```

Related Commands

Command	Description
clear flow monitor	Clears the Flexible NetFlow flow monitor.

debug flow record

To enable debugging output for Flexible NetFlow flow records, use the **debug flow record** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug flow record [[**name**] *record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**] | **netflow-v5** | **options** {**exporter-statistics** | **interface-table** | **sampler-table** | **vrf-id-name-table**}]

no debug flow record [[**name**] *record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**] | **netflow-v5** | **options** {{**exporter-statistics** | **interface-table** | **sampler-table** | **vrf-id-name-table**}]

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

debug flow record [[**name**] *record-name* | **netflow-v5** | **options** {**exporter-statistics** | **interface-table** | **sampler-table** | **vrf-id-name-table**} | **platform-original** {**ipv4** | **ipv6**} *record* [**detailed** | **error**]]

no debug flow record [[**name**] *record-name* | **netflow-v5** | **options** {**exporter-statistics** | **interface-table** | **sampler-table** | **vrf-id-name-table**} | **platform-original {ipv4 | ipv6}** *record* [**detailed** | **error**]]

Syntax Description

name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.
netflow-original	(Optional) Traditional IPv4 input NetFlow with origin autonomous systems.
netflow {**ipv4** | **ipv6**} *record*	(Optional) The name of the NetFlow predefined record. See Table 8.
peer	(Optional) Includes peer information for the NetFlow predefined records that support the peer keyword. **Note** The peer keyword is not supported for every type of NetFlow predefined record. See Table 8.
options	(Optional) Includes information on other flow record options.
exporter-statistics	(Optional) Includes information on the flow exporter statistics.
interface-table	(Optional) Includes information on the interface tables.
sampler-table	(Optional) Includes information on the sampler tables.
vrf-id-name-table	(Optional) Includes information on the virtual routing and forwarding (VRF) ID-to-name tables.
platform-original ipv4 *record*	Configures the flow monitor to use one of the predefined IPv4 records.
platform-original ipv6*record*	Configures the flow monitor to use one of the predefined IPv6 records.
detailed	(Optional) Displays detailed information.
error	(Optional) Displays errors only.

Command Modes Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	The **ipv6** keyword was added in Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was modified. The **vrf-id-name-table** keyword was added in Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **netflow-original**, **netflow ipv4**, **netflow ipv6**, and **peer** keywords were removed in Cisco IOS Release 12.2(50)SY. The **platform-original ipv4** and **platform-original ipv6** keywords were added.

Usage Guidelines Table 8 describes the keywords and descriptions for the *record* argument.

Table 8 Keywords and Descriptions for the record Argument

Keyword	Description	IPv4 Support	IPv6 Support
as	Autonomous system record.	Yes	Yes
as-tos	Autonomous system and type of service (ToS) record.	Yes	—
bgp-nexthop-tos	BGP next-hop and ToS record.	Yes	—
bgp-nexthop	BGP next-hop record.	—	Yes
destination	Original 12.2(50)SY platform IPv4/IPv6 destination record.	Yes	Yes
destination-prefix	Destination prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
destination-prefix-tos	Destination prefix and ToS record.	Yes	—
destination-source	Original 12.2(50)SY platform IPv4/IPv6 destination-source record.	Yes	Yes
full	Original 12.2(50)SY platform IPv4/IPv6 full record.	Yes	Yes
interface-destination	Original 12.2(50)SY platform IPv4/IPv6 interface-destination record.	Yes	Yes
interface-destination-source	Original 12.2(50)SY platform IPv4/IPv6 interface-destination-source record.	Yes	Yes
interface-full	Original 12.2(50)SY platform IPv4/IPv6 interface-full record.	Yes	Yes

Table 8 Keywords and Descriptions for the record Argument (continued)

interface-source	Original 12.2(50)SY platform IPv4/IPv6 interface-source only record.	Yes	Yes
original-input	Traditional IPv4 input NetFlow.	Yes	Yes
original-output	Traditional IPv4 output NetFlow.	Yes	Yes
prefix	Source and destination prefixes record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
prefix-port	Prefix port record. **Note** The **peer** keyword is not available for this record.	Yes	—
prefix-tos	Prefix ToS record.	Yes	—
protocol-port	Protocol ports record. **Note** The **peer** keyword is not available for this record.	Yes	Yes
protocol-port-tos	Protocol port and ToS record. **Note** The **peer** keyword is not available for this record.	Yes	—
source	Original 12.2(50)SY platform IPv4/IPv6 source only record.	Yes	Yes
source-prefix	Source autonomous system and prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
source-prefix-tos	Source prefix and ToS record.	Yes	—

Examples

The following example enables debugging for the flow record:

```
Router# debug flow record FLOW-record-1
```

Related Commands

Command	Description
flow record	Create a Flexible NetFlow flow record.

debug sampler

To enable debugging output for Flexible NetFlow samplers, use the **debug sampler** command in privileged EXEC mode. To disable debugging output, use the **no** form of this command.

debug sampler [**detailed** | **error** | [**name**] *sampler-name* [{**detailed** | **error** | **sampling** *samples*}]]

no debug sampler [**detailed** | **error** | [**name**] *sampler-name* [{**detailed** | **error** | **sampling** *samples*}]]

Syntax Description

detailed	(Optional) Enables detailed debugging for sampler elements.
error	(Optional) Enables debugging for sampler errors.
name	(Optional) Specifies the name of a sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.
sampling *samples*	(Optional) Enables debugging for sampling and specifies the number of samples to debug.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following sample output shows that the debug process has obtained the ID for the sampler named SAMPLER-1:

```
Router# debug sampler detailed

*Oct 28 04:14:30.883: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et1/0,O)
get ID succeeded:1
*Oct 28 04:14:30.971: Sampler: Sampler(SAMPLER-1: flow monitor FLOW-MONITOR-1 (ip,Et0/0,I)
get ID succeeded:1
```

Related Commands

Command	Description
clear sampler	Clears the Flexible NetFlow sampler statistics.

default (Flexible NetFlow)

To configure the default values for a Flexible NetFlow (FNF) flow exporter, use the **default** command in Flexible NetFlow flow exporter configuration mode.

default {**description** | **destination** | **dscp** | **export-protocol** | **option** {**application-table** | **exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} | **output-features** | **source** | **template data timeout** | **transport** | **ttl**}

Syntax Description

description	Provides a description for the flow exporter.
destination	Configures the export destination.
dscp	Configures optional Differentiated Services Code Point (DSCP) values.
export-protocol	Configures the export protocol version.
option	Selects the option for exporting.
application-table	Selects the application table option.
exporter-stats	Selects the exporter statistics option.
interface-table	Selects the interface SNMP-index-to-name table option.
sampler-table	Selects the export sampler option.
vrf-table	Selects the VRF ID-to-name table option.
output-features	Sends export packets via the Cisco IOS output feature path.
source	Configures the originating interface.
template	Configures the flow exporter template.
data	Configure the flow exporter data.
timeout	Resends data based on a timeout.
transport	Configures the transport protocol.
ttl	Configures optional time-to-live (TTL) or hop limit.

Command Modes

FNF flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was implemented on Cisco 7200 series routers.
12.2(33)SRE	This command was implemented on the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Use the **default** command to configure the default values for an FNF flow exporter. The flow exporter information is needed to export the data metrics to a specified destination, port number, and so on.

Examples

The following example shows how to set the default destination for an FNF flow exporter:

```
Router(config)# flow exporter e1
Router(config-flow-exporter)# default destination
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

description (Flexible NetFlow)

To configure a description for a Flexible NetFlow flow sampler, flow monitor, flow exporter, or flow record, use the **description** command in the appropriate configuration mode. To remove a description, use the **no** form of this command.

description *description*

no description

Syntax Description

description	Text string that describes the flow sampler, flow monitor, flow exporter, or flow record.

Command Default

The default description for a Flexible NetFlow flow sampler, flow monitor, flow exporter, or flow record is "User defined."

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)
Flexible NetFlow flow monitor configuration (config-flow-monitor)
Flexible NetFlow flow record configuration (config-flow-record)
Flexible NetFlow sampler configuration (config-sampler)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following example configures a description for a flow monitor:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# description Monitors traffic to 172.16.100.0 255.255.255.0
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.
flow record	Creates a flow record.
sampler	Creates a flow sampler.

destination

To configure an export destination for a Flexible NetFlow flow exporter, use the **destination** command in Flexible NetFlow flow exporter configuration mode. To remove an export destination for a Flexible NetFlow flow exporter, use the **no** form of this command.

destination {{*ip-address* | *hostname*} | **vrf** *vrf-name*}

no destination

Syntax Description

ip-address	IP address of the workstation to which you want to send the NetFlow information.
hostname	Hostname of the device to which you want to send the NetFlow information.
vrf *vrf-name*	Specifies that the export data packets are to be sent to the named Virtual Private Network (VPN) routing and forwarding (VRF) instance for routing to the destination, instead of to the global routing table.

Command Default An export destination is not configured.

Command Modes Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines Each flow exporter can have only one destination address or hostname.

When you configure a hostname instead of the IP address for the device, the hostname is resolved immediately and the IP address is stored in the running configuration. If the hostname-to-IP-address mapping that was used for the original domain name system (DNS) name resolution changes dynamically on the DNS server, the router does not detect this, and the exported data continues to be sent to the original IP address, resulting in a loss of data. Resolving the hostname immediately is a prerequisite of the export protocol, to ensure that the templates and options arrive before the data

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

```
Router(config)# flow exporter FLOW-EXPORTER-1
```

```
Router(config-flow-exporter)# destination 10.0.0.4
```

The following example shows how to configure the networking device to export the Flexible NetFlow cache entry to a destination system using a VRF named VRF-1:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# destination 172.16.10.2 vrf VRF-1
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

dscp (Flexible NetFlow)

To configure a differentiated services code point (DSCP) value for Flexible NetFlow flow exporter datagrams, use the **dscp** command in Flexible NetFlow flow exporter configuration mode. To remove a DSCP value for Flexible NetFlow flow exporter datagrams, use the **no** form of this command.

dscp *dscp*

no dscp

Syntax Description

dscp	The DSCP to be used in the DSCP field in exported datagrams. Range: 0 to 63. Default 0.

Command Default

The differentiated services code point (DSCP) value is 0.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example sets 22 as the value of the DSCP field in exported datagrams:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# dscp 22
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

execute (Flexible NetFlow)

To execute a shell function for a Flexible NetFlow (FNF) flow exporter, use the **execute** command in FNF flow exporter configuration mode.

execute *name* [*description...*]

Syntax Description

name	Name of the shell function to execute.
description	(Optional) Description of the shell function parameter values. You can enter multiple descriptions.

Command Default No shell function is executed.

Command Modes FNF flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
15.4(M)	This command was introduced.

Examples The following example shows how to execute a shell function, function1:

```
Router(config)# flow exporter e1
Router(config-flow-exporter)# execute function1
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

exporter

To configure a flow exporter for a Flexible NetFlow flow monitor, use the **exporter** command in Flexible NetFlow flow monitor configuration mode. To remove a flow exporter for a Flexible NetFlow flow monitor, use the **no** form of this command.

exporter *exporter-name*

no exporter *exporter-name*

Syntax Description

exporter-name	Name of a flow exporter that was previously configured.

Command Default

An exporter is not configured.

Command Modes

Flexible NetFlow flow monitor configuration (config-flow-monitor)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

You must have already created a flow exporter by using the **flow exporter** command before you can apply the flow exporter to a flow monitor with the **exporter** command.

Examples

The following example configures an exporter for a flow monitor:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# exporter EXPORTER-1
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.

export-protocol

To configure the export protocol for a Flexible NetFlow exporter, use the **export-protocol** command in Flexible NetFlow flow exporter configuration mode. To restore the use of the default export protocol for a Flexible NetFlow exporter, use the **no** form of this command.

export-protocol {**netflow-v5** | **netflow-v9**}

no export-protocol

Syntax Description

netflow-v5	Configures NetFlow Version 5 export as the export protocol.
netflow-v9	Configures NetFlow Version 9 export as the export protocol.

Command Default

NetFlow Version 9 export is used as the export protocol for a Flexible NetFlow exporter.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The NetFlow Version 5 export protocol is supported only for flow monitors that use the Flexible NetFlow predefined records.

Examples

The following example configures NetFlow Version 5 export as the export protocol for a Flexible NetFlow exporter:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# export-protocol netflow-v5
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter

flow exporter

To create a Flexible NetFlow flow exporter, or to modify an existing Flexible NetFlow flow exporter, and enter Flexible NetFlow flow exporter configuration mode, use the **flow exporter** command in global configuration mode. To remove a Flexible NetFlow flow exporter, use the **no** form of this command.

flow exporter *exporter-name*

no flow exporter *exporter-name*

Syntax Description

exporter-name	Name of the flow exporter that is being created or modified.

Command Default

Flexible NetFlow flow exporters are not present in the configuration.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

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

Examples

The following example creates a flow exporter named FLOW-EXPORTER-1 and enters Flexible NetFlow flow exporter configuration mode:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)#
```

Related Commands

Command	Description
clear flow exporter	Clears the statistics for flow exporters.
debug flow exporter	Enables debugging output for flow exporters.

flow hardware

To configure Flexible NetFlow hardware parameters, use the **flow hardware** command in global configuration mode. To unconfigure Flexible NetFlow hardware parameters, use the **no** form of this command.

flow hardware [**egress** | **export threshold** *total-cpu-threshold-percentage* [**linecard** *linecard-threshold-percentage*] | **usage notify** {**input** | **output**} [*table-threshold-percentage seconds*]]

no flow hardware [**egress** | **export threshold** | **usage notify** {**input** | **output**}]

Syntax Description

egress	(Optional) Configures hardware egress NetFlow parameters.
export threshold	(Optional) Configures export threshold parameters.
total-cpu-threshold-percentage	(Optional) The total CPU utilization threshold percentage.
linecard-threshold-percentage	(Optional) The line-card CPU utilization threshold percentage.
usage notify input	(Optional) Configures NetFlow table utilization parameters for traffic that the router is receiving.
usage notify output	(Optional) Configures NetFlow table utilization parameters for traffic that the router is transmitting.
table-threshold-percentage	(Optional) The NetFlow table utilization threshold percentage.
seconds	(Optional) The NetFlow table utilization time interval, in seconds.

Command Default

Flexible NetFlow hardware parameters are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Flow exporters export the data in the flow monitor cache to a remote system, such as a server running Flexible NetFlow collector, for analysis and storage. The number and complexity of flow records to be exported is the prime cause of CPU use in NetFlow. The CPU Friendly NetFlow Export feature (also known as Yielding NetFlow Data Export, or Yielding NDE) monitors CPU use for both the supervisor and line cards according to user-configured thresholds and dynamically adjusts the rate of export as needed.

A system reload is needed for egress NetFlow mode change. If egress NetFlow is disabled and you attempt to configure any feature that requires an egress NetFlow, an error message will be displayed indicating that egress NetFlow must be enabled for this feature to function. You should enable egress NetFlow, reload the system, and reconfigure the feature.

Examples

The following example configures CPU utilization thresholds for Flexible NetFlow flow export:

```
Router(config)# flow hardware export threshold 25 linecard 25
```

Related Commands

Command	Description
show platform flow	Displays Flexible NetFlow platform parameter information.

flow monitor

To create a Flexible NetFlow flow monitor, or to modify an existing Flexible NetFlow flow monitor, and enter Flexible NetFlow flow monitor configuration mode, use the **flow monitor** command in global configuration mode. To remove a Flexible NetFlow flow monitor, use the **no** form of this command.

flow monitor *monitor-name*

no flow monitor *monitor-name*

Syntax Description

monitor-name	Name of the flow monitor that is being created or modified.

Command Default

Flexible NetFlow Flow monitors are not present in the configuration.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

Flow monitors are the Flexible NetFlow component that is applied to interfaces to perform network traffic monitoring. Flow monitors consist of a record and a cache. You add the record to the flow monitor after you create the flow monitor. The flow monitor cache is automatically created at the time the flow monitor is applied to the first interface. Flow data is collected from the network traffic during the monitoring process based on the key and nonkey fields in the record, which is configured for the flow monitor and stored in the flow monitor cache.

