Cisco IOS Media Monitoring Command Reference

April 8, 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

Cisco IOS Media Monitoring 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 XIX.

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 MediaTrace Commands

admin-params

To configure adminitrator parameters for a Mediatrace performance monitoring profile, use the **admin-params** command in monitoring profile configuration mode. To return to the default setting, use the **no** form of this command.

admin-params

no admin-params

Syntax Description

This command has no arguments or keywords.

Command Modes

Monitoring profile configuration (config-mt-prof-perf)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

This command enters admin parameters configuration mode and enables you to configure administrator parameters for a performance monitoring profile. You can configure the sampling interval.

Examples

The following example shows how to configure administrator parameters for a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# admin-params
Router(config-mt-prof-perf-params)#sampling-interval 10
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

clear mediatrace incomplete-sessions

To clear ongoing Mediatrace polls, use the **clear mediatrace incomplete-sessions** command in privileged EXEC mode.

clear mediatrace incomplete-sessions

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

This command clears ongoing Mediatrace polls. This command must be entered in different session.

Examples

The following example clears incomplete Mediatrace sessions:

```
Router# clear mediatrace incomplete-sessions
```

Related Commands

Command	Description
mediatrace schedule	Schedules Mediatrace sessions.

clock-rate (RTP parameters)

To configure the clock rate for samples taken of Real-Time Transport Protocol (RTP) metrics for a Mediatrace performance monitoring profile, use the **clock-rate** command in RTP parameters configuration mode. To return to the default setting, use the **no** form of this command.

clock-rate {*type-number* | *type-name* | **default**} *rate*

no clock-rate {*type-name* | **default**}

Syntax Description

type-number	An integer between 0 and 34. This value is compared with the payload type field in the RTP header. Values between 0 and 23 are reserved for audio streams, and values between 24 and 34 are reserved for video streams.
type-name	The name of the payload type field in the RTP header.
rate	Clock rate in Hz. The range is from 9600 to 124000.

Command Default

The clock rate is set to 96000 Hz

Command Modes

RTP parameters configuration (config-mt-prof-perf-rtp-params)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

Each payload type has a specific clock rate associated with it. However, because the clock rate can vary depending on the payload codec type, a keyword is provided to set the expected clock rate.

The available values for *type-name and type-number* are celb (25), cn (13), dvi4 (5) (8000 Hz as described in RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*), dvi4-2 (6) (8000 Hz as described in RFC 3551), dvi4-3 (16) (DVI4 Dipol 11025 Hz), dvi4-4 (17) DVI4 Dipol 22050 Hz), g722 (9), g723 (4), g728 (15), g729 (18), gsm (3), h261 (31), h263 (34), jpeg (26), l16 (11) (L16 channel 1), l16-2 (10) (L16 channel 2), lpc (7), mp2t (33), mpa (14), mpv (32), nv (28), pcma (8), pcmu (0), qcelp (12).

Examples

The following example shows how to configure the clock rate for a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# metric-list rtp
Router(config-mt-prof-perf-rtp-params)#clock-rate gsm 10000
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

dest-ip (flow)

To configure the IP address of the destination node for the flow, use the **dest-ip** command in flow configuration mode. To remove the configuration for the destination node, use the **no** form of this command.

dest-ip *ip-address* **dest-port** *port*

no dest-ip *ip-address*

Syntax Description

ip-address	IP address of the destination node for the flow.
dest-port *port*	Specifies the port number of the destination node for the flow.

Defaults

No destination node for the flow is configured.

Command Modes

Flow configuration (config-mt-flowspec)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

When specifying the IP address of the destination node for the flow, you must also specify the port number.

Examples

The following example shows how to configure the IP address of the destination node for the flow:

```
Router(config)# mediatrace flow-specifier flow-4
Router(config-mt-flowspec)# dest-ip 10.10.10.4 dest-port 4800
```

Related Commands

Command	Description
mediatrace flow-specifier	Configures Mediatrace flow specifier.

frequency (session parameters)

To configure the interval between samples taken of metrics, use the **frequency** command in session parameters configuration mode. To return to the default setting, use the **no** form of this command.

frequency {*frequency* | **on-demand**} **inactivity-timeout** *seconds*

no frequency

Syntax Description

frequency	Interval, in seconds, between samples taken of metrics. The range is 10 to 3000.
on-demand	Take samples only when the **mediatrace poll** command is entered.
inactivity-timeout *seconds*	Specifies the number of seconds the Mediatrace Responder will wait without any requests from the Initiator. The range is 1 to 10800.

Command Default

The frequency is set to 120 seconds
The inactivity-timeout is set to 360 seconds.

Command Modes

Session parameters configuration (config-mt-sesparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The value of the inactivity-timeout should be three times the value of the frequency.

Examples

The following example shows how to configure the frequency for a session parameters:

```
Router(config)# mediatrace session-params sess-4
Router(config-mt-sesparam)# frequency 20 inactivity-timeout 20
```

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

history (session parameters)

To configure the number of history buckets retained for metrics collected for a Mediatrace session, use the **history** command in session parameters configuration mode. To return to the default setting, use the **no** form of this command.

history data-sets-kept *buckets*

no history data-sets-kept

Syntax Description

data-sets-kept *buckets*	Number of history buckets retained. The default is 3. The maximum value is 10.

Command Default

The number of history buckets retained is set to three.

Command Modes

Session parameters configuration (config-mt-sesparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The maximum number of history buckets allowed is 10.

Examples

The following example shows how to configure the number of history buckets retained for a session parameters:

```
Router(config)# mediatrace session-params sess-4
Router(config-mt-sesparam)# history data-sets-kept 1
```

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

ip-protocol (flow)

To specify which metrics are monitored for a Mediatrace flow-specifier or path-specifier profile, use the **ip-protocol** command in flow configuration mode. To return to the default setting, use the **no** form of this command.

ip-protocol {tcp | udp}

no ip-protocol

Syntax Description

tcp	Specifies that TCP metrics are monitored.
udp	Specifies that UDP metrics are monitored.

Command Default

The UDP metrics are monitored.

Command Modes

Flow configuration (config-mt-flowspec)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no protocol is specified, UDP metrics are monitored.

Examples

The following example shows how to specify that UDP metrics are monitored for a flow-specifier profile:

```
Router(config)# mediatrace flow-specifier flow-4
Router(config-mt-flowspec)# ip-protocol tcp
```

Related Commands

Command	Description
mediatrace flow-specifier	Configures Mediatrace flow specifier.

max-dropout

To configure the maximum number of dropouts allowed when sampling Real-Time Transport Protocol (RTP) metrics for a Mediatrace performance monitoring profile, use the **max-dropout** command in RTP parameters configuration mode. To return to the default setting, use the **no** form of this command.

max-dropout *number*

no max-dropout

Syntax Description

number	Maximum number of allowed dropouts. The default is 10. The maximum value is 20.

Command Default

The maximum number of allowed dropouts is set to 10.

Command Modes

RTP parameters configuration (config-mt-prof-perf-rtp-params)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The definition of maximum dropouts is the maximum number of packets to ignore ahead the current packet in terms of sequence number.

Examples

The following example shows how to configure the maximum number of allowed dropouts for a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# metric-list rtp
Router(config-mt-prof-perf-rtp-params)# max-dropout 4
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

max-reorder

To configure the maximum number of reorders allowed when sampling Real-Time Transport Protocol (RTP) metrics for a Mediatrace performance monitoring profile, use the **max-reorder** command in RTP parameters configuration mode. To return to the default setting, use the **no** form of this command.

max-reorder *number*

no max-reorder

Syntax Description

number	Maximum number of allowed reorders. The default is 5. The maximum value is 20.

Command Default

The maximum number of allowed reorders is set to 5.

Command Modes

RTP parameters configuration (config-mt-prof-perf-rtp-params)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The definition of maximum rereorders is the maximum number of packets to ignore behind the current packet in terms of sequence number.The maximum value for the maximum number of allowed reorders is 20.

Examples

The following example shows how to configure the maximum number of allowed reorders for a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# metric-list rtp
Router(config-mt-prof-perf-rtp-params)# max-reorder 4
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

mediatrace

To configure Mediatrace sessions, use the **mediatrace** command in global configuration mode. To remove Mediatrace sessions, use the **no** form of this command.

mediatrace *session-number*

no mediatrace *session-number*

Syntax Description

session-number	ID number of the mediatrace session to configure.

Command Default

No Mediatrace sessions are configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

This command enters Mediatrace session configuration mode and enables you to associate the following Mediatrace profile configurations with the session:

- Path-specifier profile
- Session-params profile
- Flow-specifier profile
- System profile
- Perf-monitor profile

Examples

The following example shows how to enter Mediatrace session configuration mode:

```
Router(config)# mediatrace 4
```

Related Commands

Command	Description
mediatrace flow-specifier	Configures the Mediatrace flow-specifier.
mediatrace path-specifier	Configures the Mediatrace path-specifier.
mediatrace profile perf-monitor	Configures the Mediatrace performance monitoring profile.
mediatrace profile system	Configures Mediatrace system profile.
mediatrace session-params	Configures Mediatrace session parameters.

mediatrace initiator

To enable the Mediatrace Initiator, use the **mediatrace initiator** command in global configuration mode. To disable the Mediatrace Initiator, use the **no** form of this command.

mediatrace initiator {**source-ip** *ip-address* | **source-interface** *interface-name*} [**force**] [**max-sessions** *number*]

no mediatrace initiator [**force**]

Syntax Description

source-ip *ip-address*	Specifies the IP address to use for the Mediatrace Initiator.
source-interface *interface-name*	Specifies the interface to use for the Mediatrace Initiator.
force	(Optional) Forces mediatrace to be disabled.
max-sessions *number*	(Optional) Sets the maximum number of Mediatrace sessions.