Examples

The following example creates a flow monitor named FLOW-MONITOR-1 and enters Flexible NetFlow flow monitor configuration mode:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)#
```

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor.
debug flow monitor	Enables debugging output for flow monitors.

flow platform

To configure Flexible NetFlow platform parameters, use the **flow platform** command in global configuration mode. To unconfigure Flexible NetFlow platform parameters, use the **no** form of this command.

flow platform cache timeout {**active** *seconds* | **fast** [**threshold** *count*] [**time** *seconds*] | **inactive** *seconds*}]

no flow platform cache timeout {**active | fast | inactive**}

Syntax Description

cache timeout	Configures platform flow cache timeout parameters.
active *seconds*	Configures the active flow timeout, in seconds.
fast threshold *count*	Configures the fast aging threshold packet count.
fast time *seconds*	Configures the active flow timeout, in seconds.
inactive *seconds*	Configures the inactive flow timeout, in seconds.

Command Default

Flexible NetFlow platform parameters are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Usage Guidelines

Hardware Flexible NetFlow table space is a valuable resource and needs to managed. Older flows need to be identified as quickly as possible and aged out (purged) to make way ultimately for new, more active flows. The older the Flexible NetFlow data, the less it is useful for real-time monitoring of traffic.

The common aging schemes are:

- Inactive/normal aging: age out flows that have had no activity in the preceding configured time.
- Active/long aging: age out flows that have lived for longer than the configured long aging period.
- Fast aging: age out flows that had some bursty activity followed by inactivity, for example, Domain Name Service (DNS) resolution requests. This aging scheme is a function of the creation time of a flow and the packet count.
- TCP session aging: age out flows pertaining to terminated TCP sessions.
- Aggressive aging: age out flows with user-configured aggressive aging inactivity timeout when table space utilization exceeds a user-configured threshold.

In addition to purging older entries, NetFlow entries need to be purged in response to certain configuration and network topology changes; for example, interface or link going out of service.

Examples

The following example configures the active platform flow cache timeout:

```
Router(config)# flow platform cache timeout active 60
```

Related Commands

Command	Description
show platform flow	Displays Flexible NetFlow platform parameter information.

flow record

To create a Flexible NetFlow flow record, or to modify an existing Flexible NetFlow flow record, and enter Flexible NetFlow flow record configuration mode, use the **flow record** command in global configuration mode. To remove a Flexible NetFlow flow record, use the **no** form of this command.

flow record *record-name*

no flow record *record-name*

Syntax Description

record-name	Name of the flow record that is being created or modified.

Command Default

A flow record is not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Flexible NetFlow uses key and nonkey fields just as original NetFlow does to create and populate flows in a cache. In Flexible NetFlow a combination of key and nonkey fields is called a *record*. Original NetFlow and Flexible NetFlow both use the values in key fields in IP datagrams, such as the IP source or destination address and the source or destination transport protocol port, as the criteria for determining when a new flow must be created in the cache while network traffic is being monitored. A *flow* is defined as a stream of packets between a given source and a given destination. New flows are created whenever a packet that has a unique value in one of the key fields is analyzed.

Examples

The following example creates a flow record named FLOW-RECORD-1, and enters Flexible NetFlow flow record configuration mode:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)#
```

Related Commands

Command	Description
show flow record	Displays flow record status and statistics.

granularity

To configure the granularity of sampling for a Flexible NetFlow sampler, use the **granularity** command in Flexible NetFlow sampler configuration mode. To return the sampling configuration to the default value, use the **no** form of this command.

granularity {**connection** | **packet**}

no granularity

Syntax Description

connection	Specifies that the sampling is done by connection.
packet	Specifies that the sampling is done by packet.

Command Default

Sampling is done by packet.

Command Modes

Flexible NetFlow sampler configuration (config-sampler)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

To use this command, you must configure the **match application name** command for the flow record.

Examples

The following example shows how to configure the granularity of the sampling to be by connection for a Flexible NetFlow sampler:

```
Router(config)# sampler SAMPLER-2
Router(config-sampler)# granularity connection
Router(config-sampler)# mode random 1 out-of 20
```

Related Commands

Command	Description
sampler	Configures a Flexible NetFlow sampler, and enters Flexible NetFlow sampler configuration mode.

ip flow monitor

To enable a Flexible NetFlow flow monitor for IPv4 traffic that the router is receiving or forwarding, use the **ip flow monitor** command in interface configuration mode or subinterface configuration mode. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

ip flow monitor *monitor-name* [**sampler** *sampler-name*] [**multicast** | **unicast**] {**input** | **output**}

no ip flow monitor *monitor-name* [**sampler** *sampler-name*] [**multicast** | **unicast**] {**input** | **output**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

ip flow monitor *monitor-name* [**sampler** *sampler-name*] [**layer2-switched** | **multicast** | **unicast**] {**input** | **output**}

no ip flow monitor *monitor-name* [**sampler** *sampler-name*] [**layer2-switched** | **multicast** | **unicast**] {**input** | **output**}

Syntax Description

monitor-name	Name of a flow monitor that was previously configured.
sampler *sampler-name*	(Optional) Enables a flow sampler for this flow monitor using the name of a sampler that was previously configured.
layer2-switched	(Optional) Applies the flow monitor for Layer 2-switched traffic only.
multicast	(Optional) Applies the flow monitor for multicast traffic only.
unicast	(Optional) Applies the flow monitor for unicast traffic only.
input	Monitors traffic that the router is receiving on the interface.
output	Monitors traffic that the router is transmitting on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

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

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(22)T	The **unicast** and **multicast** keywords were added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **layer2-switched** keyword was added in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

You must have already created a flow monitor by using the **flow monitor** command before you can apply the flow monitor to an interface with the **ip flow monitor** command to enable traffic monitoring with Flexible NetFlow.

ip flow monitor sampler

When a sampler is added to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on an interface. You must remove the flow monitor from the interface prior to enabling the same flow monitor with a sampler. See the "Examples" section for more information.

Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 10 sampler it is expected that the packet and byte counters will have to be multiplied by 10.

Multicast Traffic and Unicast Traffic

In Cisco IOS Release 12.4(22)T and later releases, the default behavior of the **ip flow monitor** command is to analyze unicast *and* multicast traffic. If you need to monitor only unicast traffic, use the **unicast** keyword. If you need to monitor only multicast traffic, use the **multicast** keyword.

Examples

The following example enables a flow monitor for monitoring input traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring output traffic on a subinterface:

```
Router(config)# interface ethernet0/0.1
Router(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables a flow monitor for monitoring only multicast input traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 multicast input
```

The following example enables a flow monitor for monitoring only unicast output traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 unicast output
```

The following example enables the same flow monitor on the same interface for monitoring input and output traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
Router(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables two different flow monitors on the same interface for monitoring input and output traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
Router(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
Router(config-if)# exit
Router(config)# interface ethernet1/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 output
```

The following example enables two different flow monitors on two different interfaces for monitoring input and output traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
Router(config-if)# exit
Router(config)# interface ethernet1/0
Router(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

The following example enables a flow monitor for monitoring input traffic, with a sampler to limit the input packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example enables a flow monitor for monitoring output traffic, with a sampler to limit the output packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 output
```

The following example enables two different flow monitors for monitoring input and output traffic, with a sampler on the flow monitor that is monitoring input traffic to limit the input packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
Router(config-if)# ip flow monitor FLOW-MONITOR-2 output
```

The following example enables two different flow monitors for monitoring input and output traffic, with a sampler on the flow monitor that is monitoring output traffic to limit the output packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-2 input
Router(config-if)# ip flow monitor FLOW-MONITOR-2 sampler SAMPLER-2 output
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 input
Router(config-if)# ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# no ip flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
Router(config-if)# ip flow monitor FLOW-MONITOR-1 input
```

Related Commands

Command	Description
flow monitor	Creates a flow monitor.
sampler	Creates a flow sampler.

ipv6 flow monitor

To enable a Flexible NetFlow flow monitor for IPv6 traffic that the router is receiving or forwarding, use the **ipv6 flow monitor** command in interface configuration mode or subinterface configuration mode. To disable a Flexible NetFlow flow monitor, use the **no** form of this command.

ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] [**multicast** | **unicast**] {**input** | **output**}

no ipv6 flow monitor *monitor-name* [**sampler** *sampler-name*] [**multicast** | **unicast**] {**input** | **output**}

Syntax Description

monitor-name	Name of a flow monitor that was previously configured.
sampler *sampler-name*	(Optional) Enables a flow sampler for this flow monitor using the name of a sampler that was previously configured.
multicast	(Optional) Applies the flow monitor for multicast traffic only.
unicast	(Optional) Applies the flow monitor for unicast traffic only.
input	Monitors traffic that the router is receiving on the interface.
output	Monitors traffic that the router is transmitting on the interface.

Command Default

A flow monitor is not enabled.

Command Modes

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

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.4(22)T	The **unicast** and **multicast** keywords were added.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

You must have already created a flow monitor by using the **flow monitor** command before you can apply the flow monitor to an interface with the **ipv6 flow monitor** command to enable traffic monitoring with Flexible NetFlow.

ipv6 flow monitor sampler

When a sampler is added to a flow monitor, only packets that are selected by the named sampler will be entered into the cache to form flows. Each use of a sampler causes separate statistics to be stored for that usage.

You cannot add a sampler to a flow monitor after the flow monitor has been enabled on an interface. You must remove the flow monitor from the interface prior to enabling the same flow monitor with a sampler. See the “Examples” section for more information.

Note The statistics for each flow must be scaled to give the expected true usage. For example, with a 1 in 10 sampler it is expected that the packet and byte counters will have to be multiplied by 10.

Multicast Traffic and Unicast Traffic

In Cisco IOS Release 12.4(22)T and later releases, the default behavior of the **ip flow monitor** command is to analyze unicast *and* multicast traffic. If you need to monitor only unicast traffic, use the **unicast** keyword. If you need to monitor only multicast traffic, use the **multicast** keyword.

Examples

The following example enables a flow monitor for monitoring input IPv6 traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

The following example enables a flow monitor for monitoring output IPv6 traffic on a subinterface:

```
Router(config)# interface ethernet0/0.1
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

The following example enables a flow monitor for monitoring only multicast input traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 multicast input
```

The following example enables a flow monitor for monitoring only unicast output traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 unicast output
```

The following example enables the same flow monitor on the same interface for monitoring input and output IPv6 traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

The following example enables two different flow monitors on the same interface for monitoring input and output IPv6 traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output
```

The following example enables the same flow monitor on two different interfaces for monitoring input and output IPv6 traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Router(config-if)# exit
Router(config)# interface ethernet1/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 output
```

The following example enables two different flow monitors on two different interfaces for monitoring input and output IPv6 traffic:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
Router(config-if)# exit
Router(config)# interface ethernet1/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output
```

The following example enables a flow monitor for monitoring input IPv6 traffic, with a sampler to limit the input packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
```

The following example enables a flow monitor for monitoring output IPv6 traffic, with a sampler to limit the output packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 output
```

The following example enables two different flow monitors for monitoring input and output IPv6 traffic, with a sampler on the flow monitor that is monitoring input IPv6 traffic to limit the input packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-1 input
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 output
```

The following example enables two different flow monitors for monitoring input and output IPv6 traffic, with a sampler on the flow monitor that is monitoring output IPv6 traffic to limit the output packets that are sampled:

```
Router(config)# interface ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 input
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-2 sampler SAMPLER-2 output
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in full mode and cannot be
enabled with a sampler.
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 input
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
% Flow Monitor: Flow Monitor 'FLOW-MONITOR-1' is already on in sampled mode and cannot be
enabled in full mode.
```

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

```
Router(config)# interface Ethernet0/0
Router(config-if)# no ipv6 flow monitor FLOW-MONITOR-1 sampler SAMPLER-2 input
Router(config-if)# ipv6 flow monitor FLOW-MONITOR-1 input
```

Related Commands

Command	Description
flow monitor	Creates a flow monitor.
sampler	Creates a flow sampler.

match application name

To configure the use of the application name as a key field for a Flexible NetFlow flow record, use the **match application name** command in Flexible NetFlow flow record configuration mode. To disable the use of the application name as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match application name [**account-on-resolution**]

no match application name [**account-on-resolution**]

Syntax Description

account-on-resolution	Specifies that an accurate accounting for the beginning of the flow is provided.

Command Default

The application name is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
15.0(1)M	This command was introduced.
Cisco IOS XE Release 3.4S	This command was modified. The **account-on-resolution** keyword was added.

Usage Guidelines

When the **account-on-resolution** keyword is used, the system temporarily stores the record data until the application is resolved and then it combines the data with the created flow.

Examples

The following example shows how to configure the application name as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match application name
```

Related Commands

Command	Description
collect application name	Configures the use of application name as a nonkey field for a Flexible NetFlow flow record.
flow record	Creates a flow record for Flexible NetFlow, and enters Flexible NetFlow flow record configuration mode.

match connection transaction-id

To configure the transaction ID as a key field for a flow record, use the **match connection transaction-id** command in flow record configuration mode. To disable the use of a transaction ID field as a key field for a flow record, use the **no** form of this command.

match connection transaction-id

no match connection transaction-id

Syntax Description

This command has no arguments or keywords.

Command Default

The transaction ID is not configured as a key field.

Command Modes

Flow record configuration (config-flow-record)

Command History

Release	Modification
Cisco IOS XE Release 3.4S	This command was introduced.

Usage Guidelines

To use this command, you must configure the **match connection transaction id** command and the **match application name** command for the flow record.

The transaction ID identifies a transaction within a connection, for protocols where multiple transactions are used. A transaction is a meaningful exchange of application data between two network devices or a client and server.

A transaction ID is assigned the first time a flow is reported, so that later reports for the same flow will have the same transaction ID. A different transaction ID is used for each concurrent transaction within a TCP or UDP connection. Two flows can receive the same transaction ID if they are not running concurrently. The identifiers are randomly assigned and are not required to be sequential.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example shows how to configure the transaction ID as a key field:

```
Router(config)# flow record RECORD-4
Router(config-flow-record)# match connection transaction-id
```

Related Commands

Command	Description
flow record	Creates a flow record.

match datalink dot1q vlan

To configure the 802.1Q (dot1q) VLAN value as a key field for a Flexible NetFlow flow record, use the **match datalink dot1q vlan** command in Flexible NetFlow flow record configuration mode. To disable the use of the 802.1Q VLAN value as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match datalink dot1q vlan {**input** | **output**}

no match datalink dot1q vlan {**input** | **output**}

Syntax Description

input	Configures the VLAN ID of traffic being received by the router as a key field.
output	Configures the VLAN ID of traffic being transmitted by the router as a key field.

Command Default

The 802.1Q VLAN ID is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

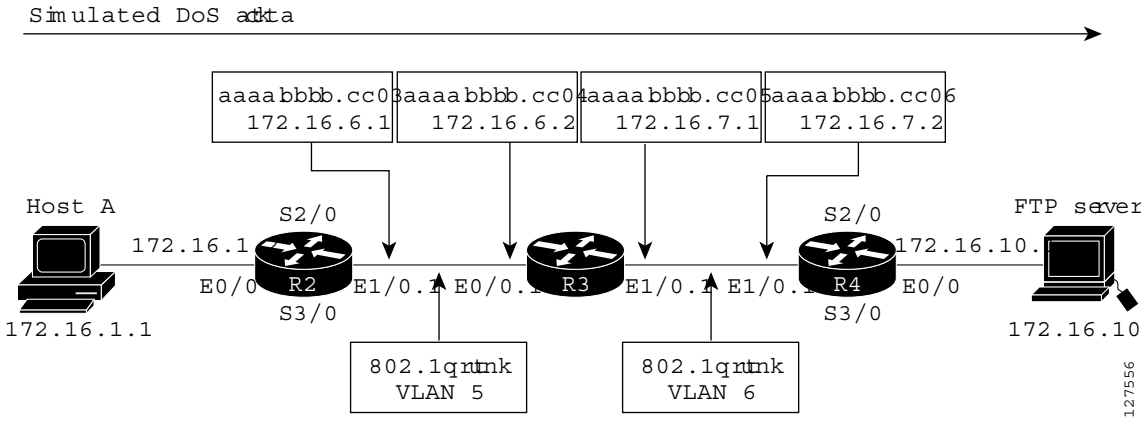
Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The **input** and **output** keywords of the **match datalink dot1q vlan** command are used to specify the observation point that is used by the **match datalink dot1q vlan** command to create flows based on the unique 802.1q VLAN IDs in the network traffic. For example, when you configure a flow record with the **match datalink dot1q vlan input** command to monitor the simulated denial of service (DoS) attack in Figure 3 and apply the flow monitor to which the flow record is assigned in either input (ingress) mode on interface Ethernet 0/0.1 on R3 or output (egress) mode on interface Ethernet 1/0.1 on R3, the observation point is always Ethernet 0/0.1 on R3. The 802.1q VLAN ID that is used as a key field is 5.

Figure 3 Simulated DoS Attack



The observation point of **match** commands that do not have the input and/or output keywords is always the interface to which the flow monitor that contains the flow record with the **match** commands is applied.

Examples

The following example configures the 802.1Q VLAN ID of traffic being received by the router as a key field for a Flexible NetFlow flow record

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match datalink dot1q vlan input
```

Related Commands

Command	Description
flow record	Creates a flow record.

match datalink mac

To configure the use of MAC addresses as a key field for a Flexible NetFlow flow record, use the **match datalink mac** command in Flexible NetFlow flow record configuration mode. To disable the use of MAC addresses as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match datalink mac {**destination** | **source**} **address** {**input** | **output**}}

no match datalink mac {**destination** | **source**} **address** {**input** | **output**}}

Syntax Description

destination address	Configures the use of the destination MAC address as a key field.
source address	Configures the use of the source MAC address as a key field.
input	Packets received by the router.
output	Packets transmitted by the router.

Command Default

MAC addresses are not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

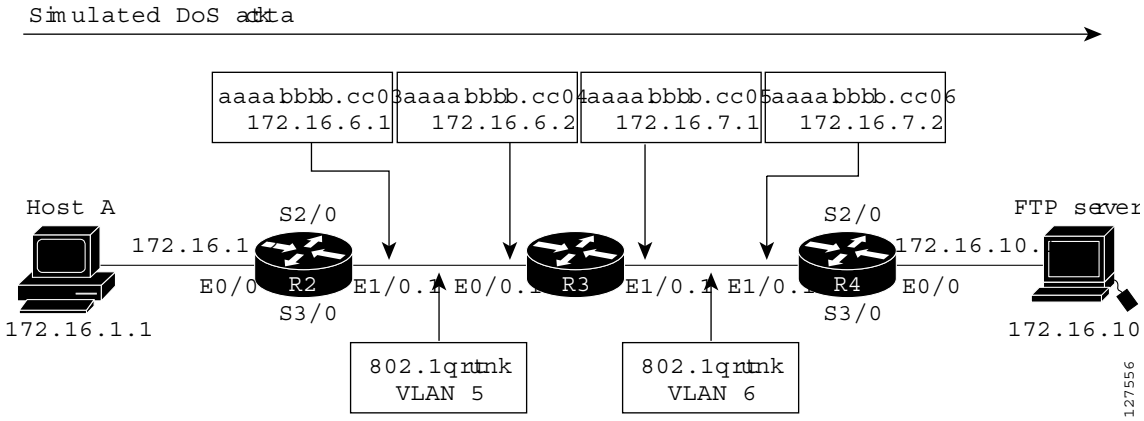
Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

The **input** and **output** keywords of the **match datalink mac** command are used to specify the observation point that is used by the **match datalink mac** command to create flows based on the unique MAC addressees in the network traffic. For example, when you configure a flow record with the **match datalink mac destination address input** command to monitor the simulated denial of service (DoS) attack in Figure 4 and apply the flow monitor to which the flow record is assigned in either input (ingress) mode on interface Ethernet 0/0.1 on R3 or output (egress) mode on interface Ethernet 1/0.1 on R3, the observation point is always Ethernet 0/0.1 on R3. The destination MAC address that is used a key field is aaaa.bbbb.cc04.