Command Default

The Mediatrace Initiator is disabled.
When the Mediatrace Initiator is enabled, the maximum number of mediatrace sessions is set to 20.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

Mediatrace Initiator is disabled by default. Therefore, no Mediatrace services are available until you issue this command for the Mediatrace Initiator. Before you can use Mediatrace, you must issue this command on one of the nodes in the media path and issue the **mediatrace responder** command on all nodes that you want to support Mediatrace.

Tip When you enable the Mediatrace Initiator, you must specify a local interface or an address on a local interface. For large deployments, The use of the **source-interface keyword** is recommended.

You can also use this command to set the maximum sessions that can be started by the Mediatrace Initiator. The upper limit for the maximum number of mediatrace sessions is platform-dependant.

Examples

The following example shows how to enable the Mediatrace Initiator on the local interface with an IP address of 10.10.2.2:

```
Router(config)# mediatrace initiator source-ip 10.10.2.2
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

mediatrace responder

To enable the Mediatrace Responder, use the **mediatrace responder** command in global configuration mode. To disable the Mediatrace Responder, use the **no** form of this command.

mediatrace responder [max-sessions *number***]**

no mediatrace responder

Syntax Description

max-sessions *number*	(Optional) Sets the maximum number of Mediatrace sessions.

Command Default

The Mediatrace Responder are disabled.
The maximum number of mediatrace sessions is set to 20.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

Mediatrace Responder is disabled by default. Therefore, no Mediatrace services are available until you issue this command for the Mediatrace Responder. Before you can use Mediatrace, you must issue the **mediatrace initiator** command on one of the nodes in the media path and issue this command on all nodes that you want to support Mediatrace.

You can also use this command to set the maximum sessions that can be used by the Mediatrace Responder. The upper limit for the maximum number of mediatrace sessions is platform-dependant.

Examples

The following example shows how to enable the Mediatrace Responder on a node with an IP address of 10.10.10.4:

```
Router(config)# mediatrace responder max-sessions 12
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

mediatrace path-specifier

To configure the path-specifier profile for Mediatrace, use the **mediatrace path-specifier** command in global configuration mode. To remove the path specifier profile, use the **no** form of this command.

mediatrace path-specifier *name* **[disc-proto rsvp] destination-ip** *ip-address* **[port** *number***]**

no mediatrace path-specifier *name*

Syntax Description

name	Name of the path-specifier profile.
disc-proto rsvp	(Optional) Specifies that RSVP is used as the discovery protocol for the path.
destination-ip *ip-address*	Specifies on the destination address for the path.
port *number*	(Optional) Specifies on the destination port for the path.

Command Default

No path-specifier profile is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

After using this command to enter path configuration mode, you can configure the source address and port of the path.

You can associate a path-specifier profile with one or more actual Mediatrace sessions when they are configured.

Examples

The following example shows how to configure a path-specifier profile with a destination address of 10.10.2.8:

```
Router(config)# mediatrace path-specifier path-2 destination ip 10.10.2.8
```

Related Commands

Command	Description
mediatrace	Configures Mediatrace sessions.

mediatrace poll

To perform an on-demand fetch of data, use the **mediatrace poll** command in privileged EXEC mode.

mediatrace poll {**session** *number* | {[**timeout** *value*] **path-specifier** {**name** *path-name*} | [**disc-proto rsvp**] **destination** *ip-address* [**port** *number*]} [**source** *ip-address* [**port** *number*]] [**ip-protocol {tcp | udp**}] } {**app-health | hops | system** [**profile** *system-profile-name*] | [**configless**] **perf-monitor** [**profile** *profile-name*]} {**flow-specifier** *name* | **source-ip** *ipaddress* **source-port** *number* **dest-ip** *ipaddress* **dest-port** *numbern* **ip-protocol** {**tcp | udp**}}}

Syntax Description

session *number*	Specifies the session for which to fetch data.
timeout *value*	(Optional) Specifies the amount of time to wait for a reply.
path-specifier	Fetches data for a specific path.
name *path-name*	Specifies the path for which data is fetched.
disc-proto rsvp	(Optional) Uses the RSVP transport protocol to perform hop discovery. This is currently the only protocol supported and the default.
destination *ip-address*	Specifies the destination of the path for which data is fetched.
port *number*	Specifies the destination or source port of the path for which data is fetched.
source *ip-address*	Specifies the source of the path for which data is fetched.
ip-protocol	(Optional) Specifies the protocol for which data is fetched.
tcp	Fetches data for the TCP packets.
udp	Fetches data. for the UDP packets.
app-health	Fetches data on application health.
hops	Fetches data on hops.
system	Fetches data on a system profile
profile *system-profile-name*	(Optional) Specifies the system profile for which data is fetched.
configless	(Optional) Fetch data from the nodes along a media path, which have existing Performance Monitor policies configured.
perf-monitor	Fetches data on a perf-monitor profile.
flow-specifier -*name*	Fetches data for a specific flow.
source-ip *ipaddress*	Specifies the source address of the flow for which data is fetched.
source-port *number*	(Optional) Specifies the source port of the flow for which data is fetched.
dest-ip *ipaddress*	Specifies the destination address of the flow for which data is fetched.
dest-port *number*	(Optional) Specifies the destination port of the flow for which data is fetched.
ip-protocol	(Optional) Specifies the protocol for which data is fetched.

Command Default

The timeout is 60 seconds.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

For existing Performance Monitor profiles, the minimum value of the timeout allowed will depend on the sampling-interval configured in profile. If default perf-monitor profile is used then default value of sampling-interval is 30 second so minimum timeout value is 60 seconds.

The following examples show some ways you can use the **mediatrace poll** command to perform an on-demand fetch of data from the hops on a specific path:

- To retrieve data using a pre-configured session. In this case, no other parameters have to be specified inline. The pre-configured session must be have the frequency type set to on-demand.
- To retrieve the system data, hop or video monitoring information from hops along the specified path. You can specify the path as a pre-configured path-specifier or an inline path specification, in case you do not have config mode privileges. Note that by default, Cisco Mediatrace tries to configure nodes along the path to report passive monitoring metrics, and then waits for a configurable amount of time before going out again to collect the data.
- The **configless** keyword can be used to fetch data from the nodes along a media path, which already have Performance Monitor policies configured using the Performance Monitor commands. Some key things to keep in mind when fetching data using this method are that:
  - The default perf-monitor profile or associated perf-monitor profile will have a sampling interval. If the sampling interval of the static policy does not match the one in the associated perf-monitor profile, no data is returned.
  - If there is no Performance Monitor policy configured on a Responder node, the Cisco Mediatrace Responder does not try to configure Performance Monitor and simply reports error to the Mediatrace Initiator.

If Cisco Mediatrace is not collecting all of the data that you want:

- Use the **show mediatrace session** command to verify that the intended values are set for the parameters for a specific session or all sessions.
- Use the **show mediatrace responder app-health** command and the **show mediatrace responder sessions** command to determine the status of the nodes being monitored.
- Use the **debug mediatrace** command to view error messages.

Examples

Note For examples of poll output, see the end of this section.

The following example shows how to fetch the default system metrics when the source IP address, source port, and destination port are not known. Cisco Mediatrace uses the best local IP address as source IP address to find which hops are using RSVP.

mediatrace poll path dest *ip-address* **system**

The following example shows how to fetch the default system metrics when the source and destination port numbers are not known. RSVP finds the hop between the specified source and destination.

mediatrace poll path source *ip-address* **dest** *ip-address* **system**

The following example shows how to fetch the default system metrics when the source and destination port numbers are known. RSVP finds the hop using this information.

mediatrace poll path source *ip-address* **port** *number* **destination** *ip-address* **port** *number* **ip-protocol udp system**

The following example shows how to fetch the default set of RTP metrics. Cisco Mediatrace uses the path parameters to discover hops and uses the inline flow specifier profile as a filter for Performance Monitor data.

mediatrace poll path source *ip-address* **dest** *ip-address* **perf-monitor source-ip** *ip-address* **source-port** *number* **dest-ip** *ip-address* **dest-port** *number* **ip-protocol udp**

The following example shows how to fetch the default set of TCP metrics. Cisco Mediatrace uses the path parameters to discover hops and uses the inline flow-specifier profile as a filter for Performance Monitor data.

mediatrace poll path source *ip-address* **dest** *ip-address* **perf-monitor source-ip** *ip-address* **source-port** *number* **dest-ip** *ip-address* **dest-port** *number* **ip-protocol tcp**

The following example shows how to fetch the default set of RTP metrics. Cisco Mediatrace uses the best local IP address as source IP address for finding hops on the path and uses the inline flow specifier profile as a filter for Performance Monitor data.

mediatrace poll path dest *ip-address* **perf-monitor source-ip** *ip-address* **source-port** *number* **dest-ip** *ip-address* **dest-port** *number* **ip-protocol udp**

The following example shows how to fetch the default set of TCP metrics. Cisco Mediatrace uses the best local IP address as source IP address for finding hops on the path and uses the inline flow-specifier profile as a filter for Performance Monitor data.

mediatrace poll path dest *ip-address* **perf-monitor source-ip** *ip-address* **source-port** *number* **dest-ip** *ip-address* **dest-port** *number* **ip-protocol tcp**

The following example shows how to fetch the default set of RTP metrics from an existing static policy configured on the Responders. This command does not configure the Performance Monitor, so for more information, see *Configuring Performance Monitor*. Cisco Mediatrace uses the path parameters to discover hops and use the inline flow specifier profile as a filter for Performance Monitor data.

mediatrace poll path source *ip-address* **dest** *ip-address* **configless perf-monitor flow-specifier source** *ip-address* **port** *number* **dest** *ip-address* **port** *number* **ip-protocol udp**

This example shows the output is produced by the following hops poll command:

```
mediatrace poll path-specifier source 10.10.130.2 destination 10.10.132.2 hops

Started the data fetch operation.
Waiting for data from hops.
This may take several seconds to complete...
Data received for hop 1
```

```
Data received for hop 2
Data fetch complete.
Results:
Data Collection Summary:
  Request Timestamp: 22:47:56.788 PST Fri Oct 29 2010
  Request Status: Completed
  Number of hops responded (includes success/error/no-record): 2
  Number of hops with valid data report: 2
  Number of hops with error report: 0
  Number of hops with no data record: 0
Detailed Report of collected data:
    Number of Mediatrace hops in the path: 2

    Mediatrace Hop Number: 1 (host=responder1, ttl=254)
      Reachability Address: 10.10.12.3
      Ingress Interface: Gi0/1
      Egress Interface: Gi0/2

    Mediatrace Hop Number: 2 (host=responder2, ttl=253)
      Reachability Address: 10.10.34.3
      Ingress Interface: Gi0/1
      Egress Interface: Gi0/2
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

mediatrace profile perf-monitor

To configure a Mediatrace performance monitoring profile, use the **mediatrace profile perf-monitor** command in global configuration mode. To remove a performance monitoring profile, use the **no** form of this command.

mediatrace profile perf-monitor *name*

no mediatrace profile perf-monitor *name*

Syntax Description

name	Name used to identify the profile.

Command Default

No Mediatrace performance monitoring profile is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

After using this command to enter perf-prof configuration mode, you can configure the following optional parameters:

- Sampling interval
- Clock rate
- Maximum number of dropouts
- Maximum number of reorders
- Minimum number of sequential errors

You can associate a performance monitoring profile with one or more actual Mediatrace sessions when they are configured.

Examples

The following example shows how to configure a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# metric-list rtp
Router(config-mt-prof-perf-rtp-params)# clock-rate 84
Router(config-mt-prof-perf-rtp-params)# max-dropout 2
Router(config-mt-prof-perf-rtp-params)# max-reorder 4
Router(config-mt-prof-perf-rtp-params)# min-sequential 2
Router(config-mt-prof-perf-rtp-params)# exit
Router(config-mt-prof-perf)# admin-params
Router(config-mt-prof-perf-params)# sampling-interval 20
```

Related Commands

Command	Description
mediatrace flow-specifier	Configures Mediatrace flow specifier.

mediatrace profile system

To configure a system-data monitoring profile, use the **mediatrace profile system** command in global configuration mode. To remove a system profile, use the **no** form of this command.

mediatrace profile system *name*

no mediatrace profile system *name*

Syntax Description

name	Name used to identify the profile.

Command Default

No Mediatrace system-data profile is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

After using this command to enter system-data profile configuration mode, you can configure which of the following types of system data are monitored:

- Interface
- CPU
- Memory

You can associate a system-data monitoring profile with one or more actual Mediatrace sessions when they are configured.

Examples

The following example shows how to configure a sysem-data monitoring profile:

```
Router(config)# mediatrace profile system system-8
Router(config-sys-prof)# metric-list CPU MEMORY
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

mediatrace schedule

To configure when a Mediatrace session will occur, use the **mediatrace schedule** command in global configuration mode. To remove a Mediatrace schedule, use the **no** form of this command.

mediatrace schedule *session ID* [**life** {**forever** | *seconds*}] [**start-time** {*hh*:*mm*[:*ss*] [*month day* | *day month*] | **pending** | **now** | **after** *hh*:*mm*:*ss*}] [**ageout** *seconds*] [**recurring**]

no mediatrace schedule *session ID*

Syntax Description

session ID	ID number of the session to schedule.
life	Specifies how long the session schedule will last.
forever	(Optional) Specifies that the session schedule will last forever.
seconds	(Optional) Number of seconds the session schedule will last.
start-time	(Optional) Specifies when the session schedule will start.
hh:*mm*:*ss*	(Optional) Time of day the session schedule will start.
month day	(Optional) Date that the session schedule will start.
day month	(Optional) Date that the session schedule will start.
pending	(Optional) Specifies that the start time of the session schedule is pending.
now	(Optional) Specifies that the session schedule will start now.
after	(Optional) Specifies that the session schedule will end at the specified time.
ageout	(Optional) Specifies that the session schedule will stop after the specified number of seconds.
recurring	(Optional) Specifies that the session schedule will recur.

Command Default

No schedule is specified for the session and it is in the pending state.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to configure a session schedule that will start now and last 60 seconds:

```
Router(config)# mediatrace schedule 22 life 60 now
```

Related Commands

Command	Description
mediatrace *session-number*	Configures a Mediatrace session.

mediatrace session-params

To configure session-parameters, use the **mediatrace session-params** command in global configuration mode. To remove the session-parameters configuration, use the **no** form of this command.

mediatrace session-params *name*

no mediatrace session-params *name*

Syntax Description

name	Name used to identify the profile.

Command Default

No session-parameters profile is configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

After using this command to enter session-parameters configuration mode, you can configure the following parameters:

- Sampling frequency
- Inactivity timeout
- Number of historical data sets kept
- Response timeout
- Route change reaction time

You can associate a session-parameters profile with one or more actual Mediatrace sessions when they are configured.

Examples

The following example shows how to configure a session-parameters profile:

```
Router(config)# mediatrace session-params session-4
Router(config-mt-sesparam)# frequency 20 inactivity-timeout 40
Router(config-mt-sesparam)# history data-sets-kept 2
Router(config-mt-sesparam)# response-timeout 20
Router(config-mt-sesparam)# route-change reaction-time 4
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

metric-list (monitoring profile)

To specify monitoring parameters for a Mediatrace performance monitoring profile, use the **metric-list** command in monitoring profile configuration mode. To return to the default setting, use the **no** form of this command.

metric-list {tcp | rtp}

no metric-list {tcp | rtp}

Syntax Description

tcp	Configures monitoring parameters for TCP packets.
rtp	Configures monitoring parameters for Real-Time Transport Protocol (RTP) packets.

Command Default

The RTP metrics are monitored.

Command Modes

Monitoring profile configuration (config-mt-prof-perf)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

This command specifies whether TCP packet or RTP packet are monitored and enters monitoring parameters configuration mode for a performance monitoring profile. For RTP, you can configure the following parameters:

- Clock rate
- Maximum number of dropouts allowed
- Maximum number of packet allowed to be received out of order
- Minimum number of packets in a sequence used to classify a RTP flow

Examples

The following example shows how to configure monitoring parameters for RTP packets:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# metric-list rtp
Router(config-mt-prof-perf-rtp-params)# clock-rate 84
Router(config-mt-prof-perf-rtp-params)# max-dropout 2
Router(config-mt-prof-perf-rtp-params)# max-reorder 4
Router(config-mt-prof-perf-rtp-params)# min-sequential 2
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

metric-list (system profile)

To specify which metrics are monitored for a Mediatrace system-data profile.use the **metric-list** command in system profile configuration mode. To return to the default setting, use the **no** form of this command.

metric-list {**intf** | **cpu** | **memory**}

no metric-list {intf | cpu | memory}

Syntax Description

intf	(Optional) Monitor interface metrics.
cpu	(Optional) Monitor CPU metrics.
memory	(Optional) Monitor memory metrics.

Command Default

The interface metrics are monitored.

Command Modes

System profile configuration (config-mt-prof-sys)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no metric list is specified, Interface metrics are monitored.

Examples

The following example shows how to specify that CPU metrics are monitored:

```
Router(config)# mediatrace profile system sp-4
Router(config-mt-prof-sys)# metric-list cpu
```

Related Commands

Command	Description
mediatrace profile system	Configures Mediatrace system profiles.

min-sequential

To configure the minimum number of packets in a sequence used to classify a Real-Time Transport Protocol (RTP) flow for a Mediatrace performance monitoring profile, use the **min-sequential** command in RTP parameters configuration mode. To return to the default setting, use the **no** form of this command.

min-sequential *number*

no min-sequential *number*

Syntax Description

number	Minimum number of packets in a sequence used to classify a RTP flow.