Figure 4 Simulated DoS Attack



When the destination output mac address is configured, the value is the destination mac address of the output packet, even if the monitor the flow record is applied to is input only.

When the destination input mac address is configured, the value is the destination mac address of the input packet, even if the monitor the flow record is applied to is output only.

When the source output mac address is configured, the value is the source mac address of the output packet, even if the monitor the flow record is applied to is input only.

When the source input mac address is configured, the value is the source mac address of the input packet, even if the monitor the flow record is applied to is output only.

Examples

The following example configures the use of the destination MAC address of packets that are received by the router as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match datalink mac destination address input
```

The following example configures the use of the source MAC addresses of packets that are transmitted by the router as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match datalink mac source address output
```

Related Commands

Command	Description
flow record	Creates a flow record.

match datalink vlan

To configure the VLAN ID as a key field for a Flexible NetFlow flow record, use the **match datalink vlan** command in Flexible NetFlow flow record configuration mode. To disable the use of the VLAN ID value as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match datalink vlan input

no match datalink vlan input

Syntax Description

input	Configures the VLAN ID of traffic being received by the router as a key field.

Command Default

The VLAN ID is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Examples

The following example configures the VLAN ID of traffic being received by the router as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match datalink vlan input
```

Related Commands

Command	Description
flow record	Creates a flow record.

match flow

To configure the flow direction and the flow sampler ID number as key fields for a flow record, use the **match flow** command in flow record configuration or policy inline configuration mode. To disable the use of the flow direction and the flow sampler ID number as key fields for a flow record, use the **no** form of this command.

match flow {**direction** | **sampler**}

no match flow {**direction** | **sampler**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match flow {**cts** {**destination | source**} **group-tag** | **direction**}

no match flow {**cts** {**destination | source**} **group-tag** | **direction**}

Syntax Description

direction	Configures the direction in which the flow was monitored as a key field.
sampler	Configures the flow sampler ID as a key field.
cts destination group-tag	Configures the CTS destination field group as a key field.
cts source group-tag	Configures the CTS source field group as a key field.

Command Default

The CTS destination or source field group, flow direction and the flow sampler ID are not configured as key fields.

Command Modes

flow record configuration (config-flow-record)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and implemented on the Cisco 7200 series routers.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor. Support was added for policy inline configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.
12.2(50)SY	This command was modified. The **cts destination group-tag** and **destination source-tag** keywords were added in Cisco IOS Release 12.2(50)SY. The **sampler** keyword was not supported.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor. These products use different commands to enter the configuration mode in which you issue this command.

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

You must first enter the s**ervice-policy type performance-monitor inline** command.

match flow direction

This field indicates the direction of the flow. This is of most use when a single flow monitor is configured for input and output flows. It can be used to find and eliminate flows that are being monitored twice, once on input and once on output. This field may also be used to match up pairs of flows in the exported data when the two flows are flowing in opposite directions.

match flow sampler

This field contains the ID of the flow sampler used to monitor the flow. This is useful when more than one flow sampler is being used with different sampling rates. The flow exporter **option sampler-table** command will export options records with mappings of the flow sampler ID to the sampling rate so the collector can calculate the scaled counters for each flow.

Examples

The following example configures the direction the flow was monitored in as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match flow direction
```

The following example configures the flow sampler ID as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match flow sampler
```

The following example configures the CTS destination fields group as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match flow cts destination group-tag
```

The following example configures the CTS source fields group as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match flow cts source group-tag
```

Cisco Performance Monitor in Cisco IOS Release 15.1(3)T and 12.2(58)SE

The following example shows how to use the policy inline configuration mode to configure a service policy for Performance Monitor. The policy specifies that packets traversing Ethernet interface 0/0 that match the flow sampler ID will be monitored based on the parameters specified in the flow monitor configuration named **fm-2**:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# match flow sampler
Router(config-if-spolicy-inline)# flow monitor fm-2
Router(config-if-spolicy-inline)# exit
```

Related Commands

Command	Description
class-map	Creates a class map to be used for matching packets to a specified class.
service-policy type performance-monitor	Associates a Performance Monitor policy with an interface.
flow exporter	Creates a flow exporter.
flow record	Creates a flow record.

match interface (Flexible NetFlow)

To configure the input and output interfaces as key fields for a Flexible NetFlow flow record, use the **match interface** command in Flexible NetFlow flow record configuration mode. To disable the use of the input and output interfaces as key fields for a Flexible NetFlow flow record, use the **no** form of this command.

match interface {**input** | **output**}

no match interface {**input** | **output**}

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

match interface {**input** [**physical**] | **output**} [**snmp**]

no match interface {**input** [**physical**] | **output**} [**snmp**]

Syntax Description

input	Configures the input interface as a key field.
physical	(Optional) Configures the physical input interface as a key field and enables collecting the input interface from the flows.
snmp	(Optional) Configures the simple network management protocol (SNMP) index of the input interface as a key field.
output	Configures the output interface as a key field.

Command Default

The input and output interfaces are not configured as key fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **physical** and **snmp** keywords were added in Cisco IOS Release 12.2(50)SY.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the input interface as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match interface input
```

The following example configures the output interface as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match interface output
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4

To configure one or more of the IPv4 fields as a key field for a Flexible NetFlow flow record, use the **match ipv4** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 {**dscp** | **header-length** | **id** | **option map** | **precedence** | **protocol** | **tos** | **version**}

no match ipv4 {**dscp** | **header-length** | **id** | **option map** | **precedence** | **protocol** | **tos** | **version**}

Syntax Description

dscp	Configures the IPv4 differentiated services code point (DSCP) (part of type of service (ToS)) as a key field.
header-length	Configures the IPv4 header length (in 32-bit words) as a key field.
id	Configures the IPv4 ID as a key field.
option map	Configures the bitmap representing which IPv4 options have been seen as a key field.
precedence	Configures the IPv4 precedence (part of ToS) as a key field.
protocol	Configures the IPv4 protocol as a key field.
tos	Configures the IPv4 ToS as a key field.
version	Configures the IP version from IPv4 header as a key field.

Command Default

The use of one or more of the IPv4 fields as a key field for a user-defined Flexible NetFlow flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Note Some of the keywords of the **match ipv4** command are documented as separate commands. All of the keywords for the **match ipv4** command that are documented separately start with **match ipv4**. For example, for information about configuring the IPv4 time-to-live (TTL) field as a key field for a Flexible NetFlow flow record, refer to the **match ipv4 ttl** command.

Examples

The following example configures the IPv4 DSCP field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4 destination

To configure the IPv4 destination address as a key field for a Flexible NetFlow flow record, use the **match ipv4 destination** command in Flexible NetFlow flow record configuration mode. To disable the IPv4 destination address as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no match ipv4 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv4 destination address as a key field.
mask	Configures the mask for the IPv4 destination address as a key field.
prefix	Configures the prefix for the IPv4 destination address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range 1 to 32.

Command Default

The IPv4 destination address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a 16-bit IPv4 destination address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 destination prefix minimum-mask 16
```

The following example specifies a 16-bit IPv4 destination address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 destination mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4 fragmentation

To configure the IPv4 fragmentation flags and the IPv4 fragmentation offset as key fields for a Flexible NetFlow flow record, use the **match ipv4 fragmentation** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 fragmentation flags and the IPv4 fragmentation offset as key fields for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 fragmentation {**flags** | **offset**}

no match ipv4 fragmentation {**flags** | **offset**}

Syntax Description

flags	Configures the IPv4 fragmentation flags as a key field.
offset	Configures the IPv4 fragmentation offset as a key field.

Command Default

The IPv4 fragmentation flags and the IPv4 fragmentation offset are not configured as key fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

match ipv4 fragmentation flags

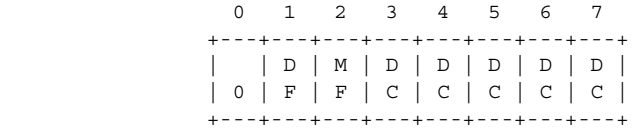
This field matches the “don’t fragment” and “more fragments” flags.

Bit 0: reserved, must be zero

Bit 1: (DF) 0 = May Fragment, 1 = Don’t Fragment

Bit 2: (MF) 0 = Last Fragment,1 = More Fragments

Bits 3–7: (DC) Don’t Care, value is irrelevant



For more information on IPv4 fragmentation flags, see RFC 791, *Internet Protocol* at the following URL: http://www.ietf.org/rfc/rfc791.txt.

Examples

The following example configures the IPv4 fragmentation flags as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 fragmentation flags
```

The following example configures the IPv4 offset flag as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 fragmentation offset
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4 section

To configure a section of an IPv4 packet as a key field for a Flexible NetFlow flow record, use the **match ipv4 section** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv4 packet as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 section {**header size** *header-size* | **payload size** *payload-size*}

no match ipv4 section {**header size** *header-size* | **payload size** *payload-size*}

Syntax Description

header size *header-size*	Configures the number of bytes of raw data starting at the IPv4 header, to use as a key field. Range: 1 to 1200
payload size *payload-size*	Configures the number of bytes of raw data starting at the IPv4 payload, to use as a key field. Range: 1 to 1200

Command Default

A section of an IPv4 packet is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

match ipv4 section header

This command uses the section of the IPv4 header indicated by the **header size** *header-size* keyword and argument as a key field. Only the configured size in bytes will be matched, and part of the payload will also be matched if the configured size is larger than the size of the header.

Note This command can result in large records that use a large amount of router memory and export bandwidth.

match ipv4 section payload

This command uses the section of the IPv4 payload indicated by the **payload size** *payload-size* keyword and argument as a key field.

Note This command can result in large records that use a large amount of router memory and export bandwidth.

Examples

The following example configures the first four bytes (the IPv4 version field) as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 section header size 4
```

The following example configures the first 16 bytes from the payload of the IPv4 packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 section payload size 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4 source

To configure the IPv4 source address as a key field for a Flexible NetFlow flow record, use the **match ipv4 source** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 source address as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no match ipv4 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv4 source address as a key field.
mask	Configures the mask for the IPv4 source address as a key field.
prefix	Configures the prefix for the IPv4 source address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 32.

Command Default

The IPv4 source address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

match ipv4 source prefix minimum-mask

The source address prefix field is the network part of the source address. The optional minimum mask allows a more information to be gathered about large networks.

match ipv4 source mask minimum-mask

The source address mask is the number of bits that make up the network part of the source address. The optional minimum mask allows a minimum value to be configured. This command is useful when there is a minimum mask configured for the source prefix field and the mask is to be used with the prefix. In this case, the values configured for the minimum mask should be the same for the prefix and mask fields.

Alternatively, if the collector knows the minimum mask configuration of the prefix field, the mask field can be configured without a minimum mask so that the true mask and prefix can be calculated.

Examples

The following example configures a 16-bit IPv4 source address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 source prefix minimum-mask 16
```

The following example specifies a 16-bit IPv4 source address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 source mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4 total-length

To configure the IPv4 total-length field as a key field for a Flexible NetFlow flow record, use the **match ipv4 total-length** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 total-length field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 total-length

no match ipv4 total-length

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 total-length field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the total-length value as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 total-length
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv4 ttl

To configure the IPv4 time-to-live (TTL) field as a key field for a Flexible NetFlow flow record, use the **match ipv4 ttl** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv4 TTL field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv4 ttl

no match ipv4 ttl

Syntax Description

This command has no arguments or keywords.

Command Default

The IPv4 time-to-live (TTL) field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures IPv4 TTL as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv4 ttl
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6

To configure one or more of the IPv6 fields as a key field for a Flexible NetFlow flow record, use the **match ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the IPv6 fields as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

no match ipv6 {**dscp** | **flow-label** | **next-header** | **payload-length** | **precedence** | **protocol** | **traffic-class** | **version**}

Syntax Description

dscp	Configures the IPv6 differentiated services code point DSCP (part of type of service (ToS)) as a key field.
flow-label	Configures the IPv6 flow label as a key field.
next-header	Configures the IPv6 next header as a key field.
payload-length	Configures the IPv6 payload length as a key field.
precedence	Configures the IPv6 precedence (part of ToS) as a key field.
protocol	Configures the IPv6 protocol as a key field.
traffic-class	Configures the IPv6 traffic class as a key field.
version	Configures the IPv6 version from IPv6 header as a key field.

Command Default

The IPv6 fields are not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Note Some of the keywords of the **match ipv6** command are documented as separate commands. All of the keywords for the **match ipv6** command that are documented separately start with **match ipv6**. For example, for information about configuring the IPv6 hop limit as a key field for a Flexible NetFlow flow record, refer to the **match ipv6 hop-limit** command.

Examples

The following example configures the IPv6 DSCP field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 dscp
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 destination

To configure the IPv6 destination address as a key field for a Flexible NetFlow flow record, use the **match ipv6 destination** command in Flexible NetFlow flow record configuration mode. To disable the IPv6 destination address as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no match ipv6 destination {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv6 destination address as a key field.
mask	Configures the mask for the IPv6 destination address as a key field.
prefix	Configures the prefix for the IPv6 destination address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range 1 to 128.

Command Default

The IPv6 destination address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a 16-bit IPv6 destination address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination prefix minimum-mask 16
```

The following example specifies a 16-bit IPv6 destination address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 destination mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 extension map

To configure the bitmap of the IPv6 extension header map as a key field for a Flexible NetFlow flow record, use the **match ipv6 extension map** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 bitmap of the IPv6 extension header map as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 extension map

no match ipv6 extension map

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the bitmap of the IPv6 extension header map as a key field for a user-defined Flexible NetFlow flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

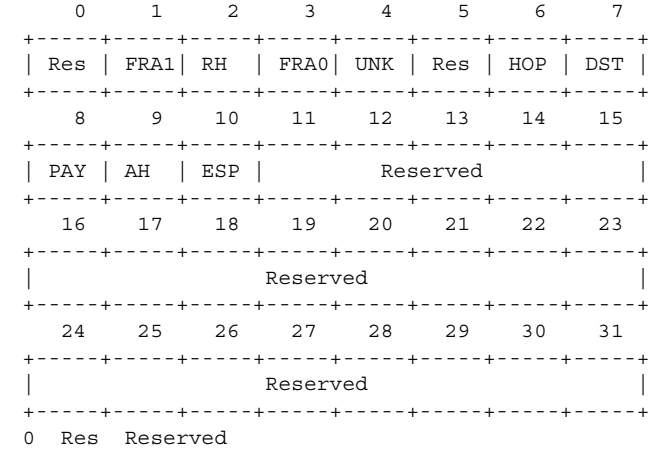
Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Bitmap of the IPv6 Extension Header Map

The bitmap of IPv6 extension header map is made up of 32 bits.



```
1  FRA1 Fragmentation header - not first fragment
2  RH   Routing header
3  FRA0 Fragment header - first fragment
4  UNK  Unknown Layer 4 header
        (compressed, encrypted, not supported)
5  Res  Reserved
6  HOP  Hop-by-hop option header
7  DST  Destination option header
8  PAY Payload compression header
9  AH  Authentication Header
10 ESP Encrypted security payload
11 to 31 Reserved
```

For more information on IPv6 headers, refer to RFC 2460 *Internet Protocol, Version 6 (IPv6)* at the following URL: http://www.ietf.org/rfc/rfc2460.txt.

Examples

The following example configures the IPv6 bitmap of the IPv6 extension header map of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 extension map
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 fragmentation

To configure one or more of the IPv6 fragmentation fields as a key field for a Flexible NetFlow flow record, use the **match ipv6 fragmentation** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 fragmentation field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match IPv6 fragmentation {**flags** | **id** | **offset**}

no match IPv6 fragmentation {**flags** | **id** | **offset**}

Syntax Description

flags	Configures the IPv6 fragmentation flags as a key field.
id	Configures the IPv6 fragmentation ID as a key field.
offset	Configures the IPv6 fragmentation offset value as a key field.

Command Default

The IPv6 fragmentation field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv6 fragmentation flags a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation flags
```

The following example configures the IPv6 offset value a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 fragmentation offset
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 hop-limit

To configure the IPv6 hop limit as a key field for a Flexible NetFlow flow record, use the **match ipv6 hop-limit** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 hop-limit

no match ipv6 hop-limit

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the IPv6 hop limit as a key field for a user-defined Flexible NetFlow flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the hop limit of the packets in the flow as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 hop-limit
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 length

To configure one or more of the IPv6 length fields as a key field for a Flexible NetFlow flow record, use the **match ipv6 length** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 length field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 length {**header** | **payload** | **total**}

no match ipv6 length {**header** | **payload** | **total**}

Syntax Description

header	Configures the length in bytes of the IPv6 header, not including any extension headers as a key field.
payload	Configures the length in bytes of the IPv6 payload, including any extension header as a key field.
total	Configures the total length in bytes of the IPv6 header and payload as a key field.

Command Default

The IPv6 length field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the length of the IPv6 header in bytes, not including any extension headers, as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 length header
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 section

To configure a section of an IPv6 packet as a key field for a Flexible NetFlow flow record, use the **match ipv6 section** command in Flexible NetFlow flow record configuration mode. To disable the use of a section of an IPv6 packet as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 section {**header size** *header-size* | **payload size** *payload-size*}

no match ipv6 section {**header size** *header-size* | **payload size** *payload-size*}

Syntax Description

header size *header-size*	Configures the number of bytes of raw data starting at the IPv6 header, to use as a key field. Range: 1 to 1200
payload size *payload-size*	Configures the number of bytes of raw data starting at the IPv6 payload, to use as a key field. Range: 1 to 1200

Command Default

A section of an IPv6 packet is not configured as a key.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

match ipv6 section header

This command uses the section of the IPv6 header indicated by the **header size** *header-size* keyword and argument as a key field. Only the configured size in bytes will be matched, and part of the payload will also be matched if the configured size is larger than the size of the header.

Note This command can result in large records that use a large amount of router memory and export bandwidth.

match ipv6section payload

This command uses the section of the IPv6 payload indicated by the **payload size** *payload-size* keyword and argument as a key field.

Note This command can result in large records that use a large amount of router memory and export bandwidth.

Examples

The following example configures the first four bytes (the IP version field) from the IPv6 header of the packets in the flows as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 section header size 4
```

The following example configures the first 16 bytes from the payload of the IPv6 packets in the flows as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 section payload size 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match ipv6 source

To configure the IPv6 source address as a key field for a Flexible NetFlow flow record, use the **match ipv6 source** command in Flexible NetFlow flow record configuration mode. To disable the use of the IPv6 source address as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match ipv6 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

no match ipv6 source {**address** | {**mask** | **prefix**} [**minimum-mask** *mask*]}

Syntax Description

address	Configures the IPv6 source address as a key field.
mask	Configures the mask for the IPv6 source address as a key field.
prefix	Configures the prefix for the IPv6 source address as a key field.
minimum-mask *mask*	(Optional) Specifies the size, in bits, of the minimum mask. Range: 1 to 128.

Command Default

The IPv6 source address is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures a 16-bit IPv6 source address prefix as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 source prefix minimum-mask 16
```

The following example specifies a 16-bit IPv6 source address mask as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match ipv6 source mask minimum-mask 16
```

Related Commands

Command	Description
flow record	Creates a flow record.

match routing

To configure one or more of the routing fields as a key field for a Flexible NetFlow flow record, use the **match routing** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the routing fields as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match routing {{**destination** | **source**} {**as** [[**4-octet**] **peer**] [**4-octet**] | **traffic-index**} | **forwarding-status** | **next-hop address** {**ipv4** | **ipv6**} [**bgp**] | **vrf input**}

no match routing {{**destination** | **source**} {**as** [[**4-octet**] **peer**] [**4-octet**] | **traffic-index**} | **forwarding-status** | **next-hop address** {**ipv4** | **ipv6**} [**bgp**] | **vrf input**}

destination	Specifies one or more of the destination routing attributes fields as a key field.
source	Specifies one or more of the source routing attributes fields as a key field.
as	Configures the autonomous system field as a key field.
4-octet	(Optional) Configures the 32-bit autonomous system number as a key field.
peer	(Optional) Configures the autonomous system number of the peer network as a key field.
traffic-index	Configures the Border Gateway Protocol (BGP) destination traffic index as a key field.
forwarding-status	Configures the forwarding status of the packet as a key field.
next-hop address	Configures the next hop address value as a key field. The type of address (IPv4 or IPv6) is determined by the next keyword entered.
ipv4	Specifies that the **next-hop address** value is an IPv4 address.
ipv6	Specifies that the **next-hop address** value is an IPv6 address.
bgp	(Optional) Configures the IPv4 address of the BGP next hop as a key field.
vrf input	Configures the virtual routing and forwarding (VRF) ID for incoming packets as a key field.

Command Default

The use of one or more of the routing fields as a key field for a user-defined Flexible NetFlow flow record is disabled.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	The **ipv6** keyword was added in Cisco IOS Release 12.4(20)T.

Release	Modification
15.0(1)M	This command was modified. The **vrf input** keywords were added in Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS Release XE 3.2S	This command was modified. The **4-octet** keyword was added.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

match routing source as [peer]

This command matches the 16-bit autonomous system number based on a lookup of the router's routing table using the source IP address. The optional **peer** keyword provides the expected next network, as opposed to the originating network.

match routing source as 4-octet [4-octet peer]

This command matches the 32-bit autonomous system number based on a lookup of the router's routing table using the source IP address. The optional **peer** keyword provides the expected next network, as opposed to the originating network.

match routing destination as [peer]

This command matches the 16-bit autonomous system number based on a lookup of the router's routing table using the destination IP address. The **peer** keyword will provide the expected next network as opposed to the destination network.

match routing destination as 4-octet [4-octet peer]

This command matches the 32-bit autonomous system number based on a lookup of the router's routing table using the destination IP address. The **peer** keyword will provide the expected next network as opposed to the destination network.

match routing destination traffic-index

This command matches the traffic-index field based on the destination autonomous system for this flow. The traffic-index field is a value propagated through BGP.

This command is not supported for IPv6.

match routing source traffic-index

This command matches the traffic-index field based on the source autonomous system for this flow. The traffic-index field is a value propagated through BGP.

This command is not supported for IPv6.

match routing forwarding-status

This command matches a field to indicate if the packets were successfully forwarded. The field is in two parts and may be up to 4 bytes in length. For the releases specified in the Command History table, only the status field is used:

```
+-+-+-+-+-+-+-+-+
    | S | Reason    |
    | t | codes     |
    | a | or        |
    | t | flags     |
    | u |           |
    | s |           |
    +-+-+-+-+-+-+-+-+
     0 1 2 3 4 5 6 7

  Status:
  00b=Unknown, 01b = Forwarded, 10b = Dropped, 11b = Consumed
```

match routing vrf input

This command matches the VRF ID from incoming packets on a router. In the case where VRFs are associated with an interface via methods such as VRF Selection Using Policy Based Routing/Source IP Address, a VRF ID of 0 will be recorded. If a packet arrives on an interface that does not belong to a VRF, a VRF ID of 0 is recorded.

Examples

The following example configures the source autonomous system as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing source as
```

The following example configures the destination autonomous system as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing destination as
```

The following example configures the BGP source traffic index as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing source traffic-index
```

The following example configures the forwarding status as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing forwarding-status
```

The following example configures the VRF ID for incoming packets as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing vrf input
```

Related Commands

Command	Description
flow record	Creates a flow record, and enters Flexible NetFlow flow record configuration mode.

match routing is-multicast

To configure the use of the is-multicast field (indicating that the IPv4 traffic is multicast traffic) as a key field for a Flexible NetFlow flow record, use the **match routing is-multicast** command in Flexible NetFlow flow record configuration mode. To disable the use of the is-multicast field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match routing is-multicast

no match routing is-multicast

Syntax Description

This command has no arguments or keywords

Command Default

The is-multicast field is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example configures the is-multicast field as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing is-multicast
```

Related Commands

Command	Description
flow record	Creates a flow record.

match routing multicast replication-factor

To configure the multicast replication factor value for IPv4 traffic as a key field for a Flexible NetFlow flow record, use the **match multicast replication-factor** command in Flexible NetFlow flow record configuration mode. To disable the use of the multicast replication factor value as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match routing multicast replication-factor

no match routing multicast replication-factor

Syntax Description

This command has no arguments or keywords.

Command Default

The multicast replication factor value is not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

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

Examples

The following example configures the multicast replication factor value as a key field for a Flexible NetFlow flow record:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match routing multicast replication-factor
```

Related Commands

Command	Description
flow record	Creates a flow record.

match transport

To configure one or more of the transport fields as a key field for a Flexible NetFlow flow record, use the **match transport** command in Flexible NetFlow flow record configuration mode. To disable the use of one or more of the transport fields as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match transport {**destination-port** | **igmp type** | **source-port**}

no match transport {**destination-port** | **igmp type** | **source-port**}

Syntax Description

destination-port	Configures the transport destination port as a key field.
igmp type	Configures time stamps based on the system uptime as a key field.
source-port	Configures the transport source port as a key field.

Command Default

The transport fields are not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the destination port as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport destination-port
```

The following example configures the source port as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport source-port
```

Related Commands

Command	Description
flow record	Creates a flow record.

match transport icmp ipv4

To configure the ICMP IPv4 type field and the code field as key fields for a Flexible NetFlow flow record, use the **match transport icmp ipv4** command in Flexible NetFlow flow record configuration mode. To disable the use of the ICMP IPv4 type field and code field as key fields for a Flexible NetFlow flow record, use the **no** form of this command.

match transport icmp ipv4 {**code** | **type**}

no match transport icmp ipv4 {**code** | **type**}

Syntax Description

code	Configures the IPv4 ICMP code as a key field.
type	Configures the IPv4 ICMP type as a key field.

Command Default

The ICMP IPv4 type field and the code field are not configured as key fields.

Command Modes

Flexible NetFlow flow record configuration

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the IPv4 ICMP code field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport icmp ipv4 code
```

The following example configures the IPv4 ICMP type field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport icmp ipv4 type
```

Related Commands

Command	Description
flow record	Creates a flow record.

match transport icmp ipv6

To configure the internet control message protocol ICMP IPv6 type field and the code field as key fields for a Flexible NetFlow flow record, use the **match transport icmp ipv6** command in Flexible NetFlow flow record configuration mode. To disable the use of the ICMP IPv6 type field and code field as key fields for a Flexible NetFlow flow record, use the **no** form of this command.

match transport icmp ipv6 {**code** | **type**}

no match transport icmp ipv6 {**code** | **type**}

Syntax Description

code	Configures the ICMP code as a key field.
type	Configures the ICMP type as a key field.

Command Default

The ICMP IPv6 type field and the code field are not configured as key fields.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(20)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A Flow Record requires at least one key field before it can be used in a Flow Monitor. The Key fields differentiate Flows, with each flow having a unique set of values for the key fields. The Key fields are defined using the **match** command.

Examples

The following example configures the IPv6 ICMP code field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport icmp ipv6 code
```

The following example configures the IPv6 ICMP type field as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport icmp ipv6 type
```

Related Commands

Command	Description
flow record	Creates a flow record.

match transport tcp

To configure one or more of the TCP fields as a key field for a Flexible NetFlow flow record, use the **match transport tcp** command in Flexible NetFlow flow record configuration mode. To disable the use of a TCP field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

see collect

match transport tcp {**acknowledgement-number** | **destination-port** | **flags** {[**ack**] | [**cwr**] | [**ece**] | [**fin**] | [**psh**] | [**rst**] | [**syn**] | [**urg**]} | **header-length** | **sequence-number** | **source-port** | **urgent-pointer** | **window-size**}

no match transport tcp {**acknowledgement-number** | **destination-port** | **flags** {**ack**] | [**cwr**] | [**ece**] | [**fin**] | [**psh**] | [**rst**] | [**syn**] | [**urg**]} | **header-length** | **sequence-number** | **source-port** | **urgent-pointer** | **window-size**}

Syntax Description

acknowledgement -number	Configures the TCP acknowledgement number as a key field.
destination-port	Configures the TCP destination port as a key field.
flags	Configures one or more of the TCP flags as a key field. If you configure the **flags** keyword you must also configure at least one of the optional keywords for the **flags** keyword.
ack	(Optional) Configures the TCP acknowledgement flag as a key field.
cwr	(Optional) Configures the TCP congestion window reduced flag as a key field.
ece	(Optional) Configures the TCP Explicit Notification Congestion echo (ECE) flag as a key field.
fin	(Optional) Configures the TCP finish flag as a key field.
psh	(Optional) Configures the TCP push flag as a key field.
rst	(Optional) Configures the TCP reset flag as a key field.
syn	(Optional) Configures the TCP synchronize flag as a key field.
urg	(Optional) Configures the TCP urgent flag as a key field.
header-length	Configures the TCP header length (in 32-bit words) as a key field.
sequence-number	Configures the TCP sequence number as a key field.
source-port	Configures the TCP source port as a key field.
urgent-pointer	Configures the TCP urgent pointer as a key field.
window-size	Configures the TCP window size as a key field.

Command Default

The use of one or more of the TCP fields as a key field for a user-defined Flexible NetFlow flow record is not enabled by default.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the TCP acknowledgement flag as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport tcp flags ack
```

The following example configures the TCP finish flag as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport tcp flags fin
```

The following example configures the TCP reset flag as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport tcp flags rst
```

The following example configures the transport destination port as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport tcp destination-port
```

The following example configures the transport source port as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport tcp source-port
```

Related Commands

Command	Description
flow record	Creates a flow record.

match transport udp

To configure one or more of the user datagram protocol UDP fields as a key field for a Flexible NetFlow flow record, use the **match transport udp** command in Flexible NetFlow flow record configuration mode. To disable the use of a UDP field as a key field for a Flexible NetFlow flow record, use the **no** form of this command.

match transport udp {**destination-port** | **message-length** | **source-port**}

no match transport udp {**destination-port** | **message-length** | **source-port**}

Syntax Description

destination-port	Configures the UDP destination port as a key field.
message-length	Configures the UDP message length as a key field.
source-port	Configures the UDP source port as a key field.

Command Default

The UDP fields are not configured as a key field.

Command Modes

Flexible NetFlow flow record configuration (config-flow-record)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

A flow record requires at least one key field before it can be used in a flow monitor. The key fields differentiate flows, with each flow having a unique set of values for the key fields. The key fields are defined using the **match** command.

Examples

The following example configures the UDP destination port as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport udp destination-port
```

The following example configures the UDP message length as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport udp message-length
```

The following example configures the UDP source port as a key field:

```
Router(config)# flow record FLOW-RECORD-1
Router(config-flow-record)# match transport udp source-port
```

Related Commands

Command	Description
flow record	Creates a flow record.

mode (Flexible NetFlow)

To specify the type of sampling and the packet interval for a Flexible NetFlow sampler, use the **mode** command in Flexible NetFlow sampler configuration mode. To unconfigure the type of sampling and the packet interval for a Flexible NetFlow sampler, use the **no** form of this command.

mode {**deterministic** | **random**} **1 out-of** *window-size*

no mode

Syntax Description

deterministic	Enables deterministic mode sampling for the sampler.
random	Enables random mode sampling for the sampler.
1 out-of *window-size*	Specifies the window size from which to select packets. Range: 2 to 32768.

Command Default

The mode and the packet interval for a sampler are not configured.

Command Modes

Flexible NetFlow sampler configuration (config-sampler)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Deterministic Mode

In deterministic mode, packets are chosen periodically based on the configured interval. This mode has less overhead than random mode and can be useful when sampling traffic that is random in nature. For more information about deterministic sampling, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module in the *Cisco IOS Flexible NetFlow Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/use_fnflow_redce_cpu.html.

Random Mode

In random mode, packets are chosen in a manner that should eliminate any bias from traffic patterns and counter any attempt by users to avoid monitoring. For more information about random sampling, refer to the "Using Cisco IOS Flexible NetFlow Flow Sampling to Reduce the CPU Overhead of Analyzing Traffic" module in the *Cisco IOS Flexible NetFlow Configuration Guide* at the following URL: http://www.cisco.com/en/US/docs/ios/fnetflow/configuration/guide/use_fnflow_redce_cpu.html.

Examples

The following example enables deterministic sampling with a window size of 1000:

```
Router(config)# sampler SAMPLER-1
Router(config-sampler)# mode deterministic 1 out-of 1000
```

The following example enables random sampling with a window size of 1000:

```
Router(config)# sampler SAMPLER-1
Router(config-sampler)# mode random 1 out-of 1000
```

Related Commands

Command	Description
clear sampler	Clears the sampler statistics.
debug sampler	Enables debugging output for samplers.
show sampler	Displays sampler status and statistics.

option (Flexible NetFlow)

To configure options data parameters for a Flexible NetFlow flow exporter, use the **option** command in Flexible NetFlow flow exporter configuration mode. To remove options for a Flexible NetFlow flow exporter, use the **no** form of this command.

option {**application-table | exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**} [**timeout** *seconds*]

no option {**application-table | exporter-stats** | **interface-table** | **sampler-table** | **vrf-table**}

Syntax Description

application-table	Configures the application table option for flow exporters.
exporter-stats	Configures the exporter statistics option for flow exporters.
interface-table	Configures the interface table option for flow exporters.
sampler-table	Configures the export sampler information option for flow exporters.
vrf-table	Configures the virtual routing and forwarding (VRF) ID-to-name table option for flow exporters.
timeout *seconds*	(Optional) Configures the option resend time in seconds for flow exporters. Range: 1 to 86400. Default 600.

Command Default

The options data parameters are not configured.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
15.0(1)M	This command was modified. The **application-table** and **vrf-table** keywords were added in Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

option application-table

This command causes the periodic sending of an options table, which will allow the collector to map the Network Based Application Recognition (NBAR) application IDs provided in the flow records to application names. The optional timeout can alter the frequency at which the reports are sent.

option exporter-stats

This command causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent. This command allows your collector to estimate packet loss for the export records it is receiving. The optional timeout alters the frequency at which the reports are sent.

option interface-table

This command causes the periodic sending of an options table, which will allow the collector to map the interface SNMP indexes provided in the flow records to interface names. The optional timeout can alter the frequency at which the reports are sent.

option sampler-table

This command causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics. The optional timeout can alter the frequency at which the reports are sent.

option vrf-table

This command causes the periodic sending of an options table, which will allow the collector to map the VRF IDs provided in the flow records to VRF names. The optional timeout can alter the frequency at which the reports are sent.

Examples

The following example causes the periodic sending of the exporter statistics, including the number of records, bytes, and packets sent:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option exporter-stats
```

The following example causes the periodic sending of an options table, which allows the collector to map the interface SNMP indexes provided in the flow records to interface names:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option interface-table
```

The following example causes the periodic sending of an options table, which details the configuration of each sampler and allows the collector to map the sampler ID provided in any flow record to a configuration that it can use to scale up the flow statistics:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option sampler-table
```

The following example causes the periodic sending of an options table, which allows the collector to map the NBAR application IDs provided in the flow records to application names:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option application-table
```

The following example causes the periodic sending of an options table, which allows the collector to map the VRF IDs provided in the flow records to VRF names:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# option vrf-table
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

output-features

To enable sending Flexible NetFlow export packets using quality of service (QoS) or encryption, use the **output-features** command in Flexible NetFlow flow exporter configuration mode. To disable sending export packets using QoS or encryption, use the **no** form of this command.

output-features

no output-features

Syntax Description

This command has no arguments or keywords.