Command Default

The minimum number of packets in a sequence is set to 5.

Command Modes

RTP parameters configuration (config-mt-prof-perf-rtp-params)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The maximum value for the minimum number of packets in a sequence used to classify a RTP flow is 10.

Examples

The following example shows how to configure the minimum number of packets in a sequence used to classify a RTP flow for a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# metric-list rtp
Router(config-mt-prof-perf-rtp-params)# min-sequential 4
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

path-specifier

To associate a Mediatrace path-specifier profile with a Mediatrace session, use the **path-specifier** command in session configuration mode. To remove the association, use the **no** form of this command.

path-specifier *name*

no path-specifier *name*

Syntax Description

name	Name used to identify the profile.

Command Default

No path-specifier profile is configured.

Command Modes

Session configuration (config-mt-session)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can associate a path-specifier profile with one or more actual Mediatrace sessions.

Examples

The following example shows how to associate a Mediatrace path-specifier profile to a Mediatrace session:

```
Router(config)# mediatrace 4
Router(config-mt-session)# path-specifier ps-4
```

Related Commands

Command	Description
mediatrace	Configures a Mediatrace session.

profile perf-monitor

To associate a performance monitoring profile and a flow-specifier profile with a Mediatrace session, use the **profile perf-monitor** command in session configuration mode. To remove the association, use the **no** form of this command.

profile perf-monitor *pm-name* **flow-specifier** *fs-name*

no profile perf-monitor *pm-name* **flow-specifier** *fs-name*

Syntax Description

pm-name	Name used to identify the performance monitoring profile to associate with a Mediatrae session.
flow-specifier *fs-name*	Specifies the name of the flow-specifier profile to associate with a Mediatrae session.

Command Default

No performance monitoring profile is configured.

Command Modes

Session configuration (config-mt-session)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can associate a performance monitoring profile with one or more actual Mediatrace sessions.

Examples

The following example shows how to associate a Mediatrace performance monitoring profile to a Mediatrace session:

```
Router(config)# mediatrace 4
Router(config-mt-session)# profile perf-monitor pm-4 flow-specifier fs-2
```

Related Commands

Command	Description
mediatrace	Configures a Mediatrace session.

profile system

To associate a Mediatrace system profile to a Mediatrace session, use the **profile system** command in session configuration mode. To remove the association, use the **no** form of this command.

profile system *name*

no profile system *name*

Syntax Description

name	Name used to identify the profile.

Command Default

No system profile is configured.

Command Modes

Session configuration (config-mt-session)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can associate a system profile with one or more actual Mediatrace sessions.

Examples

The following example shows how to associate a Mediatrace system profile to a Mediatrace session:

```
Router(config)# mediatrace 4
Router(config-mt-session)# profile system sprofile-4
```

Related Commands

Command	Description
mediatrace	Configures a Mediatrace session.

response-timeout (session parameters)

To configure the number of seconds the Mediatrace Initiator will wait for the Responder to provide metrics, use the **response-timeout** command in session parameters configuration mode. To return to the default setting, use the **no** form of this command.

response-timeout *seconds*

no response-timeout *seconds*

Syntax Description

seconds	The number of seconds the Mediatrace Initiator will wait for the Responder to provide metrics.

Command Default

The response-timeout is set to 60 seconds.

Command Modes

Session parameters configuration (config-mt-sesparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The maximum value for the response-timeout is 65535 seconds. The response timeout should be less than the frequency.

Examples

The following example shows how to configure the response-timeout for a session parameters:

```
Router(config)# mediatrace session-params sess-4
Router(config-mt-sesparam)# response-timeout 20
```

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

route-change reaction-time

To configure the number of seconds the Mediatrace Initiator will wait for a response to a route change notification, use the **route change** command in session parameters configuration mode. To return to the default setting, use the **no** form of this command.

route-change reaction-time *seconds*

no route-change reaction-time *seconds*

Syntax Description

seconds	Number of seconds the Mediatrace Initiator will wait for a response to a route change notification.

Command Default

The route change reaction time is set to 5 seconds.

Command Modes

Session parameters configuration (config-mt-sesparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The maximum value for the route change reaction time is 60 seconds.

Examples

The following example shows how to configure the route change reaction time for a session parameters:

```
Router(config)# mediatrace session-params sess-4
Router(config-mt-sesparam)# route-change reaction-time 20
```

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

sampling-interval

To configure the interval, in seconds, between samples taken of metrics for a Mediatrace performance monitoring profile, use the **sampling-interval** command in admin parameters configuration mode. To return to the default setting, use the **no** form of this command.

sampling-interval *seconds*

no sampling-interval *seconds*

Syntax Description

seconds	Number of seconds between samples are taken of metrics.

Command Default

The sampling interval is set to 30 minutes.

Command Modes

Admin parameters configuration (config-mt-prof-perf-params)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The sampling interval can set to a maximum of 30 minutes.

Examples

The following example shows how to configure the sampling interval for a performance monitoring profile:

```
Router(config)# mediatrace profile perf-monitor v-mon-4
Router(config-mt-prof-perf)# admin-params
Router(config-mt-prof-perf-params)#sampling-interval 10
```

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

session-params

To associate a Mediatrace session-params profile to a Mediatrace session, use the **session-params** command in session configuration mode. To remove the association, use the **no** form of this command.

session-params *name*

no session-params *name*

Syntax Description

name	Name used to identify the profile.

Command Modes

Session configuration (config-mt-session)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can associate a session-params profile with one or more actual Mediatrace sessions.

Examples

The following example shows how to associate a Mediatrace session-params profile to a Mediatrace session:

```
Router(config)# mediatrace 4
Router(config-mt-session)# session-params sp-4
```

Related Commands

Command	Description
mediatrace	Configures a Mediatrace session.

show mediatrace flow-specifier

To display the parameters configured for flow-specifier profiles, use the **show mediatrace flow-specifier** command in privileged EXEC mode.

show mediatrace flow-specifier [*name*]

Syntax Description

name	(Optional) Name used to identify the profile.

Command Default

All flow-specifier profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no flow-specifier profile name is entered with this command, all profiles are displayed.

Examples

The following example displays flow-specifier profiles:

```
Router# show mediatrace flow-specifier flow-1
Flow Specifier: flow-1
    Source address/port:
    Destination address/port:
    Protocol: udp
```

Table 8 describes the significant fields shown in the display.

Table 8 show mediatrace flow-specifier Field Descriptions

Field	Description
Flow Specifier	Name assigned to the profile.
Source address/port	Address of the source node.
Destination address/port	Address of the destination node.
Protocol	Whether metrics are collected for TCP or UDP.

Related Commands

Command	Description
mediatrace flow-specifier	Configures Mediatrace monitoring flow specifier.

show mediatrace initiator

To display the parameters configured for the Mediatrace Initiator profile, use the **show mediatrace initiator** command in privileged EXEC mode.

show mediatrace initiator

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

There is only one Mediatrace Initiator profile that can be displayed.

Examples

The following example displays the Mediatrace Initiator profile:

```
Router# show mediatrace initiator

Version: Mediatrace 1.0
Mediatrace Initiator status: enabled

Source IP: 1.1.1.1

Number of Maximum Allowed Active Session: 127
Number of Configured Session: 1
Number of Active Session    : 0
Number of Pending Session   : 0
Number of Inactive Session  : 1

Note: the number of active session may be higher than max active session
      because the max active session count was changed recently.
```

Table 9 describes the significant fields shown in the display.

Table 9 show mediatrace initiator Field Descriptions

Field	Description
Verion	Version of the Mediatrace software.
Mediatrace Initiator status	Whether the Initiator is enabled.
Source IP	IP address of the Initiator.
Number of Maximum Allowed Active Session	Maximum number of active sessions allowed on the Initiator.
Number of Configured Session	Number of sessions configured on the Initiator.

Table 9 show mediatrace initiator Field Descriptions (continued)

Field	Description
Number of Active Session	Number of sessions active on the Initiator.
Number of Pending Session	Number of sessions pending on the Initiator.
Number of Inactive Session	Number of inactive sessions on the Initiator.

Related Commands

Command	Description
mediatrace path-specifier	Configures Mediatrace monitoring path specifier.

show mediatrace path-specifier

To display the parameters configured for path-specifier profiles, use the **show mediatrace path-specifier** command in privileged EXEC mode.

show mediatrace path-specifier [*name*]

Syntax Description

name	(Optional) Name used to identify the profile.

Command Default

All path-specifier profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no path-specifier profile name is entered with this command, all profiles are displayed.

Examples

The following example displays path-specifier profiles:

```
Router# show mediatrace path-specifier flow-1
Path Configuration: ps1
    Destination address/port: 10.10.10.1
    Source address/port: 10.10.10.4
    Gateway address/vlan:
    Discovery protocol: rsvp
```

Table 12 describes the significant fields shown in the display.

Table 10 show mediatrace path-specifier Field Descriptions

Field	Description
Path Configuration	Name of the path-specifier configuration.
Destination address/port	Address of the node at the end of the flow.
Source address/port	Address of the node at the beginning of the flow.
Gateway address/port	Address of the gateway.
Discovery protocol	Protocol used for path discovery.