Command Default

If QoS or encryption is configured on the router, neither QoS or encryption is run on Flexible NetFlow export packets.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(20)T	This command was introduced.

Usage Guidelines

If the router has the output feature quality of service (QoS) or encryption configured, the **output-features** command causes the output features to be run on Flexible NetFlow export packets.

Examples

The following example configures the use of QoS or encryption on Flexible NetFlow export packets:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# output-features
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

record

To configure a flow record for a Flexible NetFlow flow monitor, use the **record** command in Flexible NetFlow flow monitor configuration mode. To remove a flow record for a Flexible NetFlow flow monitor, use the **no** form of this command.

record {*record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]}

no record

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

record {*record-name* | **platform-original** {**ipv4 | ipv6**} *record* }

no record

Syntax Description

record-name	Name of a user-defined flow record that was previously configured.
netflow-original	Configures the flow monitor to use the Flexible NetFlow implementation of original NetFlow with origin autonomous systems.
netflow ipv4	Configures the flow monitor to use one of the predefined IPv4 records.
netflow ipv6	Configures the flow monitor to use one of the predefined IPv6 records. This keyword is not supported on the Cisco ASR 1000 Series Aggregation Services router.
record	Name of the predefined record. See Table 9 for a listing of the available records and their definitions.
peer	(Optional) Configures the flow monitor to use one of the predefined records with peer autonomous systems. The peer keyword is not supported for every type of Flexible NetFlow predefined record. See Table 9.
platform-original ipv4	Configures the flow monitor to use one of the predefined IPv4 records.
platform-original ipv6	Configures the flow monitor to use one of the predefined IPv6 records.

Command Default

A flow record is not configured.

Command Modes

Flexible NetFlow flow monitor configuration (config-flow-monitor)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	The **ipv6** keyword was added in Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Release	Modification
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
12.2(50)SY	This command was modified. The **netflow-original**, **netflow ipv4**, **netflow ipv6**, and **peer** keywords were removed in Cisco IOS Release 12.2(50)SY. The **platform-original ipv4** and **platform-original ipv4** keywords were added.

Usage Guidelines

Each flow monitor requires a record to define the contents and layout of its cache entries. The flow monitor can use one of the wide range of predefined record formats, or advanced users may create their own record formats.

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

Table 9 describes the keywords and descriptions for the *record* argument.

Table 9 Keywords and Descriptions for the record Argument

Keyword	Description	IPv4 Support	IPv6 Support
as	Autonomous system record.	Yes	Yes
as-tos	Autonomous system and ToS record.	Yes	—
bgp-nexthop-tos	BGP next-hop and ToS record.	Yes	—
bgp-nexthop	BGP next-hop record.	—	Yes
destination	Original 12.2(50)SY platform IPv4/IPv6 destination record.	Yes	Yes
destination-prefix	Destination Prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
destination-prefix-tos	Destination prefix and ToS record.	Yes	—
destination-source	Original 12.2(50)SY platform IPv4/IPv6 destination-source record.	Yes	Yes
full	Original 12.2(50)SY platform IPv4/IPv6 full record.	Yes	Yes
interface-destination	Original 12.2(50)SY platform IPv4/IPv6 interface-destination record.	Yes	Yes
interface-destination-source	Original 12.2(50)SY platform IPv4/IPv6 interface-destination-source record.	Yes	Yes
interface-full	Original 12.2(50)SY platform IPv4/IPv6 interface-full record.	Yes	Yes
interface-source	Original 12.2(50)SY platform IPv4/IPv6 interface-source only record.	Yes	Yes
original-input	Traditional IPv4 input NetFlow.	Yes	Yes

Table 9 Keywords and Descriptions for the record Argument (continued)

original-output	Traditional IPv4 output NetFlow.	Yes	Yes
prefix	Source and destination prefixes record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
prefix-port	Prefix port record. **Note** The **peer** keyword is not available for this record.	Yes	—
prefix-tos	Prefix ToS record.	Yes	—
protocol-port	Protocol ports record. **Note** The **peer** keyword is not available for this record.	Yes	Yes
protocol-port-tos	Protocol port and ToS record. **Note** The **peer** keyword is not available for this record.	Yes	—
source-prefix	Source autonomous system and prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
source-prefix-tos	Source Prefix and ToS record.	Yes	—

Examples

The following example configures the flow monitor to use the NetFlow original record:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# record netflow-original
```

The following example configures the flow monitor to use a user-defined record named collect-ipv4-data:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# record collect-ipv4-data
```

The following example configures the flow monitor to use the Flexible NetFlow IPv4 destination prefix record:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# record netflow ipv4 destination-prefix
```

The following example configures the flow monitor to use a the Flexible NetFlow IPv6 destination prefix record:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# record netflow ipv6 destination-prefix
```

Related Commands

Command	Description
flow monitor	Creates a flow monitor.

sampler

To create a Flexible NetFlow flow sampler, or to modify an existing Flexible NetFlow flow sampler, and to enter Flexible NetFlow sampler configuration mode, use the **sampler** command in global configuration mode. To remove a sampler, use the **no** form of this command.

sampler *sampler-name*

no sampler *sampler-name*

Syntax Description

sampler-name	Name of the flow sampler that is being created or modified.

Command Default

Samplers are not configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Flow samplers are used to reduce the load placed by Flexible NetFlow on the networking device to monitor traffic by limiting the number of packets that are analyzed. You configure a rate of sampling that is 1 out of a range of 2 to 32,768 packets. For example, a rate of 1 out of 2 results in analysis of 50 percent of the packets sampled. Flow samplers are applied to interfaces in conjunction with a flow monitor to implement sampled Flexible NetFlow.

To enable flow sampling, you configure the record that you want to use for traffic analysis and assign it to a flow monitor. When you apply a flow monitor with a sampler to an interface, the sampled packets are analyzed at the rate specified by the sampler and compared with the flow record associated with the flow monitor. If the analyzed packets meet the criteria specified by the flow record, they are added to the flow monitor cache.

Examples

The following example creates a flow sampler name SAMPLER-1:

```
Router(config)# sampler SAMPLER-1
Router(config-sampler)#
```

Related Commands

Command	Description
clear sampler	Clears the flow sampler statistics.
debug sampler	Enables debugging output for flow samplers.
mode	Configures a packet interval for a flow sampler.
show sampler	Displays flow sampler status and statistics.

show flow exporter

To display Flexible NetFlow flow exporter status and statistics, use the **show flow exporter** command in privileged EXEC mode.

show flow exporter [**export-ids** {**netflow-v5** | **netflow-v9**} | [**name**] *exporter-name* [**statistics** | **templates**] [**option application** {**engines** | **table**}]]

Syntax Description

export-ids netflow-v5	(Optional) Displays the NetFlow Version 5 export fields that can be exported and their IDs.
export-ids netflow-v9	(Optional) Displays the NetFlow Version 9 export fields that can be exported and their IDs.
name	(Optional) Specifies the name of a flow exporter.
exporter-name	(Optional) Name of a flow exporter that was previously configured.
statistics	(Optional) Displays flow exporter statistics.
templates	(Optional) Displays flow exporter template information.
option	(Optional) Displays flow exporter options data.
application engines	(Optional) Displays the application engines option for flow exporters.
application table	(Optional) Displays the application table option for flow exporters.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S. The **option** and **application** keywords were added.

Examples

The following example displays the status and statistics for all of the flow exporters configured on a router:

```
Router# show flow exporter

Flow Exporter FLOW-MONITOR-1:
  Description:              Exports to the datacenter
  Export protocol:          NetFlow Version 9
  Transport Configuration:
    Destination IP address: 172.16.10.2
    Source IP address:      172.16.6.2
    Source Interface:       Ethernet0/0
    Transport Protocol:     UDP
```

```
    Destination Port:       650
    Source Port:            55864
    DSCP:                   0x3F
    TTL:                    15
    Output Features:        Used
  Options Configuration:
    exporter-stats (timeout 120 seconds)
    interface-table (timeout 120 seconds)
    sampler-table (timeout 120 seconds)
```

Table 10 describes the significant fields shown in the display.

Table 10 show flow exporter Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.
Description	The description that you configured for the exporter, or the default description “User defined.”
Transport Configuration	The transport configuration fields for this exporter.
Destination IP address	The IP address of the destination host.
Source IP address	The source IP address used by the exported packets.
Transport Protocol	The transport layer protocol used by the exported packets.
Destination Port	The destination UDP port to which the exported packets are sent.
Source Port	The source UDP port from which the exported packets are sent.
DSCP	The differentiated services code point (DSCP) value.
TTL	The time-to-live value.

The following example displays the NetFlow Version 9 export IDs for all of the flow exporters configured on a router. This output will vary according to the flow record configured:

```
Router# show flow exporter export-ids netflow-v9

Export IDs used by fields in NetFlow-common export format:
  ip version                                :    60
  ip tos                                    :   194
  ip dscp                                   :   195
  ip precedence                             :   196
  ip protocol                               :     4
  ip ttl                                    :   192
  ip ttl minimum                            :    52
  ip ttl maximum                            :    53
  ip length header                          :   189
  ip length payload                         :   204
  ip section header                         :   313
  ip section payload                        :   314
  routing source as                         :    16
  routing destination as                    :    17
  routing source as peer                    :   129
  routing destination as peer               :   128
  routing source traffic-index              :    92
  routing destination traffic-index         :    93
  routing forwarding-status                 :    89
```

```
routing is-multicast                        :   206
routing next-hop address ipv4               :    15
routing next-hop address ipv4 bgp           :    18
routing next-hop address ipv6 bgp           :    63
ipv4 header-length                          :   207
ipv4 tos                                    :     5
ipv4 total-length                           :   190
ipv4 total-length minimum                   :    25
ipv4 total-length maximum                   :    26
ipv4 id                                     :    54
ipv4 fragmentation flags                    :   197
ipv4 fragmentation offset                   :    88
ipv4 source address                         :     8
ipv4 source prefix                          :    44
ipv4 source mask                            :     9
ipv4 destination address                    :    12
ipv4 destination prefix                     :    45
ipv4 destination mask                       :    13
ipv4 options                                :   208
transport source-port                       :     7
transport destination-port                  :    11
transport icmp-ipv4 type                    :   176
transport icmp-ipv4 code                    :   177
transport igmp type                         :    33
transport tcp source-port                   :   182
transport tcp destination-port              :   183
transport tcp sequence-number               :   184
transport tcp acknowledgement-number        :   185
transport tcp header-length                 :   188
transport tcp window-size                   :   186
transport tcp urgent-pointer                :   187
transport tcp flags                         :     6
transport udp source-port                   :   180
transport udp destination-port              :   181
transport udp message-length                :   205
interface input snmp                        :    10
interface output snmp                       :    14
interface name                              :    82
interface description                       :    83
flow direction                              :    61
flow exporter                               :   144
flow sampler                                :    48
flow sampler algorithm export               :    49
flow sampler interval                       :    50
flow sampler name                           :    84
flow class                                  :    51
v9-scope system                             :     1
v9-scope interface                          :     2
v9-scope linecard                           :     3
v9-scope cache                              :     4
v9-scope template                           :     5
counter flows                               :     3
counter bytes                               :     1
counter bytes long                          :     1
counter packets                             :     2
counter packets long                        :     2
counter bytes squared long                  :   198
counter bytes permanent                     :    85
counter packets permanent                   :    86
counter bytes squared permanent             :   199
counter bytes exported                      :    40
counter packets exported                    :    41
counter flows exported                      :    42
timestamp sys-uptime first                  :    22
```

```
  timestamp sys-uptime last                  :    21
```

The following example displays the status and statistics for all of the flow exporters configured on a router:

```
Router# show flow exporter name FLOW-MONITOR-1 statistics

Flow Exporter FLOW-MONITOR-1:
  Packet send statistics:
    Ok 0
    No FIB 0
    Adjacency failure 0
    Enqueued to process level 488
    Enqueueing failed 0
    IPC failed 0
    Output failed 0
    Fragmentation failed 0
    Encap fixup failed 0
    No destination address 0
  Client send statistics:
    Client: Flow Monitor FLOW-MONITOR-1
      Records added 558
      Packets sent 486 (51261 bytes)
      Packets dropped 0 (0 bytes)
      No Packet available errors 0
```

Table 11 describes the significant fields shown in the display.

Table 11 show flow exporter name exporter-name statistics Field Descriptions

Field	Description
Flow Exporter	The name of the flow exporter that you configured.
Packet send statistics	The packet transmission statistics for this exporter.
Ok	The number of packets that have been sent successfully.
No FIB	No entry in the Forwarding Information Base (FIB) to forward to.
Adjacency failure	No Cisco Express Forwarding (CEF) adjacency available for forwarding.
Enqueued to process level	Packets that were sent to the processor for forwarding.
Enqueueing failed	Packets that could not be queued for transmission.
IPC failed	Packets for which interprocess communication (IPC) failed.
Output failed	Packets that were dropped because the output queue was full.
Fragmentation failed	Packets that were not able to be fragmented.
Encap fixup failed	Packets that were not able to be encapsulated for transmission on the egress interface.
No destination address	No destination address configured for the exporter.
Client send statistics	Statistics for the flow monitors that are using the exporters.
Client	The name of the flow monitor that is using the exporter.
Records added	The number of flow records that have been added for this flow monitor.

Table 11 show flow exporter name exporter-name statistics Field Descriptions (continued)

Field	Description
Packets sent	The number of packets that have been exported for this flow monitor.
Packets dropped	The number of packets that were dropped for this flow monitor.
No Packet available error	The number of times that no packets were available to transmit the records.

The following example displays the template format for the exporters configured on the router. This output will vary according to the flow record configured:

```
Router# show flow exporter FLOW_EXPORTER-1 templates

Flow Exporter FLOW-MONITOR-1:
  Client: Flow Monitor FLOW-MONITOR-1
  Exporter Format: NetFlow Version 9
  Template ID    : 256
  Record Size    : 53
  Template layout
  ____________________________________________________________________
  |                 Field                    |  Type[1] | Offset[2] |  Size[3] |
  --------------------------------------------------------------------
  | ipv4 source address                      |      8 |      0 |      4 |
  | ipv4 destination address                 |     12 |      4 |      4 |
  | interface input snmp                     |     10 |      8 |      4 |
  | flow sampler                             |     48 |     12 |      4 |
  | transport source-port                    |      7 |     16 |      2 |
  | transport destination-port               |     11 |     18 |      2 |
  | ip tos                                   |    194 |     20 |      1 |
  | ip protocol                              |      4 |     21 |      1 |
  | ipv4 source mask                         |      9 |     22 |      1 |
  | ipv4 destination mask                    |     13 |     23 |      1 |
  | transport tcp flags                      |      6 |     24 |      1 |
  | routing source as                        |     16 |     25 |      2 |
  | routing destination as                   |     17 |     27 |      2 |
  | routing next-hop address ipv4            |     15 |     29 |      4 |
  | interface output snmp                    |     14 |     33 |      4 |
  | counter bytes                            |      1 |     37 |      4 |
  | counter packets                          |      2 |     41 |      4 |
  | timestamp sys-uptime first               |     22 |     45 |      4 |
  | timestamp sys-uptime last                |     21 |     49 |      4 |
  --------------------------------------------------------------------
```

[1]The field type from the display output of the **show flow exporter export-ids netflow-v9** command.
[2]Where this field is located in the flow record.
[3]Size of the field in octets (8-bit bytes).

Related Commands

Command	Description
clear flow exporter	Clears the statistics for exporters.
debug flow exporter	Enables debugging output for flow exporters.
flow exporter	Creates a flow exporter.

show flow interface

To display the Flexible NetFlow configuration and status for an interface, use the **show flow interface** command in privileged EXEC mode.

show flow interface [*type number*]

Syntax Description

type	(Optional) The type of interface on which you want to display Flexible NetFlow accounting configuration information.
number	(Optional) The number of the interface on which you want to display Flexible NetFlow accounting configuration information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example displays the Flexible NetFlow accounting configuration on Ethernet interfaces 0/0 and 0/1:

```
Router# show flow interface ethernet 1/0

Interface Ethernet1/0
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Output
        traffic(ip):      on

Router# show flow interface ethernet 0/0

Interface Ethernet0/0
  FNF:  monitor:          FLOW-MONITOR-1
        direction:        Input
        traffic(ip):      sampler SAMPLER-2#
```

Table 12 describes the significant fields shown in the display.

Table 12 show flow interface Field Descriptions

Field	Description
Interface	The interface to which the information applies.
monitor	The name of the flow monitor that is configured on the interface.

Table 12 show flow interface Field Descriptions (continued)

Field	Description
direction:	The direction of traffic that is being monitored by the flow monitor. The possible values are: • Input—Traffic is being received by the interface. • Output—Traffic is being transmitted by the interface.
traffic(ip)	Indicates if the flow monitor is in normal mode or sampler mode. The possible values are: • on—The flow monitor is in normal mode. • sampler—The flow monitor is in sampler mode (the name of the sampler will be included in the display).

Related Commands

Command	Description
show flow monitor	Displays flow monitor status and statistics.

show flow monitor

To display the status and statistics for a Flexible NetFlow flow monitor, use the **show flow monitor** command in privileged EXEC mode.

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

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
monitor-name	(Optional) Name of a flow monitor that was previously configured.
cache	(Optional) Displays the contents of the cache for the flow monitor.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	(Optional) Displays the flow monitor cache contents in comma separated variables (CSV) format.
record	(Optional) Displays the flow monitor cache contents in record format.
table	(Optional) Displays the flow monitor cache contents in table format.
statistics	(Optional) Displays the statistics for the flow monitor.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	Support for displaying IPv6 data in Flexible NetFlow flow monitor caches was added in Cisco IOS Release 12.4(20)T.
15.0(1)M	This command was modified. Support for displaying virtual routing and forwarding (VRF) and Network Based Application Recognition (NBAR) data in Flexible NetFlow flow monitor caches was added in Cisco IOS Release 15.0(1)M.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The **cache** keyword uses the table format by default.

The uppercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are key fields that Flexible NetFlow uses to differentiate flows. The lowercase field names in the display output of the **show flow monitor** *monitor-name* **cache** command are nonkey fields from which Flexible NetFlow collects values as additional data for the cache.

Examples

The following example displays the status for a flow monitor:

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

Flow Monitor FLOW-MONITOR-1:
  Description:       Used for basic traffic analysis
  Flow Record:       netflow-original
  Flow Exporter:     EXP-DC-TOPEKA
                     EXP-DC-PHOENIX
  Cache:
    Type:              normal
    Status:            allocated
    Size:              4096 entries / 311316 bytes
    Inactive Timeout:  15 secs
    Active Timeout:    1800 secs
    Update Timeout:    1800 secs
```

Table 13 describes the significant fields shown in the display.

Table 13 show flow monitor monitor-name Field Descriptions

Field	Description
Flow Monitor	Name of the flow monitor that you configured.
Description	Description that you configured or the monitor, or the default description "User defined."
Flow Record	Flow record assigned to the flow monitor.
Flow Exporter	Exporters that are assigned to the flow monitor.
Cache	Information about the cache for the flow monitor. **Note** On a Cisco Catalyst 6000 series switch and a Cisco ASR 1000 Series Aggregation Services router, additional output for "Platform cache" is displayed to provide information about the type, status, and size of the hardware cache.
Type	Flow monitor cache type. The possible values are: • immediate—Flows are expired immediately. • normal—Flows are expired normally. • Permanent—Flows are never expired.
Status	Status of the flow monitor cache. The possible values are: • allocated—The cache is allocated. • being deleted—The cache is being deleted. • not allocated—The cache is not allocated.
Size	Current cache size.
Inactive timeout	Current value for the inactive timeout in seconds.
Active timeout	Current value for the active timeout in seconds.
Update timeout	Current value for the update timeout in seconds.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1:

```
Router# show flow monitor FLOW-MONITOR-1 cache

  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               8
  High Watermark:                               10

  Flows added:                                1560
  Flows aged:                                 1552
    - Active timeout    (  1800 secs)           24
    - Inactive timeout (    15 secs)          1528
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0


IP TOS:                     0x00
IP PROTOCOL:                6
IPV4 SOURCE ADDRESS:        10.10.10.2
IPV4 DESTINATION ADDRESS:   172.16.10.2
TRNS SOURCE PORT:           20
TRNS DESTINATION PORT:      20
INTERFACE INPUT:            Et0/0
FLOW SAMPLER ID:            0
ip source as:               0
ip destination as:          0
ipv4 next hop address:      172.16.7.2
ipv4 source mask:           /0
ipv4 destination mask:      /24
tcp flags:                  0x00
interface output:           Et1/0
counter bytes:              198520
counter packets:            4963
timestamp first:            10564356
timestamp last:             12154104
```

Table 14 describes the significant fields shown in the display.

Table 14 show flow monitor monitor-name cache Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The possible values are: • Immediate—Flows are expired immediately. • Normal—Flows are expired normally. • Permanent—Flows are never expired.
Cache size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
High Watermark	Highest number of cache entries seen.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.

Table 14 show flow monitor monitor-name cache Field Descriptions (continued)

Field	Description
Inactive timeout	Current value for the inactive timeout in seconds.
Event aged	Number of flows that have been aged by an event such as using the **force-export** option for the **clear flow monitor** command.
Watermark aged	Number of flows that have been aged because they exceeded the maximum high watermark value.
Emergency aged	Number of flows that have been aged because the cache size was exceeded.
IP TOS	IP type of service (ToS) value.
IP PROTOCOL	Protocol number.
IPV4 SOURCE ADDRESS	IPv4 source address.
IPV4 DESTINATION ADDRESS	IPv4 destination address.
TRNS SOURCE PORT	Source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.
INTERFACE INPUT	Interface on which the input is received.
FLOW SAMPLER ID	Flow sampler ID number.
ip source as	Border Gateway Protocol (BGP) source autonomous system number.
ip destination as	BGP destination autonomous system number.
ipv4 next hop address	IPv4 address of the next hop to which the packet is forwarded.
ipv4 source mask	IPv4 source address mask.
ipv4 destination mask	IPv4 destination address mask.
tcp flags	Value of the TCP flags.
interface output	Interface on which the input is transmitted.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.
timestamp first	Time stamp of the first packet in the flow.
timestamp last	Time stamp of the last packet in the flow.

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-1 in a table format:

```
Router# show flow monitor FLOW-MONITOR-1 cache format table

  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               4
  High Watermark:                                6

  Flows added:                                  90
  Flows aged:                                   86
    - Active timeout    (  1800 secs)            0
```

```
    - Inactive timeout (    15 secs)         86
    - Event aged                              0
    - Watermark aged                          0
    - Emergency aged                          0

IP TOS  IP PROT  IPV4 SRC ADDR    IPV4 DST ADDR    TRNS SRC PORT  TRNS DST PORT
======  =======  ===============  ===============  =============  ==============
0x00          1  10.251.10.1      172.16.10.2                 0              02
0x00          1  10.251.10.1      172.16.10.2                 0           20484
0xC0         17  172.16.6.1       224.0.0.9                 520            5202
0x00          6  10.10.11.1       172.16.10.5                25             252
Router#
```

The following example displays the status, statistics, and data for the flow monitor named FLOW-MONITOR-IPv6 (the cache contains IPv6 data) in record format:

```
Router# show flow monitor name FLOW-MONITOR-IPv6 cache format record

Cache type:                               Normal
  Cache size:                               4096
  Current entries:                             6
  High Watermark:                              8

  Flows added:                              1048
  Flows aged:                               1042
    - Active timeout   (  1800 secs)          11
    - Inactive timeout (    15 secs)        1031
    - Event aged                                0
    - Watermark aged                            0
    - Emergency aged                            0

IPV6 FLOW LABEL:           0
IPV6 EXTENSION MAP:        0x00000040
IPV6 SOURCE ADDRESS:       2001:DB8:1:ABCD::1
IPV6 DESTINATION ADDRESS:  2001:DB8:4:ABCD::2
TRNS SOURCE PORT:          3000
TRNS DESTINATION PORT:     55
INTERFACE INPUT:           Et0/0
FLOW DIRECTION:            Input
FLOW SAMPLER ID:           0
IP PROTOCOL:               17
IP TOS:                    0x00
ip source as:              0
ip destination as:         0
ipv6 next hop address:     ::
ipv6 source mask:          /48
ipv6 destination mask:     /0
tcp flags:                 0x00
interface output:          Null
counter bytes:             521192
counter packets:           9307
timestamp first:           9899684
timestamp last:            11660744
```

Table 15 describes the significant fields shown in the display.

Table 15 show flow monitor monitor-name cache format record Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The possible values are: • Immediate—Flows are expired immediately. • Normal—Flows are expired normally. • Permanent—Flows are never expired.
Cache size	Number of entries in the cache.
Current entries	Number of entries in the cache that are in use.
High Watermark	Highest number of cache entries seen.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
Event aged	Number of flows that have been aged by an event such as using the **force-export** option for the **clear flow monitor** command.
Watermark aged	Number of flows that have been aged because they exceeded the maximum high watermark value.
Emergency aged	Number of flows that have been aged because the cache size was exceeded.
IPV6 FLOW LABEL	Label number for the flow.
IPV6 EXTENSION MAP	Pointer to the IPv6 extensions.
IPV6 SOURCE ADDRESS	IPv6 source address.
IPV6 DESTINATION ADDRESS	IPv6 destination address.
TRNS SOURCE PORT	source port for the transport protocol.
TRNS DESTINATION PORT	Destination port for the transport protocol.
INTERFACE INPUT	Interface on which the input is received.
FLOW DIRECTION	Input or output.
FLOW SAMPLER ID	Flow sampler ID number.
IP PROTOCOL	IP protocol number.
IP TOS	IP ToS number.
ip source as	BGP source autonomous system number.
ip destination as	BGP destination autonomous system number.
ipv6 next hop address	IPv4 address of the next hop to which the packet is forwarded.
ipv6 source mask	IPv6 source address mask.
ipv6 destination mask	IPv6 destination address mask.

Table 15 show flow monitor monitor-name cache format record Field Descriptions (continued)

Field	Description
tcp flags	Value of the TCP flags.
interface output	Interface on which the input is transmitted.
counter bytes	Number of bytes that have been counted.
counter packets	Number of packets that have been counted.
timestamp first	Time stamp of the first packet in the flow.
timestamp last	Time stamp of the last packet in the flow.

The following example displays the status and statistics for a flow monitor:

```
Router# show flow monitor FLOW-MONITOR-1 statistics

  Cache type:                               Normal
  Cache size:                                 4096
  Current entries:                               4
  High Watermark:                                6

  Flows added:                                 116
  Flows aged:                                  112
    - Active timeout    (  1800 secs)            0
    - Inactive timeout (    15 secs)           112
    - Event aged                                 0
    - Watermark aged                             0
    - Emergency aged                             0
```

Table 16 describes the significant fields shown in the display.

Table 16 show flow monitor monitor-name statistics Field Descriptions

Field	Description
Cache type	Flow monitor cache type. The possible values are: • Immediate—Flows are expired immediately. • Normal—Flows are expired normally. • Permanent—Flows are never expired.
Cache size	Size of the cache.
Current entries	Number of entries in the cache that are in use.
High Watermark	Highest number of cache entries seen.
Flows added	Flows added to the cache since the cache was created.
Flows aged	Flows expired from the cache since the cache was created.
Active timeout	Current value for the active timeout in seconds.
Inactive timeout	Current value for the inactive timeout in seconds.
Event aged	Number of flows that have been aged by an event such as using the **force-export** option for the **clear flow monitor** command.

Table 16 show flow monitor monitor-name statistics Field Descriptions (continued)

Field	Description
Watermark aged	Number of flows that have been aged because they exceeded the maximum high watermark value.
Emergency aged	Number of flows that have been aged because the cache size was exceeded.

Related Commands

Command	Description
clear flow monitor	Clears the flow monitor.
debug flow monitor	Enables debugging output for flow monitors.

show flow monitor cache aggregate

To display aggregated flow statistics from a flow monitor cache, use the **show flow monitor cache aggregate** command in privileged EXEC mode.

show flow monitor [**name**] *monitor-name* **cache aggregate** {{*options* [*...options*] [**collect** *options* [*...options*]] | **record** *record-name*} [**format** {**csv** | **record** | **table**}]}

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
monitor-name	Name of a flow monitor that was previously configured.
options	Fields upon which aggregation is performed; and from which additional data from the cache is displayed when the **collect** keyword is used. You can specify multiple values for the *options* argument. See the "Aggregation options Argument" section on page 166 in the "Usage Guidelines" section.
collect	(Optional) Displays additional data from the cache. See the "Cache Data Fields Displayed" section on page 167 in the "Usage Guidelines" section.
record *record-name*	Specifies the name of a user-defined flow record or a predefined flow record. See Table 17 for a listing of the available predefined records and their definitions.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	Displays the flow monitor cache contents in record format.
table	Displays the flow monitor cache contents in table format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Flexible Netflow - Top N Talkers Support

The **show flow monitor cache aggregate** command is one of a set of three commands that make up the Flexible Netflow—Top N Talkers Support feature. The Flexible Netflow—Top N Talkers Support feature is used to manipulate the display output from the Flexible NetFlow cache to facilitate the analysis of network traffic.

The other two commands that make up the Flexible Netflow—Top N Talkers Support feature are **show flow monitor cache filter** and **show flow monitor cache sort**. The three commands can be used together or on their own, depending on your requirements. For more detailed information about these commands, see the **show flow monitor cache filter** command and the **show flow monitor cache sort** command. For

information about how the three commands are used together, refer to the "Configuring Cisco IOS Flexible Netflow—Top N Talkers Support" module in the *Configuring Cisco IOS Flexible Netflow Configuration Guide.*

Flow Aggregation

Flow aggregation using the **show flow monitor cache aggregate** command allows you to dynamically display the flow information in a cache using a different flow record than the cache was originally created from. Only the fields in the cache will be available for the aggregated flows.

Note The key and nonkey fields in the flows are defined in the flow record that you assigned to the flow monitor from which the cache data is being aggregated.

Aggregation helps you achieve a higher-level view of the traffic in your network by combining flow data from multiple flows based on the criteria that interest you, for example, displaying flow data for:

- All the HTTP traffic in your network.
- All the traffic being forwarded to a specific Border Gateway Protocol (BGP) next-hop.
- Identifying a device that is sending several types of traffic to one or more hosts in your network, perhaps as part of a denial of service (DoS) attack.

Aggregation options Argument

The options that you can use for the *options* argument of the **show flow monitor cache aggregate** command are dependent on the fields that are used for the user-defined flow record that you configured for the flow monitor using the **record** command. To identify the options that you can use, use the **show flow record** *record-name* command in privileged EXEC mode, where *record-name* is the name of the record that you configured for the flow monitor.

For example, if you assigned the "NetFlow Original" predefined record to a flow monitor, you use the **show flow record netflow-original** command to display its key (match) and nonkey (collect) fields. The following is partial output from the **show flow record netflow-original** command:

```
flow record netflow-original:
  Description:        Traditional IPv4 input NetFlow with origin ASs
  No. of users:       2
  Total field space:  53 bytes
  Fields:
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
.
.
.
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

The fields from this partial output that you can use for the *option* argument follow the **match** (key fields) and **collect** (nonkey fields) words. For example, you can use the "ipv4 tos" field to aggregate the flows as shown in the first example in the "Examples" section.

Cache Data Fields Displayed

By default the data fields from the cache that are shown in the display output of the **show flow monitor cache aggregate** command are limited to the field used for aggregation and the counter fields such as flows, number of bytes, and the number of packets. The following is partial output from the **show flow monitor FLOW-MONITOR-3 cache aggregate ipv4 destination address** command:

```
IPV4 DST ADDR         flows       bytes        pkts
===============  ==========  ==========  ==========
224.192.16.1              2       97340        4867
224.192.18.1              3       96080        4804
224.192.16.4              4       79760        3988
224.192.45.12             3       77480        3874
255.255.255.255           1          52           1
```

Notice that the data contains only the IPv4 destination addresses for which flows have been aggregated and the counter values.

The flow monitor (FLOW-MONITOR-3) referenced by the **show flow monitor FLOW-MONITOR-3 cache aggregate ipv4 destination address** command uses the "NetFlow Original" predefined record, which contains the following key and nonkey fields:

- match ipv4 tos
- match ipv4 protocol
- match ipv4 source address
- match ipv4 destination address
- match transport source-port
- match transport destination-port
- match interface input
- match flow sampler
- collect routing source as
- collect routing destination as
- collect routing next-hop address ipv4
- collect ipv4 source mask
- collect ipv4 destination mask
- collect transport tcp flags
- collect interface output
- collect counter bytes
- collect counter packets
- collect timestamp sys-uptime first
- collect timestamp sys-uptime last

The **collect** keyword is used to include additional cache data in the display output of the **show flow monitor cache aggregate** command. The following partial output from the **show flow monitor FLOW-MONITOR-3 cache aggregate ipv4 destination address collect transport tcp flags** command shows the transport TCP flags data from the cache:

```
IPV4 DST ADDR    tcp flags       flows       bytes        pkts
===============  =========  ==========  ==========  ==========
224.192.16.1     0x00                4      165280        8264
224.192.18.1     0x00                4      158660        7933
```

```
224.192.16.4      0x00                3      146740        7337
224.192.45.12     0x00                4      145620        7281
255.255.255.255   0x00                1          52           1
224.0.0.13        0x00                1          54           1
```

You can add cache data fields after the **collect** keyword to show additional data from the cache in the display output of the **show flow monitor cache aggregate** command.

Keywords and Descriptions for the record Argument

Table 17 describes the keywords for the *record* argument.