Related Commands

Command	Description
mediatrace path-specifier	Configures Mediatrace monitoring path specifier.

show mediatrace profile system

To display the parameters configured for system-data profiles, use the **show mediatrace profile system** command in privileged EXEC mode.

show mediatrace profile system [*name*]

Syntax Description

name	(Optional) Name used to identify the profile.

Command Default

All system-data profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no system-data profile name is entered with this command, all profiles are displayed.

Examples

The following example displays system-data profiles:

```
Router# show mediatrace profile system
System Profile: sys-1
Metric List: intf
```

Table 11 describes the significant fields shown in the display.

Table 11 show mediatrace profile system Field Descriptions

Field	Description
System Profile	Name assigned to the profile.
Metric List	Whether metrics are collected for interfaces, CPUs, or memory.

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

show mediatrace profile perf-monitor

To display the parameters configured for performance monitoring profiles, use the **show mediatrace profile perf-monitor** command in privileged EXEC mode.

show mediatrace profile perf-monitor [*name*]

Syntax Description

name	(Optional) Name used to identify the profile.

Command Default

All performance monitoring profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no performance monitoring profile name is entered with this command, all profiles are displayed.

Examples

The following example displays performance monitoring profiles:

```
Router# show mediatrace profile perf-monitor
Perf-monitor Profile: vprof-4
Metric List: rtp
RTP Admin Parameter:
  Max Dropout: 5
  Max Reorder: 5
  Min Sequential: 5
Admin Parameter:
  Sampling Interval (sec): 30
```

Table 12 describes the significant fields shown in the display.

Table 12 show mediatrace profile perf-monitor Field Descriptions

Field	Description
Perf-monitor Profile	Name assigned to the profile.
Metric List	Whether metrics are collected for TCP or Real-Time Transport Protocol (RTP).
Max Dropout	Maximum number of packets to ignore ahead the current packet in terms of sequence number.
Max Reorder	Maximum number of packets to ignore behind the current packet in terms of sequence number.

Table 12 show mediatrace profile perf-monitor Field Descriptions (continued)

Field	Description
Min Sequential	Minimum minimum number of packets in a sequence used to classify a RTP flow.
Sampling Interval	Duration of the sampling interval in seconds.

Related Commands

Command	Description
mediatrace profile perf-monitor	Configures Mediatrace performance monitoring profiles.

show mediatrace responder app-health

To display application health information for the Mediatrace Responder, use the **show mediatrace responder app-health** command in privileged EXEC mode.

show mediatrace responder app-health

Syntax Description

This command has no arguments or keywords.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example displays application health information for the Mediatrace Responder:

```
Router# show mediatrace responder app-health
Mediatrace App-Health Stats:
   Number of all requests received: 0
   Time of the last request received:
   Initiator ID of the last request received:  0
   Requests dropped due to queue full: 0
   Responder current max sessions: 45
   Responder current active sessions: 0
   Session down or tear down requests received: 0
   Session timed out and removed: 0
   HOPS requests received: 0
   VM dynamic polling requests received: 0
   VM dynamic polling failed: 0
   VM configless polling requests received: 0
   VM configless polling failed: 0
   SYSTEM data polling requests received: 0
   SYSTEM data polling requests failed: 0
   APP-HEALTH polling requests received: 0
   Route Change or Interface Change notices received: 0
   Last time Route Change or Interface Change:
   Unknown requests received: 0
```

Table 13 describes the significant fields shown in the display.

Table 13 show mediatrace respnder app-health Field Descriptions

Field	Description
Number of all requests received	Number of requests received by the Responder.
Time of the last request received	When the last request received by the Responder.
Initiator ID of the last request received	ID of the Initiator that sent the last request received by the Responder.

Table 13 show mediatrace respnder app-health Field Descriptions (continued)

Field	Description
Requests dropped due to queue full	Number of requests dropped because the queue was full.
Responder current max sessions	Number of current max sessions on the Responder.
Responder current active sessions	Number of current active sessions on the Responder.
Session down or tear down requests received	Number of session down or tear down requests received by the Responder.
Session timed out and removed	Number of sessions that timed out and were removed by the Responder.
HOPS requests received	Number of HOPS requests received by the Responder.
VM dynamic polling requests received	Number of VM dynamic polling requests received by the Responder.
VM dynamic polling failed	Number of VM dynamic polls that failed.
VM configless polling requests received	Number of VM configless polling requests received by the Responder.
VM configless polling failed	Number of VM configless polls that failed.
SYSTEM data polling requests received	Number of SYSTEM data polling requests received by the Responder.
SYSTEM data polling requests failed	Number of SYSTEM data polling requests that failed.
APP-HEALTH polling requests received	Number of APP-HEALTH polling requests received by the Responder.
Route Change or Interface Change notices received	Number of Route Change or Interface Change notices received by the Responder.
Last time Route Change or Interface Change	When the last time Route Change or Interface Change occurred.
Unknown requests received	Number of Unknown requests received by the Responder.

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

show mediatrace responder sessions

To display session information for the Mediatrace Responder, use the **show mediatrace responder sessions** command in privileged EXEC mode.

show mediatrace responder sessions [*global-session-id* | **brief** | **details**]

Syntax Description

global-session-id	ID of the Mediatrace session for which to display information.
brief	Displays only the destination and source address/port of the path, their role as either Initiator or Responder, and some state information.
details	Displays all session information.

Command Default

The detailed session information is displayed for the Mediatrace Responder

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no session ID is entered with this command, inforamtion for all sessions is displayed.

Examples

The following example displays brief session information for the Mediatrace Responder:

```
Router# show mediatrace responder sessions brief

Local Responder configured session list:
Current configured max sessions: 45
Current number of active sessions: 0
session-id initiator-name       src-ip          src-port   dst-ip          dst-port det-l
  2        host-18           10.10.10.2         200        10.10.10.8         200
```

Table 14 describes the significant fields shown in the display.

Table 14 show mediatrace responder breif sessions Field Descriptions

Field	Description
Current configured max sessions	Number of maximum sessions curerntly configured on the Responder.
Current number of active sessions	Number of sessions curerntly active on the Responder.
session-id	ID of each active session.

Table 14 show mediatrace responder breif sessions Field Descriptions (continued)

Field	Description
initiator-name	Host name of the Initiator for each session.
src-ip	IP address of the source of the flow for each session.
src-port	Port of the source of the flow for each session.
dst-ip	IP address of the destination of the flow for each session.
dst-port	Port of the destination of the flow for each session.

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

show mediatrace session

To display information for Mediatrace sessions, use the **show mediatrace session** command in privileged EXEC mode.

show mediatrace session [**config** | **data** | **hops** | **stats**]

Syntax Description

config	(Optional) Display configuration information for Mediatrace sessions.
data	(Optional) Display data collected for Mediatrace sessions.
hops	(Optional) Display hop information for Mediatrace sessions.
stats	(Optional) Display statistics for Mediatrace sessions.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You must have at least one active session before most session information can be displayed.

Examples

The following example displays session configuration information:

```
Router# show mediatrace session config

Session Index: 1
Global Session Id: 0
---------------------------
Session Details:
    Path-Specifier: ps1
    Session Params: sp1
    Collectable Metrics Profile: s1
    Flow Specifier: fs1
Schedule:
   Operation frequency (seconds): 120  (not considered if randomly scheduled)
   Next Scheduled Start Time: Pending trigger
   Group Scheduled : FALSE
   Randomly Scheduled : FALSE
   Life (seconds): 3600
   Entry Ageout (seconds): never
   Recurring (Starting Everyday): FALSE
   Status of entry (SNMP RowStatus): notInService
```

Table 16 describes the significant fields shown in the display.

Table 15 show mediatrace profile perf-monitor Field Descriptions

Field	Description
Session Index	Local ID number of the Mediatrace session.
Global Session Id	Global ID number of the Mediatrace session.
Path-Specifier	Name of the Mediatrace path-specifier associated with this session.
Session Params	Name of the Mediatrace session parameters profile associated with this session.
Collectable Metrics Profile	Name of the Mediatrace collectable metrics profile associated with this session.
Flow Specifier	Name of the Mediatrace flow-specifier associated with this session.
Operation frequency (seconds)	Interval between sessions/
Next Scheduled Start Time	Time that the next session will start.
Group Scheduled	Whether this session is part of a group of scheduled sessions.
Randomly Scheduled	Whether this session is part of a regularly occurring schedule of sessions.
Life (seconds)	Duration of the session.
Entry Ageout (seconds)	Amount of time before entries are removed.
Recurring (Starting Everyday)	Whether this session is part of a recurring schedule of sessions.
Status of entry (SNMP RowStatus)	Status of the SNMP entry.

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

show mediatrace session-params

To display the parameters configured for Mediatrace sessions, use the **show mediatrace session-params** command in privileged EXEC mode.

show mediatrace session-params [*name*]

Syntax Description

name	(Optional) Name used to identify the profile.

Command Default

All session profiles are displayed.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no session profile name is entered with this command, all profiles are displayed.