Table 17 Keywords and Descriptions for the Aggregate record Argument

Keyword	Description	IPv4 Support	IPv6 Support
as	Autonomous system record.	Yes	Yes
as-tos	Autonomous system and ToS record.	Yes	—
bgp-nexthop-tos	BGP next-hop and ToS record.	Yes	—
bgp-nexthop	BGP next-hop record.	—	Yes
destination-prefix	Destination prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
destination-prefix-tos	Destination prefix and ToS record.	Yes	—
original-input	Traditional IPv4 input NetFlow.	Yes	Yes
original-output	Traditional IPv4 output NetFlow.	Yes	Yes
prefix	Source and destination prefixes record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
prefix-port	Prefix port record. **Note** The **peer** keyword is not available for this record.	Yes	—
prefix-tos	Prefix ToS record.	Yes	—
protocol-port	Protocol ports record. **Note** The **peer** keyword is not available for this record.	Yes	Yes
protocol-port-tos	Protocol port and ToS record. **Note** The **peer** keyword is not available for this record.	Yes	—
source-prefix	Source autonomous system and prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
source-prefix-tos	Source prefix and ToS record.	Yes	—

Examples

The following example aggregates the flow monitor cache data on the IPv4 ToS value:

```
Router# show flow monitor FLOW-MONITOR-2 cache aggregate ipv4 tos

Processed 12 flows
Aggregated to 3 flows

IP TOS       flows       bytes        pkts
======  ==========  ==========  ==========
0x90             6      706800       35340
0xC8             4      345192       42871
0xAC             2        7865         342
```

The following example aggregates the flow monitor cache data on the IPv4 destination address and displays the cache data for the IPv4 protocol type and input interface nonkey fields:

```
Router# show flow monitor FLOW-MONITOR-3 cache aggregate ipv4 destination address collect
ipv4 protocol interface input

Processed 17 flows
Aggregated to 7 flows

IPV4 DST ADDR    intf input                flows       bytes        pkts  ip prot
===============  ====================  ==========  ==========  ==========  =======
224.192.16.4     Et0/0                          3       42200        2110        1
224.192.16.1     Et0/0                          3       17160         858        1
224.192.18.1     Et0/0                          4       18180         909        1
224.192.45.12    Et0/0                          4       14440         722        1
255.255.255.255  Et0/0                          1          52           1       17
224.0.0.13       Et0/0                          1          54           1      103
224.0.0.1        Et0/0                          1          28           1        2
```

The following example aggregates the flow monitor cache data on the destination and source IPv4 addresses:

```
Router# show flow monitor FLOW-MONITOR-1 cache aggregate ipv4 destination address ipv4
source address

Processed 26 flows
Aggregated to 17 flows

IPV4 SRC ADDR    IPV4 DST ADDR          flows       bytes        pkts
===============  ===============  ==========  ==========  ==========
10.251.10.1      172.16.10.2                2     1400828        1364
192.168.67.6     172.16.10.200              1       19096         682
10.234.53.1      172.16.10.2                3       73656        2046
172.30.231.193   172.16.10.2                3       73616        2045
10.10.10.2       172.16.10.2                2       54560        1364
192.168.87.200   172.16.10.2                2       54560        1364
10.10.10.4       172.16.10.4                1       27280         682
10.10.11.1       172.16.10.5                1       27280         682
10.10.11.2       172.16.10.6                1       27280         682
10.10.11.3       172.16.10.7                1       27280         682
10.10.11.4       172.16.10.8                1       27280         682
10.1.1.1         172.16.10.9                1       27280         682
10.1.1.2         172.16.10.10               1       27280         682
10.1.1.3         172.16.10.11               1       27280         682
172.16.1.84      172.16.10.19               2       54520        1363
172.16.1.85      172.16.10.20               2       54520        1363
172.16.6.1       224.0.0.9                  1          52           1
```

Related Commands

Command	Description
show flow monitor cache filter	Filters the display output of flow records from a flow monitor cache.
show flow monitor cache sort	Sorts the display output of flow records from a flow monitor cache.

show flow monitor cache filter

To filter the display output of statistics from the flows in a flow monitor cache, use the **show flow monitor cache filter** command in privileged EXEC mode.

show flow monitor [**name**] *monitor-name* **cache filter** *options* [**regexp** *regexp*] [*...options* [**regexp** *regexp*]] [**format** {**csv** | **record** | **table**}]

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
monitor-name	Name of a flow monitor that was previously configured.
options	Fields upon which filtering is performed. You can specify multiple values for the *options* argument. See the "Filter options Argument" section on page 172 in the "Usage Guidelines" section.
regexp *regexp*	(Optional) Match the field specified with the *options* argument against a regular expression. See the "Regular Expressions" section on page 173 in the "Usage Guidelines" section.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	Displays the flow monitor cache contents in record format.
table	Displays the flow monitor cache contents in table format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Flexible Netflow—Top N Talkers Support

The **show flow monitor cache filter** command is one of a set of three commands that make up the Flexible Netflow—Top N Talkers Support feature. The Flexible Netflow—Top N Talkers Support feature is used to manipulate the display output from the Flexible NetFlow cache to facilitate the analysis of network traffic.

The other two commands that make up the Flexible Netflow—Top N Talkers Support feature are **show flow monitor cache sort** and **show flow monitor cache aggregate**. The three commands can be used together or on their own, depending on your requirements. For more detailed information about these commands, see the **show flow monitor cache sort** command and the **show flow monitor cache**

aggregate command. For information about how the three commands are used together, refer to the "Configuring Cisco IOS Flexible Netflow—Top N Talkers Support" module in the *Configuring Cisco IOS Flexible Netflow Configuration Guide.*

Filter options Argument

The options that you can use for the *options* argument of the **show flow monitor cache filter** command are dependent on the fields that are used for the record that you configured for the flow monitor using the **record** command. To identify the options that you can use, use the **show flow record** *record-name* command in privileged EXEC mode, where *record-name* is the name of the record that you configured for the flow monitor.

For example, if you assigned the "NetFlow Original" predefined record to a flow monitor, you use the **show flow record netflow-original** command to display its key (match) and nonkey (collect) fields. The following is partial output from the **show** command:

```
flow record netflow-original:
  Description:        Traditional IPv4 input NetFlow with origin ASs
  No. of users:       2
  Total field space:  53 bytes
  Fields:
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
.
.
.
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

The fields from this partial output that you can use for the *option* argument follow the **match** (key fields) and **collect** (nonkey fields) words. For example, you can use the "ipv4 tos" field to filter the flows as shown in the first example in the "Examples" section.

Filtering Criteria

The following are examples of the types of filtering criteria available for the **show flow monitor cache filter** command:

- Perform an exact match on any numerical fields in either decimal or hexadecimal format. For example, these two commands match flows in the flow monitor cache that contain either" 0xA001" or "1" :
  - **show flow monitor FLOW-MONITOR-1 cache filter transport source-port 0xA001**
  - **show flow monitor FLOW-MONITOR-1 cache filter transport source-port 1**
- Perform a match on a range for any numerical fields in either decimal or hexadecimal format. For example, these two commands match flows in the flow monitor cache that contain either "0xA000 0xB000" or "1 1024":
  - **show flow monitor FLOW-MONITOR-1 cache filter transport source-port 0xA000 0xB000**
  - **show flow monitor FLOW-MONITOR-1 cache filter transport source-port 1 1024**
- Perform an exact match for any alphanumerical field. For example, this command matches flows in the flow monitor cache having a MAC address of ABCD:0012:01FE:
  - **show flow monitor FLOW-MONITOR-1 cache filter datalink mac source address ABCD:0012:01FE**

- Perform a regular-expression match on any alphanumerical field. For example, this command matches flows in the flow monitor cache having a MAC address that starts with ABCD:
  - **show flow monitor FLOW-MONITOR-1 cache filter datalink mac source address regexp ABCD:***
- Perform a match on flag fields with an implicit <and>. For example, this command matches flows in the flow monitor cache that contain the **urg** and **syn** TCP flags:
  - **show flow monitor FLOW-MONITOR-1 cache filter transport tcp flags urg syn**
- Perform a match against flags that are not present. For example, this command matches flows in the flow monitor cache that contain the **syn** and **rst** TCP flags and do not contain the **urg** and **fin** TCP flags. :
  - **show flow monitor FLOW-MONITOR-1 cache filter transport tcp flags syn rst not urg fin**
- Perform an exact match on an IP address field. For example, this command matches flows in the flow monitor cache that contain the source IPv4 address “192.168.0.1” :
  - **show flow monitor FLOW-MONITOR-1 cache filter ipv4 source address 192.168.0.1**
- Perform a prefix match on an IPv4 or IPv6 address field. For example, these two commands match flows in the flow monitor cache that contain either “192.168.0.0 255.255.0.0” or “7:20ac::/64”:
  - **show flow monitor FLOW-MONITOR-1 cache filter ipv4 source address 192.168.0.0 255.255.0.0**
  - **show flow monitor FLOW-MONITOR-1 cache filter ipv6 source address 7:20ac::/64**
- Perform a match on a range of relative time stamps. For example, this command matches flows in the flow monitor cache that were created within the last “500” seconds:
  - **show flow monitor FLOW-MONITOR-1 cache filter timestamp sys-uptime first 0 500 seconds**
- Perform a match on range of the time stamp that is configured (uptime or absolute). For example, this command matches flows in the flow monitor cache that were created between 0800 and 0815, within the last 24 hours:
  - **show flow monitor FLOW-MONITOR-1 cache filter timestamp sys-uptime last 08:00:00 08:15:00 t**
- Perform an exact match on an interface. For example, this command matches flows in the flow monitor cache which are received on Ethernet interface 0/0.
  - **show flow monitor FLOW-MONITOR-1 cache filter interface input Ethernet0/0**
- Perform a regular-expression match on an interface. For example, this command matches flows in the flow monitor cache that begin with Ethernet0/ and have either “1”, “2”, or “3” as the port number:
  - **show flow monitor FLOW-MONITOR-1 cache filter interface input regexp Ethernet0/1**

Regular Expressions

Table 18 shows the syntax for regular expressions.

Table 18 Syntax for Regular Expressions

Option	Description
*	Match zero or more characters in this position.
?	Match any one character in this position.

Table 18 Syntax for Regular Expressions

Option	Description
|	Match any one character in this position.
(|)	Match one of a choice of characters in a range. For example aa:(0033|4455):3456 matches either aa:0033:3456 or aa:4455:3456.
[]	Match any character in the range specified, or one of the special characters. For example, [0-9] is all of the digits. [*] is the '*' character, and [[] is the '[' character.

Examples

The following example filters the flow monitor cache data on the IPv4 type of service (ToS) value:

```
Router# show flow monitor FLOW-MONITOR-3 cache filter ipv4 tos regexp 0x(C0|50)

Cache type:                               Normal
  Cache size:                               4096
  Current entries:                            19
  High Watermark:                             38

  Flows added:                              3516
  Flows aged:                               3497
    - Active timeout   (  1800 secs)          52
    - Inactive timeout (    15 secs)        3445
    - Event aged                               0
    - Watermark aged                           0
    - Emergency aged                           0

IPV4 SOURCE ADDRESS:       10.1.1.1
IPV4 DESTINATION ADDRESS:  255.255.255.255
TRNS SOURCE PORT:          520
TRNS DESTINATION PORT:     520
INTERFACE INPUT:           Et0/0
FLOW SAMPLER ID:           0
IP TOS:                    0xC0
IP PROTOCOL:               17
ip source as:              0
ip destination as:         0
ipv4 next hop address:     0.0.0.0
ipv4 source mask:          /24
ipv4 destination mask:     /0
tcp flags:                 0x00
interface output:          Null
counter bytes:             52
counter packets:           1
timestamp first:           18:59:46.199
timestamp last:            18:59:46.199

Matched 1 flow
```

The following example filters the flow monitor cache data on the source IPv4 address of 10.234.53.1:

```
Router# show flow monitor FLOW-MONITOR-1 cache filter ipv4 source address 10.234.53.1

  Cache type:                             Normal
  Cache size:                               4096
  Current entries:                            26
  High Watermark:                             26

  Flows added:                                87
  Flows aged:                                 61
```

```
    - Active timeout   (  1800 secs)          0
    - Inactive timeout (    15 secs)         61
    - Event aged                              0
    - Watermark aged                          0
    - Emergency aged                          0

IPV4 SOURCE ADDRESS:       10.234.53.1
IPV4 DESTINATION ADDRESS:  172.16.10.2
TRNS SOURCE PORT:          0
TRNS DESTINATION PORT:     2048
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               1
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             24724
counter packets:           883
timestamp first:           16:03:56.007
timestamp last:            16:27:07.063

IPV4 SOURCE ADDRESS:       10.234.53.1
IPV4 DESTINATION ADDRESS:  172.16.10.2
TRNS SOURCE PORT:          20
TRNS DESTINATION PORT:     20
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             35320
counter packets:           883
timestamp first:           16:03:56.267
timestamp last:            16:27:07.323

IPV4 SOURCE ADDRESS:       10.234.53.1
IPV4 DESTINATION ADDRESS:  172.16.10.2
TRNS SOURCE PORT:          21
TRNS DESTINATION PORT:     21
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             35320
counter packets:           883
timestamp first:           16:03:56.327
```

```
timestamp last:            16:27:07.363

Matched 3 flows
```

The following example uses multiple filtering criteria to filter the cache data on the IPv4 destination address and the destination port:

```
Router# show flow monitor FLOW-MONITOR-1 cache filter ipv4 destination address regexp
172.16.10* transport destination-port 21

Cache type:                               Normal
  Cache size:                               4096
  Current entries:                            26
  High Watermark:                             26

  Flows added:                               241
  Flows aged:                                215
    - Active timeout   (  1800 secs)          50
    - Inactive timeout (    15 secs)         165
    - Event aged                              0
    - Watermark aged                          0
    - Emergency aged                          0

IPV4 SOURCE ADDRESS:       10.10.10.2
IPV4 DESTINATION ADDRESS:  172.16.10.2
TRNS SOURCE PORT:          21
TRNS DESTINATION PORT:     21
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             17200
counter packets:           430
timestamp first:           17:03:58.071
timestamp last:            17:15:14.615

IPV4 SOURCE ADDRESS:       172.30.231.193
IPV4 DESTINATION ADDRESS:  172.16.10.2
TRNS SOURCE PORT:          21
TRNS DESTINATION PORT:     21
INTERFACE INPUT:           Et0/0.1
FLOW SAMPLER ID:           0
IP TOS:                    0x00
IP PROTOCOL:               6
ip source as:              0
ip destination as:         0
ipv4 next hop address:     172.16.7.2
ipv4 source mask:          /0
ipv4 destination mask:     /24
tcp flags:                 0x00
interface output:          Et1/0.1
counter bytes:             17160
counter packets:           429
timestamp first:           17:03:59.963
timestamp last:            17:15:14.887

Matched 2 flows
```

Related Commands

Command	Description
show flow monitor cache aggregate	Displays aggregated flow records of flows in a flow monitor cache.
show flow monitor cache sort	Sorts the display output of flow records from a flow monitor cache.

show flow monitor cache sort

To sort the display output of statistics from the flows in a flow monitor cache, use the **show flow monitor cache sort** command in privileged EXEC mode.

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

Syntax Description

name	(Optional) Specifies the name of a flow monitor.
monitor-name	Name of a flow monitor that was previously configured.
options	Fields upon which aggregation can be performed. See the "Sort options Argument" section on page 179 in the "Usage Guidelines" section.
top	(Optional) Limits the display output to the 20 highest volume flows (top talkers) unless overridden by the specification of a value for the *number* argument.
number	(Optional) Overrides the default value of top talkers to display.
format	(Optional) Specifies the use of one of the format options for formatting the display output.
csv	Displays the flow monitor cache contents in comma-separated variables (CSV) format.
record	Displays the flow monitor cache contents in record format.
table	Displays the flow monitor cache contents in table format.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(22)T	This command was introduced.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7200 and Cisco 7300 Network Processing Engine (NPE) series routers.

Usage Guidelines

Flexible Netflow—Top N Talkers Support

The **show flow monitor cache sort** command is one of a set of three commands that make up the Flexible Netflow—Top N Talkers Support feature. The Flexible Netflow—Top N Talkers Support feature is used to manipulate the display output from the Flexible NetFlow cache to facilitate the analysis of network traffic.

The other two commands that make up the Flexible Netflow—Top N Talkers Support feature are **show flow monitor cache filter** and **show flow monitor cache aggregate**. The three commands can be used together or on their own, depending on your requirements. For more detailed information about these commands, see the **show flow monitor cache filter** command and the **show flow monitor cache aggregate** command. For information about how the three commands are used together, refer to the "Configuring Cisco IOS Flexible Netflow—Top N Talkers Support" module in the *Configuring Cisco IOS Flexible Netflow Configuration Guide.*

Flow Sorting

The flow sorting function of the Flexible Netflow—Top N Talkers Support feature sorts flow data from the Flexible NetFlow cache based on the criteria that you specify, and displays the data. You can also use the flow sorting function of the Flexible Netflow—Top N Talkers Support feature to limit the display output to a specific number of entries (Top N Talkers) by using the **top** keyword.

Sort options Argument

The options that you can use for the *options* argument of the **show flow monitor cache filter** command are dependent on the fields that are used for the record that you configured for the flow monitor using the **record** command. To identify the options that you can use, use the **show flow record** *record-name* command in privileged EXEC mode, where *record-name* is the name of the record that you configured for the flow monitor.

For example, if you assigned the "NetFlow Original" predefined record to a flow monitor, you use the **show flow record netflow-original** command to display its key (match) and nonkey (collect) fields. The following is partial output from the **show** command:

```
flow record netflow-original:
  Description:        Traditional IPv4 input NetFlow with origin ASs
  No. of users:       2
  Total field space:  53 bytes
  Fields:
    match ipv4 tos
    match ipv4 protocol
    match ipv4 source address
    match ipv4 destination address
.
.
.
    collect counter packets
    collect timestamp sys-uptime first
    collect timestamp sys-uptime last
```

The fields from this partial output that you can use for the *option* argument follow the **match** (key fields) and **collect** (nonkey fields) words. For example, you can use the "ipv4 tos" field to sort the flows as shown in the first example in the "Examples" section.

Examples

The following example sorts the flow monitor cache data on the IPv4 type of service (ToS) value and limits the display output to the top two flows:

```
Router# show flow monitor FLOW-MONITOR-3 cache sort ipv4 tos top 2

Processed 17 flows
Aggregated to 17 flows
Showing the top 2 flows

IPV4 SOURCE ADDRESS:       10.1.1.1
IPV4 DESTINATION ADDRESS:  224.192.16.1
TRNS SOURCE PORT:          0
TRNS DESTINATION PORT:     3073
INTERFACE INPUT:           Et0/0
FLOW SAMPLER ID:           0
IP TOS:                    0x55
IP PROTOCOL:               1
ip source as:              0
ip destination as:         0
ipv4 next hop address:     0.0.0.0
ipv4 source mask:          /24
ipv4 destination mask:     /0
```

```
tcp flags:                  0x00
interface output:           Null
counter bytes:              33680
counter packets:            1684
timestamp first:            18:39:27.563
timestamp last:             19:04:28.459