Examples

The following example displays session profiles:

```
Router# show mediatrace session-params
Session Parameters: s-1
    Response timeout (sec): 60
    Frequency: On Demand
    Inactivity timeout (sec): 300
    History statistics:
       Number of history buckets kept: 3
    Route change:
       Reaction time (sec): 5
```

Table 16 describes the significant fields shown in the display.

Table 16 show mediatrace profile perf-monitor Field Descriptions

Field	Description
Session Parameters	Name assigned to the session profile.
Response timeout	Number of seconds the Mediatrace Initiator will wait for the Responder to provide metrics for a Mediatrace session.
Frequency	Amount of time between samples taken for a Mediatrace session.
Inactivity timeout	Number of seconds the Mediatrace Initiator will wait without any activity from the Responder for a Mediatrace session.

Table 16 show mediatrace profile perf-monitor Field Descriptions (continued)

Field	Description
Number of history buckets	Number of history buckets retained for metrics collected for a Mediatrace session.
Reaction time	Number of seconds the Mediatrace Initiator will wait for a response to a route change notification for a Mediatrace session.

Related Commands

Command	Description
mediatrace session-params	Configures parameters for Mediatrace sessions.

source-ip (flow)

To configure the IP address of the source node for the flow, use the **source-ip** command in flow configuration mode. To remove the configuration for the source node, use the **no** form of this command.

source-ip *ip-address* [**source-port** *port*]

no source-ip *ip-address* [**source-port** *port*]

Syntax Description

ip-address	IP address of the source node for the flow.
source-port *port*	Port number of the source node for the flow.

Command Modes

Flow configuration (config-mt-flowspec)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

When specifying the IP address of the source node for the flow, the port number is optional.

Examples

The following example shows how to configure the IP address of the source node for the flow:

```
Router(config)# mediatrace flow-specifier flow-4
Router(config-mt-flowspec)# source-ip 10.10.10.4
```

Related Commands

Command	Description
mediatrace flow-specifier	Configures Mediatrace flow specifier.

source ip (path)

To configure the IP address of the source node for the path, use the **source-ip** command in path configuration mode. To remove the configuration for the source node, use the **no** form of this command.

source ip *ip-address* [**port** *port*]

no source ip *ip-address* [**port** *port*]

Syntax Description

ip-address	IP address of the source node for the path.
port *port*	Port number of the source node for the path.

Command Modes

Path configuration (config-mt-path)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

When specifying the IP address of the source node for a path, the port number is optional.

Examples

The following example shows how to configure the IP address of the source node for the path:

```
Router(config)# mediatrace path-specifier path-4
Router(config-mt-path)# source ip 10.10.10.4
```

Related Commands

Command	Description
mediatrace path-specifier	Configures Mediatrace path specifiers

Cisco Performance Monitor Commands

action (policy react and policy inline react)

To configure which applications which will receive an alarm or notification, use the **action** command in policy react configuration mode and policy inline react configuration mode. To disable the sending alarms or notifications, use the **no** form of this command.

action {**syslog** | **snmp** | **eem**}

no action {**syslog** | **snmp** | **eem**}

Syntax Description

syslog	Sends an alarm or notification to the syslog.
snmp	Sends an alarm or notification to the SNMP MIB variables.
eem	Sends an alarm or notification to Cisco Embedded Event Manager.

Command Default

Information is saved to syslog.

Command Modes

Policy react configuration (config-pmap-c-react)
Policy inline react configuration (config-spolicy-inline-react)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can configure multiple action commands to allow more than one recipients to receive an alarm or notification.

Examples

The following example shows how to specify that SNMP MIB variables will receive an alarm or notification, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# react 2000 rtp-jitter-average
Router(config-pmap-c-react)# action snmp
```

The following example shows how to specify that SNMP MIB variables will receive an alarm or notification, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# react 2000 rtp-jitter-average
Router(config-spolicy-inline-react)# action snmp
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

alarm severity (policy react and policy inline react)

To configure the severity of alarms sent for a Performance Monitor policy, use the **alarm severity** command in policy react configuration mode and policy inline react configuration mode. To return to the default and send all alarms, use the **no** form of this command.

alarm severity {**alert** | **critical** | **emergency** | **error | info**}

no alarm severity {**alert** | **critical** | **emergency** | **error | info**}

Syntax Description

alert	Sends only alerts.
critical	Sends only critical alarms.
emergency	Sends only emergency alarms.
error	Sends only errors.
info	Sends only informational messages.

Command Default

All alarm severities are sent.

Command Modes

Policy react configuration (config-pmap-c-react)
Policy inline react configuration (config-spolicy-inline-react)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The definition of the alarms types are listed below in order of severity:

- Emergency—System unusable
- Alert—Immediate action needed
- Critical—Critical condition
- Error—Error condition

Examples

The following example shows how to specify that only emergency alarms will be sent, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# react 2000 rtp-jitter-average
Router(config-pmap-c-react)# alarm severity emergency
```

The following example shows how to specify that only emergency alarms will be sent, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# react 2000 rtp-jitter-average
Router(config-spolicy-inline-react)# alarm severity emergency
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

alarm type (policy react and policy inline react)

To configure the types of alarms sent for a Performance Monitor policy, use the **alarm type** command in policy react configuration mode and policy inline react configuration mode. To return to the default and send all alarms, use the **no** form of this command.

alarm type {**discrete** | **grouped** {**count** *number* | **percent** *number*}

no alarm type {**discrete** | **grouped** {**count** *number* | **percent** *number*}

Syntax Description

discrete	Sends only individual alarms.
grouped	Sends only grouped alarms.
count *number*	Send alarms only when the count of the monitored event is above the specified number
percent *number*	Send alarms only when percentage of the monitored event is above the specified number.

Command Default

Alarm type is set to discrete.

Command Modes

Policy react configuration (config-pmap-c-react)
Policy inline react configuration (config-spolicy-inline-react)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The monitored event is specified by the **react** command. You can group alarms by whether they exceed a specified percentage or count.

Examples

The following example shows how to specify that only percentage type alarms will be sent, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# react 2000 rtp-jitter-average
Router(config-pmap-c-react)# alarm type percent 80
```

The following example shows how to specify that only percentage type alarms will be sent, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# react 2000 rtp-jitter-average
Router(config-spolicy-inline-react)# alarm type percent 80
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

class-map

To create a class map to be used for matching packets to a specified class, use the **class-map** command in global configuration mode. To remove an existing class map from the router, use the **no** form of this command. The **class-map** command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, and 7500 Series Routers

class-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-class*}] [**match-all** | **match-any**] *class-map-name*

no class-map [**type** {**stack** | **access-control** | **port-filter** | **queue-threshold** | **logging** *log-class*}] [**match-all** | **match-any**] *class-map-name*

Cisco 7600 Series Routers

class-map *class-map-name* [**match-all** | **match-any**]

no class-map *class-map-name* [**match-all** | **match-any**]

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

class-map *class-map-name*

no class-map *class-map-name*

Syntax Description

type stack	(Optional) Enables flexible packet matching (FPM) functionality to determine the correct protocol stack to examine. If the appropriate protocol header description files (PHDFs) have been loaded onto the router (via the **load protocol** command), a stack of protocol headers can be defined so that the filter can determine which headers are present and in what order.
type access-control	(Optional) Determines the exact pattern to look for in the protocol stack of interest. **Note** You must specify a stack class map (via the **type stack** keywords) before you can specify an access-control class map (via the **type access-control** keywords).
type port-filter	(Optional) Creates a port-filter class map that enables the TCP/UDP port policing of control plane packets. When enabled, it provides filtering of traffic that is destined to specific ports on the control-plane host subinterface.
type queue-threshold	(Optional) Enables queue thresholding that limits the total number of packets for a specified protocol that are allowed in the control plane IP input queue. This feature applies only to the control-plane host subinterface.
type logging *log-class*	(Optional) Enables logging of packet traffic on the control plane. The *log-class* is the name of the log class.

match-all	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical AND function. One statement and another are accepted. If you do not specify the **match-all** or **match-any** keyword, the default keyword is **match-all**.
match-any	(Optional) Determines how packets are evaluated when multiple match criteria exist. Matches statements under this class map based on the logical OR function. One statement or another is accepted. If you do not specify the **match-any** or **match-all** keyword, the default keyword is **match-all**.
class-map-name	Name of the class for the class map. The class name is used for both the class map and to configure a policy for the class in the policy map.

Command Default

No class map is configured by default.

Command Modes

Global configuration (config)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(14)SX	This command was integrated into Cisco IOS Release 12.2(14)SX and implemented on the Cisco 7600 series routers.
12.2(17d)SXB	This command was integrated into Cisco IOS Release 12.2(17d)SXB and implemented on the Cisco 7600 series routers.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.4(4)T	This command was modified. The **type stack** and **type access-control** keywords were added to support FPM. The **type port-filter** and **type queue-threshold** keywords were added to support Control Plane Protection.
12.4(6)T	This command was modified. The **type logging** keyword was added to support control plane packet logging.
12.2(18)ZY	This command was modified. The **type stack** and **type access-control** keywords were integrated into Cisco IOS Release 12.2(18)ZY on the Catalyst 6500 series of switches equipped with the Programmable Intelligent Services Accelerator (PISA)
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on the Cisco ASR 1000 Series Routers.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with only the *class-map-name* argument.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with only the *class-map-name* argument.

Usage Guidelines

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

Only the *class-map-name* argument is available.

Cisco 2600, 3660, 3845, 6500, 7200, 7401, 7500, and ASR 1000 Series Routers

Use the **class-map** command to specify the class that you will create or modify to meet the class-map match criteria. This command enters class-map configuration mode in which you can enter one of the **match** commands to configure the match criteria for this class. Packets that arrive at either the input interface or the output interface (determined by how the **service-policy** command is configured) are checked against the match criteria configured for a class map to determine if the packets belong to that class.

When configuring a class map, you can use one or more **match** commands to specify match criteria. For example, you can use the **match access-group** command, the **match protocol** command, or the **match input-interface** command. The **match** commands vary according to the Cisco IOS release. For more information about match criteria and **match** commands, see the "Modular Quality of Service Command-Line Interface (CLI) (MQC)" chapter of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 7600 Series Routers

You apply the **class-map** command and its commands on a per-interface basis to define packet classification, marking, aggregate, and flow policing as part of a globally named service policy.

You can attach a service policy to an EtherChannel. Do not attach a service policy to a port that is a member of an EtherChannel.

After the router is in class-map configuration mode, the following configuration commands are available:

- **exit**—Used to exit from class-map configuration mode.
- **no**—Used to remove a match statement from a class map.
- **match**—Used to configure classification criteria. The following optional **match** commands are available:
  - **access-group** {*acl-index* | *acl-name*}
  - **ip** {**dscp** | **precedence**} *value1 value2 ... value8*

The following commands appear in the CLI help but are not supported on LAN interfaces or WAN interfaces on the Optical Service Modules (OSMs):

- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **destination-address mac** *mac-address*
- **source-address mac** *mac-address*

OSMs are not supported on Cisco 7600 series routers that are configured with a Supervisor Engine 32.

Policy Feature Card (PFC) QoS does not support the following commands:

- **input-interface** {*interface-type interface-number* | **null** *number* | **vlan** *vlan-id*}
- **protocol** *link-type*
- **destination-address mac** *mac-address*
- **source-address mac** *mac-address*
- **qos-group** *group-value*

If you enter these commands, PFC QoS does not detect the unsupported keywords until you attach a policy map to an interface. When you try to attach the policy map to an interface, you get an error message. For additional information, see the *Cisco 7600 Series Router Cisco IOS Software Configuration Guide* and the Cisco IOS command references.

After you have configured the class-map name and are in class-map configuration mode, you can enter the **match access-group** and **match ip dscp** commands. The syntax for these commands is as follows:

match [[**access-group** {*acl-index* | *acl-name*}] | [**ip** {**dscp** | **precedence**} *value*]]

See Table 8 for a syntax description of the **match** commands.

Table 8 match command Syntax Description

Optional command	Description
access-group *acl-index* | *acl-name*	(Optional) Specifies the access list index or access list names; valid access list index values are from 1 to 2699.
access-group *acl-name*	(Optional) Specifies the named access list.
ip dscp *value1 value2 ... value8*	(Optional) Specifies the IP DSCP values to match; valid values are from 0 to 63. You can enter up to 8 DSCP values and separate each value with one white space.
ip precedence *value1 value2 ... value8*	(Optional) Specifies the IP precedence values to match; valid values are from 0 to 7. You can enter up to 8 precedence values and separate each value with one white space.

Examples

The following example specifies class101 as the name of a class, and it defines a class map for this class. The class named class101 specifies policy for traffic that matches access control list 101.

```
Router(config)# class-map class101
Router(config-cmap)# match access-group 101
```

The following example shows how to define FPM traffic classes for slammer and UDP packets. The match criteria defined within the class maps are for slammer and UDP packets with an IP length not to exceed 404 bytes, UDP port 1434, and pattern 0x4011010 at 224 bytes from the start of the IP header.

```
Router(config)# load protocol disk2:ip.phdf
Router(config)# load protocol disk2:udp.phdf

Router(config)# class-map type stack match-all ip-udp
Router(config-cmap)# description "match UDP over IP packets"
Router(config-cmap)# match field ip protocol eq 0x11 next udp

Router(config)# class-map type access-control match-all slammer
Router(config-cmap)# description "match on slammer packets"
Router(config-cmap)# match field udp dest-port eq 0x59A
Router(config-cmap)# match field ip length eq 0x194
Router(config-cmap)# match start 13-start offset 224 size 4 eq 0x4011010
```

The following example shows how to configure a port-filter policy to drop all traffic that is destined to closed or "nonlistened" ports except SNMP.

```
Router(config)# class-map type port-filter pf-class
Router(config-cmap)# match not port udp 123
Router(config-cmap)# match closed-ports
Router(config-cmap)# exit
Router(config)# policy-map type port-filter pf-policy
```

```
Router(config-pmap)# class pf-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# end
```

The following example shows how to configure a class map named ipp5, and enter a match statement for IP precedence 5:

```
Router(config)# class-map ipp5
Router(config-cmap)# match ip precedence 5
```

Related Commands

Command	Description
class (policy-map)	Specifies the name of the class whose policy you want to create or change, and the default class (commonly known as the class-default class) before you configure its policy.
class class-default	Specifies the default class for a service policy map.
match (**class-map**)	Configures the match criteria for a class map on the basis of port filter and/or protocol queue policies.
match access-group	Configures the match criteria for a class map on the basis of the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match ip dscp	Identifies one or more DSCP, AF, and CS values as a match criterion
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or virtual circuit (VC) or to an output interface or VC to be used as the service policy for that interface or VC.
show class-map	Displays class-map information.
show policy-map interface	Displays the statistics and the configurations of the input and output policies that are attached to an interface.

clock-rate (policy RTP)

To configure the rate for the RTP packet time-stamp clock, use the **clock-rate** command in policy RTP configuration mode. To remove the configuration, use the **no** form of this command.

clock-rate {*type-number* | *type-name*} *rate*

no clock-rate

Syntax Description

type-number	An integer between 0 and 34. This value is compared with the payload type field in the RTP header. Values between 0 and 23 are reserved for audio streams, and values between 24 and 34 are reserved for video streams.
type-name	The name of the payload type field in the RTP header.
rate	Clock rate in Hz. The range is from 9600 to 124000.

Command Default

Clock rate is 90000.

Command Modes

policy RTP configuration (config-pmap-c-mrtp)
policy inline RTP configuration (config-spolicy-inline-mrtp)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

For more information about how the clock rate for RTP packet time-stamp clock is used to calculate the packet arrival latency, see RFC 3550, *RTP, A Transport Protocol for Real-Time Applications*. The clock rate has to be synchronized with the routers along the path of the flow. Because the clock rate can vary depending on the payload codec type, a keyword is provided to set the expected clock rate.

The available values for *type-name and type-number* are celb (25), cn (13), dvi4 (5) (8000 Hz as described in RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*), dvi4-2 (6) (8000 Hz as described in RFC 3551), dvi4-3 (16) (DVI4 Dipol 11025 Hz), dvi4-4 (17) DVI4 Dipol 22050 Hz), g722 (9), g723 (4), g728 (15), g729 (18), gsm (3), h261 (31), h263 (34), jpeg (26), l16 (11) (L16 channel 1), l16-2 (10) (L16 channel 2), lpc (7), mp2t (33), mpa (14), mpv (32), nv (28), pcma (8), pcmu (0), qcelp (12).

Examples

The following example shows how to set the rate for the RTP packet time-stamp clock,while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric rtp
Router(config-pmap-c-mrtp)# clock-rate 8 9600
```

The following example shows how to set the rate for the RTP packet time-stamp clock, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric rtp
Router(config-spolicy-inline-mrtp)# clock-rate 8 9600
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

collect application media

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

collect application media {**bytes** {**rate | counter** [**long**]} | **packets** {**rate** [**variation**] **| counter** [**long**]}| **events**}

no collect application media {**bytes** | **packets | events**}

Syntax Description

bytes rate	Configures the field that counts the rate of bytes collected, in Bps, for all flows, as a nonkey field.
bytes counter	Configures the field that counts the total number of bytes collected, as a nonkey field.
long	Configures the field for the long count (byte or packet) as a nonkey field.
packets rate	Configures the field that counts the total number of application media packets collected, per second, for all flows, as a nonkey field.
variation	Configures the field for the variation in the rate application media packets collected, for all flows, as a nonkey field.
packets counter	Configures the filed that counts the total number of application media packets collected, for all flows, as a nonkey field.
events	Configures the field that indicates whether one of the media application thresholds configured for the flow was crossed at least once in the monitoring interval, field as a nonkey field.