IPV4 SOURCE ADDRESS:        10.1.1.1
IPV4 DESTINATION ADDRESS:   224.192.16.1
TRNS SOURCE PORT:           0
TRNS DESTINATION PORT:      0
INTERFACE INPUT:            Et0/0
FLOW SAMPLER ID:            0
IP TOS:                     0x55
IP PROTOCOL:                1
ip source as:               0
ip destination as:          0
ipv4 next hop address:      0.0.0.0
ipv4 source mask:           /24
ipv4 destination mask:      /0
tcp flags:                  0x00
interface output:           Et3/0.1
counter bytes:              145040
counter packets:            7252
timestamp first:            18:42:34.043
timestamp last:             19:04:28.459
```

The following example displays the top three flows from the cache sorted on the IPv4 destination addresses from lowest to highest (no aggregation is performed):

```
Router# show flow monitor FLOW-MONITOR-1 cache sort lowest ipv4 destination address top 3

Processed 10 flows
Aggregated to 10 flows
Showing the top 3 flows

IPV4 SOURCE ADDRESS:                    10.1.4.2
IPV4 DESTINATION ADDRESS:               10.1.2.2
datalink dot1q vlan output:             0
datalink mac source address input:      AABB.CC00.2300
datalink mac source address output:     AABB.CC00.2001
datalink mac destination address input: AABB.CC00.2003
flow direction:                         Output
counter bytes:                          50511396
counter packets:                        35558

IPV4 SOURCE ADDRESS:                    10.1.4.2
IPV4 DESTINATION ADDRESS:               10.1.3.2
datalink dot1q vlan output:             0
datalink mac source address input:      AABB.CC00.2300
datalink mac source address output:     AABB.CC00.2002
datalink mac destination address input: AABB.CC00.2003
flow direction:                         Output
counter bytes:                          1154150
counter packets:                        787

IPV4 SOURCE ADDRESS:                    10.1.2.2
IPV4 DESTINATION ADDRESS:               10.1.4.2
datalink dot1q vlan output:             15
datalink mac source address input:      AABB.CC00.2100
datalink mac source address output:     AABB.CC00.2003
datalink mac destination address input: AABB.CC00.2001
flow direction:                         Output
counter bytes:                          50750405
```

```
counter packets:                        35722
```

Related Commands

Command	Description
show flow monitor cache aggregate	Displays aggregated flow records of flows in a flow monitor cache.
show flow monitor cache filter	Filters the display output of flow records from a flow monitor cache.

show flow record

To display the status and statistics for a Flexible NetFlow flow record, use the **show flow record** command in privileged EXEC mode.

show flow record [[**name**] *record-name* | **netflow-original** | **netflow** {**ipv4** | **ipv6**} *record* [**peer**]]

Cisco Catalyst 6500 Switches in Cisco IOS Release 12.2(50)SY

show flow record [[**name**] *record-name* | **platform-original** {**ipv4 | ipv6**} *record*]

Syntax Description

name	(Optional) Specifies the name of a flow record.
record-name	(Optional) Name of a user-defined flow record that was previously configured.
netflow-original	(Optional) Specifies the Flexible NetFlow implementation of original NetFlow with origin autonomous systems.
netflow ipv4	(Optional) Configures the flow monitor to use one of the IPv4 predefined records.
netflow ipv6	(Optional) Configures the flow monitor to use one of the IPv6 predefined records.
record	(Optional) Name of the predefined record. See Table 19 for a listing of the available records and their definitions.
peer	(Optional) Configures the flow monitor to use one of the predefined records with peer autonomous systems. The **peer** keyword is not supported for every type of Flexible NetFlow predefined record. See Table 19.
platform-original ipv4	Configures the flow monitor to use one of the predefined IPv4 records.
platform-original ipv6	Configures the flow monitor to use one of the predefined IPv6 records.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.4(20)T	The **ipv6** and **bgp-nexthop** keywords were added in Cisco IOS Release 12.4(20)T.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
12.2(50)SY	This command was modified. The **netflow-original**, **netflow ipv4**, **netflow ipv6**, and **peer** keywords were removed in Cisco IOS Release 12.2(50)SY. The **platform-original ipv4** and **platform-original ipv6** keywords were added.

Usage Guidelines

Table 19 describes the keywords and descriptions for the *record* argument.

Table 19 Keywords and Descriptions for the record Argument

Keyword	Description	IPv4 Support	IPv6 Support
as	Autonomous system record.	Yes	Yes
as-tos	Autonomous system and Type of Service (ToS) record.	Yes	—
bgp-nexthop-tos	BGP next-hop and ToS record.	Yes	—
bgp-nexthop	BGP next-hop record.	—	Yes
destination	Original platform IPv4/IPv6 destination record.	Yes	Yes
destination-prefix	Destination prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
destination-prefix-tos	Destination prefix and ToS record.	Yes	—
destination-source	Original platform IPv4/IPv6 destination-source record.	Yes	Yes
full	Original platform IPv4/IPv6 full record.	Yes	Yes
interface-destination	Original platform IPv4/IPv6 interface-destination record.	Yes	Yes
interface-destination-source	Original platform IPv4/IPv6 interface-destination-source record.	Yes	Yes
interface-full	Original platform IPv4/IPv6 interface-full record.	Yes	Yes
interface-source	Original platform IPv4/IPv6 interface-source only record.	Yes	Yes
original-input	Traditional IPv4 input NetFlow.	Yes	Yes
original-output	Traditional IPv4 output NetFlow.	Yes	Yes
prefix	Source and destination prefixes record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
prefix-port	Prefix port record. **Note** The **peer** keyword is not available for this record.	Yes	—
prefix-tos	Prefix ToS record.	Yes	—
protocol-port	Protocol ports record. **Note** The **peer** keyword is not available for this record.	Yes	Yes
protocol-port-tos	Protocol port and ToS record. **Note** The **peer** keyword is not available for this record.	Yes	—
source	Original platform IPv4/IPv6 source only record.	Yes	Yes

Table 19 Keywords and Descriptions for the record Argument (continued)

source-prefix	Source autonomous system and prefix record. **Note** For IPv6, a minimum prefix mask length of 0 bits is assumed.	Yes	Yes
source-prefix-tos	Source prefix and ToS record.	Yes	—

Examples

The following example displays the status and statistics for the original Flexible NetFlow record:

```
Router# show flow record FLOW-RECORD-1 platform-original ipv4 destination

flow record FLOW_RECORD-1:
  Description: Flow Record for IPv4 traffic
  No. of users:       3
  Total field space:  53 bytes
  Fields:
    match interface input
    match transport destination-port
    match transport source-port
    match ipv4 destination address
    match ipv4 source address
    match ipv4 protocol
    match ipv4 tos
    collect counter bytes
    collect counter packets
    collect timestamp sys-uptime last
    collect timestamp sys-uptime first
    collect ipv4 destination mask
    collect ipv4 source mask
    collect routing destination as
    collect routing source as
    collect transport tcp flags
    collect routing next-hop address ipv4
    collect interface output
```

Table 20 describes the significant fields shown in the display.

Table 20 show flow record netflow-original Field Descriptions

Field	Description
Description	Description that you configured for the record, or the default description “User defined.”
No. of users	Number of monitors in the configuration that use the flow record.
Total field space	Number of bytes required to store these fields for one flow.
Fields	The fields that are included in this record. For more information about the fields, refer to the **match** and **collect** commands.

Related Commands

Command	Description
record	Configures a flow record for a flow monitor.

show platform flow

To display information for Flexible NetFlow platform parameters. use the **show platform flow** command in privileged EXEC mode.

show platform flow [**aging** | {**export** | **usage** | **table-contention** {**aggregate** | **detailed** | **summary**} }[*instance* | *module*] | {**ip** | **ipv6**} **[***count* | *destination* | *instance* | *module* | *multicast* | *protocol* | *source*] | {**layer2** | **mpls** } **[***count* | *instance* | *module***]]**

Syntax Description

aging	(Optional) Displays the Flexible NetFlow parameter aging information.
export	(Optional) Displays the Flexible NetFlow parameter export information.
usage	(Optional) Displays the Flexible NetFlow table usage information.
table-contention	(Optional) Displays the Flexible NetFlow table contention information.
aggregate	(Optional) Displays the Flexible NetFlow table contention aggregate information.
detailed	(Optional) Displays the Flexible NetFlow table contention detailed information.
summary	(Optional) Displays theFlexible NetFlow table contention summary information.
ip	(Optional) Displays the Flexible NetFlow IP entry information.
ipv6	(Optional) Displays the Flexible NetFlow IPv6 entry information.
count	Total number of entries.
destination	(Optional) Information on entries with destination address.
instance	(Optional) Platform instance information.
module	(Optional) Platform module information.
multicast	(Optional) Flexible NetFlow multicast entry information.
protocol	(Optional) Flexible NetFlow Layer 4 protocol information.
source	(Optional) Information on entries with source address.
layer2	(Optional) Displays the Flexible NetFlow Layer 2 entry information.
mpls	(Optional) Displays the Flexible NetFlow MPLS entry information.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.2(50)SY	This command was introduced.

Examples

The following example displays Flexible NetFlow parameter export information:

```
Router# show platform flow export

Yielding NDE is enabled.
Supervisor CPU threshold = 25
Linecard CPU threshold   = 25
```

```
Module  3:
----------
No of flows read and exported = 0
No of flows discarded         = 0
No of capture+purge requests  = 1695104
No of purge-only requests     = 19

Module  5:
----------
No of flows read and exported = 0
No of flows discarded         = 0
No of capture+purge requests  = 1695158
No of purge-only requests     = 0
lionel#
```

Table 21 describes the significant fields shown in the display.

Table 21 show platform flow export Field Descriptions

Field	Description
Supervisor CPU threshold	The platform (supervisor) CPU utilization threshold (in percent) up to which NetFlow export is permitted. The number and complexity of flow records to be exported is the prime cause of CPU use in NetFlow. The CPU Friendly NetFlow Export feature (also known as Yielding NetFlow Data Export, or Yielding NDE) monitors CPU use for both the supervisor and line cards according to user-configured thresholds and dynamically adjusts the rate of export as needed.
Linecard CPU threshold	The line-card CPU utilization threshold (in percent) up to which NetFlow export is permitted. The number and complexity of flow records to be exported is the prime cause of CPU use in NetFlow. The CPU Friendly NetFlow Export feature (also known as Yielding NetFlow Data Export, or Yielding NDE) monitors CPU use for both the supervisor and line cards according to user-configured thresholds and dynamically adjusts the rate of export as needed.
No of flows read and exported	Number of Flexible NetFlow flows processed and exported.
No of flows discarded	Number of Flexible NetFlow flows discarded.
No of capture+purge requests	Number of Flexible NetFlow flow capture and purge requests.
No of purge-only requests	Number of Flexible NetFlow flow purge requests.

Related Commands

Command	Description
flow hardware	Configures Flexible NetFlow hardware parameters.
flow platform	Configures Flexible NetFlow platform parameters.

show sampler

To display the status and statistics for a Flexible NetFlow sampler, use the **show sampler** command in privileged EXEC mode.

show sampler [[**name**] *sampler-name*]

Syntax Description

name	(Optional) Specifies the name of a flow sampler.
sampler-name	(Optional) Name of a sampler that was previously configured.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.

Examples

The following example displays the status and statistics for all of the flow samplers configured:

```
Router# show sampler

Sampler SAMPLER-1:
  ID:             1
  Description:    User defined
  Type:           random
  Rate:           1 out of 3
  Samples:        189
  Requests:       23243
  Users (2):
    flow monitor FLOW-MONITOR-1 (ip,Et0/0,Input) 65 out of 10786
    flow monitor FLOW-MONITOR-2 (ipv6,Et0/0, Input) 124 out of 12457

Sampler sampler-2:
  ID:             2
  Description:    User defined
  Type:           deterministic
  Rate:           1 out of 100
  Samples:        1
  Requests:       124
  Users (1):
    flow monitor FLOW-MONITOR-1 (ip,Et0/0,Input) 1 out of 124
```

Table 22 describes the significant fields shown in the display.

Table 22 show sampler Field Descriptions

Field	Description
ID	ID number of the flow sampler. This is used to identify the sampler at the collector.
Description	Description that you configured for the flow sampler, or the default description "User defined."
Type	Sampling mode that you configured for the flow sampler. • deterministic—Deterministic mode of sampling. • random—Random mode of sampling.
Rate	Window size (for packet selection) that you configured for the flow sampler. Range: 2 to 32768.
Samples	Number of packets sampled since the flow sampler was configured or the router was restarted. This is equivalent to the number of times a positive response was received when the sampler was queried to determine if the traffic needed to be sampled. Refer to the explanation of the "Requests" field in this table.
Requests	Number of times the flow sampler was queried to determine if the traffic needed to be sampled.
Users	Interfaces on which the flow sampler is configured.

Related Commands

Command	Description
clear sampler	Clears the flow sampler statistics.
debug sampler	Enables debugging output for flow samplers.
sampler	Creates a flow sampler.

source (Flexible NetFlow)

To configure the source IP address interface for all of the packets sent by a Flexible NetFlow flow exporter, use the **source** command in Flexible NetFlow flow exporter configuration mode. To remove the source IP address interface for all of the packets sent by a Flexible NetFlow flow exporter, use the **no** form of this command.

source *interface-type interface-number*

no source

Syntax Description

interface-type	Type of interface whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.
interface-number	Interface number whose IP address you want to use for the source IP address of the packets sent by a Flexible NetFlow flow exporter.

Command Default

The IP address of the interface over which the Flexible NetFlow datagram is transmitted is used as the source IP address.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Usage Guidelines

The benefits of using a consistent IP source address for the datagrams that NetFlow sends include the following:

- The source IP address of the datagrams exported by Flexible NetFlow is used by the destination system to determine from which router the Flexible NetFlow data is arriving. If your network has two or more paths that can be used to send Flexible 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 be obtained, the router uses the IP address of the interface over which the datagram is transmitted as the source IP address of the datagram. In this situation the destination system might receive Flexible NetFlow datagrams from the same router, but with different source IP addresses. When the destination system receives Flexible NetFlow datagrams from the same router with different source IP addresses, the destination system treats the Flexible NetFlow datagrams as if they were being sent from different routers. To avoid having the destination system treat the Flexible NetFlow datagrams

as if they were being sent from different routers, you must configure the destination system to aggregate the Flexible NetFlow datagrams it receives from all of the possible source IP addresses in the router into a single Flexible NetFlow flow.

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

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

Tip When a transient outage occurs on the interface that you configured with the **source** command, the Flexible NetFlow exporter reverts to the default behavior of using the IP address of the interface over which the datagrams are being transmitted as the source IP address for the datagrams. To avoid this problem, use a loopback interface as the source interface because loopback interfaces are not subject to the transient outages that can occur on physical interfaces.

Examples

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

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# source loopback 0
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

statistics packet

To collect protocol distribution statistics and size distribution statistics for a Flexible NetFlow flow monitor, use the **statistics packet** command in Flexible NetFlow flow monitor configuration mode. To disable collecting protocol distribution statistics and size distribution statistics for a Flexible NetFlow flow monitor, use the **no** form of this command.

statistics packet {**protocol** | **size**}

no statistics packet {**protocol** | **size**}

Syntax Description

protocol	Collects packet protocol distribution statistics.
size	Collects packet size distribution statistic.

Command Default

The collection of protocol distribution statistics and size distribution statistics for a Flexible NetFlow flow monitor is not enabled by default.

Command Modes

Flexible NetFlow flow monitor configuration (config-flow-monitor)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following example enables the collection of protocol distribution statistics for flow monitors:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# statistics packet protocol
```

The following example enables the collection of size distribution statistics for flow monitors:

```
Router(config)# flow monitor FLOW-MONITOR-1
Router(config-flow-monitor)# statistics packet size
```

Related Commands

Command	Description
flow monitor	Creates a flow monitor.

template data timeout

To configure the template resend timeout for a Flexible NetFlow flow exporter, use the **template data timeout** command in Flexible NetFlow flow exporter configuration mode. To remove the template resend timeout for a Flexible NetFlow flow exporter, use the **no** form of this command.

template data timeout *seconds*

no template data timeout

Syntax Description

seconds	Configures resending of templates based on the timeout value in seconds, that you enter. Range: 1 to 86400. Default 600.

Command Default

The default template resend timeout for a Flexible NetFlow flow exporter is 600 seconds.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following example configures resending templates based on a timeout of 1000 seconds:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# template data timeout 1000
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

transport (Flexible NetFlow)

To configure the transport protocol for a Flexible NetFlow flow exporter, use the **transport** command in Flexible NetFlow flow exporter configuration mode. To remove the transport protocol for a Flexible NetFlow flow exporter, use the **no** form of this command.

transport udp *udp-port*

no transport

Syntax Description

udp *udp-port*	Specifies User Datagram Protocol (UDP) as the transport protocol and the UDP port number.

Command Default

Flow exporters use UDP on port 9995.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following example configures UDP as the transport protocol and a UDP port number of 250:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# transport udp 250
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.

ttl (Flexible NetFlow)

To configure the time-to-live (TTL) value for a Flexible NetFlow flow exporter, use the **ttl** command in Flexible NetFlow flow exporter configuration mode. To remove the TTL value for a Flexible NetFlow flow exporter, use the **no** form of this command.

ttl *ttl*

no ttl

Syntax Description

ttl	Configures the time-to-live (TTL) value for exported datagrams. Range: 1 to 255. Default 255.

Command Default

Flow exporters use a TTL of 255.

Command Modes

Flexible NetFlow flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(9)T	This command was introduced.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2.
12.2(33)SRC	Support for this command was added for Cisco 7200 series routers in Cisco IOS Release 12.2(33)SRC.
12.2(33)SRE	This command was integrated into Cisco IOS Release 12.2(33)SRE for the Cisco 7300 Network Processing Engine (NPE) series routers.
Cisco IOS XE 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.

Examples

The following example specifies a TTL of 15:

```
Router(config)# flow exporter FLOW-EXPORTER-1
Router(config-flow-exporter)# ttl 15
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.