Command Default

The application media field is not configured as a nonkey field for a user-defined flow record.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The **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 application media packet field as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect application media packets
```

Related Commands

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

collect counter

To configure one of the counter fields as a nonkey field for a flow record, use the **collect counter** command in flow record configuration mode. To disable the use of one of the counter fields as a nonkey field for a flow record, use the **no** form of this command.

collect counter {**bytes** [**long** | **rate**] | **packets** [**dropped** [**long**] | **long**]}

no collect counter {**bytes** [**long** | **rate**] | **packets** [**dropped** [**long**] | **long**]}

Syntax Description

bytes	Configures the byte counter field as a nonkey field.
long	Configures the counter for the number of long bytes or packets as a nonkey field.
rate	Configures the byte rate counter as a nonkey field.
packets	Configures the packet counter as a nonkey field.
dropped	Configures the dropped packet counter as a nonkey field.

Command Default

The counter fields are not configured as a nonkey field for a user-defined flow record.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The **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 dropped packet counter field as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect counter packets dropped
```

Related Commands

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

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**}

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.

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 flow record, use the **collect ipv4** command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a nonkey field for a 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**}

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

collect ipv4 dscp

no collect ipv4 dscp

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

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.

Release	Modification
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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 with only the **dscp** keyword.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with only the **dscp** keyword.

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.

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 flow record, refer to the **collect ipv4 ttl** command.

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

Only the the **dscp** keyword is available. You must first enter the **flow record type performance-monitor** 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
```

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

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

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# collect ipv4 dscp
```

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 destination

To configure the IPv4 destination address as a nonkey field for a flow record, use the **collect ipv4 destination** command in flow record configuration mode. To disable the use of an IPv4 destination address field as a nonkey field for a 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*]}

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

collect ipv4 destination mask [**minimum-mask** *mask*]}

no collect ipv4 destination mask [**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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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 with only the **mask** and **minimum-mask** keywords.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with only the **mask** and **minimum-mask** keywords.

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

Only the **mask** and **minimum-mask** keywords are available. You must first enter the **flow record type performance-monitor** command.

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
```

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

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 type performance-monitor RECORD-1
Router(config-flow-record)# collect ipv4 destination prefix minimum-mask 16
```

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 source

To configure the IPv4 source address as a nonkey field for a flow record, use the **collect ipv4 source** command in flow record configuration mode. To disable the use of the IPv4 source address field as a nonkey field for a 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*]}

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

collect ipv4 source mask [**minimum-mask** *mask*]}

no collect ipv4 source mask [**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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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 with only the **mask** and **minimum-mask** keywords.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with only the **mask** and **minimum-mask** keywords.

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

Only the **mask** and **minimum-mask** keywords are available. You must first enter the **flow record type performance-monitor** command.

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
```

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

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

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 ttl

To configure the IPv4 time-to-live (TTL) field as a nonkey field for a flow record, use the **collect ipv4 ttl** command in flow record configuration mode. To disable the use of the IPv4 TTL field as a nonkey field for a 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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.

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**.**

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
```

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

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

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# collect ipv4 ttl minimum
```

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 monitor event

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

collect monitor event

no collect monitor event

Syntax Description

This command has no arguments or keywords.

Command Default

The monitor event field is not configured as a nonkey field for a user-defined flow record.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

Monitor events are recorded using two bits. Bit 1 is not used. Bit 2 indicates that no media application packets were seen, in other words, a Media Stop Event occured.

The **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 monitor event field as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect monitor event
```

Related Commands

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

collect routing

To configure one or more of the routing attributes as a nonkey field for a flow record, use the **collect routing** command in flow record configuration mode. To disable the use of one or more of the routing attributes as a nonkey field for a 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**}

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

collect routing forwarding-status [**reason**]

no collect routing forwarding-status [**reason**]

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 nonkey 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 nonkey field.
reason	Configures the reason for the forwarding status as a nonkey field.

Command Default

The routing attributes are 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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and implemented on the Cisco 7200 series routers.
12.4(20)T	This command was modified. The **ipv6** keyword was added.
15.0(1)M	This command was modified. The **vrf input** 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.
Cisco IOS XE Release 3.2S	This command was modified. The **4-octet** keyword was added.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with only the **forwarding-status** keyword and the addition of the **reason** keyword.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with only the **forwarding-status** keyword and the addition of the **reason** keyword.

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

The **reason** keywordwas added and only the **forwarding-status** keyword is available. You must first enter the **flow record type performance-monitor** command.

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
```

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

The following example configures the forwarding status as a nonkey field for a Performance Monitor flow record:

```
Router(config)# flow record type performance-monitor RECORD-1
Router(config-flow-record)# collect routing forwarding-status reason
```

Related Commands

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

collect timestamp interval

To configure the start time of the monitoring interval as a nonkey field for a flow record, use the **collect timestamp interval** command in flow record configuration mode. To disable the use of the start time of the monitoring interval as a nonkey field for a flow record, use the **no** form of this command.

collect timestamp interval

no collect timestamp interval

Syntax Description

This command has no arguments or keywords.

Command Default

The start time of the monitoring interval is not configured as a nonkey field.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The **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 start time of the monitoring interval as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect timestamp interval
```

Related Commands

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

collect transport event packet-loss counter

To configure the event packet-loss counter field as a nonkey field for a flow record, use the **collect transport event packet-loss counter** command in flow record configuration mode. To disable the use of the event packet-loss counter field as a nonkey field for a flow record, use the **no** form of this command.

collect transport event packet-loss counter

no collect transport event packet-loss counter

Syntax Description

This command has no arguments or keywords.

Command Default

The event packet-loss counter field is not configured as a nonkey field for a user-defined flow record.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The event packet-loss counter is incremented when a lost RTP packet is detected. However, the counter is also incremented when a reorder occurs, in other words, when packets are received out of order.

The **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 event packet-loss counter field as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect transport event packet-loss counter
```

Related Commands

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

collect transport packets

To configure various packet fields as a nonkey field for a flow record, use the **collect transport packets** command in flow record configuration mode. To disable the use of a packet field as a nonkey field for a flow record, use the **no** form of this command.

collect transport packets{**lost counter** | **lost rate** | **expected counter** | **round-trip-time**}

no collect transport packets {**lost counter** | **lost rate** | **expected counter** | **round-trip-time**}

Syntax Description

lost counter	Configures the field that counts the number of lost packets as a nonkey field.
lost rate	Configures the field that counts the rate of lost packets as a nonkey field.
expected counter	Configures the field that counts the number of expected packets as a nonkey field.
round-trip-time	Configures the field for the packet round-trip-time as a nonkey field.

Command Default

The packet fields are not configured as a nonkey field for a user-defined flow record.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can retrieve different transport packet counters for RTP and TCP. The following transport packet counters as available:

- rtp lost counter
- rtp lost rate
- rtp expected counter
- tcp transport round-trip-time

The **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 field that counts the number of lost packets as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect transport packets lost counter
```

Related Commands

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

collect transport rtp jitter

To configure one of the RTP jitter fields as a nonkey field for a flow record, use the **collect transport rtp jitter** command in flow record configuration mode. To disable the use of a jitter field as a nonkey field for a flow record, use the **no** form of this command.

collect transport rtp jitter {**mean** | **maximum** | **minimum**}

no collect transport rtp jitter {**mean | maximum** | **minimum**}

Syntax Description

jitter	Configures the RTP jitter field as a nonkey field.
mean	Configures the mean value of the RTP jitter field as a nonkey field.
maximum	Configures the maximun value of the RTP jitter field as a nonkey field.
minimum	Configures the minumum value of the RTP jitter field as a nonkey field.

Command Default

The RTP jitter field is not configured as a nonkey field for a user-defined flow record.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The **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 RTP jitter field as a nonkey field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# collect transport rtp jitter
```

Related Commands

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

debug performance monitor

To enable debugging for performance monitor, use the **debug performance monitor** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

debug performance monitor {**database** | **dynamic** | **event** | **export** | **flow-monitor** | **metering** | **provision** | **sibling** | **snmp** | **tca** | **timer**}

no debug performance monitor {**database** | **dynamic** | **event** | **export** | **flow-monitor** | **metering** | **provision** | **sibling** | **snmp** | **tca** | **timer**}

Syntax Description

database	Enables debugging for the flow database.
dynamic	Enables debugging for dynamic monitoring.
event	Enables debugging for performance events.
export	Enables debugging for exporting.
flow-monitor	Enables debugging for flow monitors.
metering	Enables debugging for the metering layer.
provision	Enables debugging for provisioning.
sibling	Enables debugging for sibling management.
snmp	Enables debugging for SNMP.
tca	Enables debugging for Threshold Crossing Alarms (TCA).
timer	Enables debugging for timers.

Command Default

Debugging for performance monitor is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to enable debugging for dynamic monitoring:

```
Router# debug performance monitor dynamic
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor type performance-monitor	Creates a flow monitor.

description (Performance Monitor)

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

description *description*

no description

Syntax Description

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

Command Default

No description is configured.

Command Modes

Flow exporter configuration (config-flow-exporter)
Flow record configuration (config-flow-record)
Flow monitor configuration (config-flow-monitor)
Policy configuration (config-pmap)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

The description command is meant solely as a comment to be put in the configuration to help you remember information about the flow exporter, flow record, flow monitor, or policy map, such as which packets are included within the policy map.

Examples

The following example shows how to configuration a description for a flow record:

```
Router(config)# flow record type performance-monitor
Router(config-flow-record)# description collect the number of IPV4 packet dropped
Router(config-flow-record)# match ipv4 protocol
Router(config-flow-record)# collect counter packets dropped
```

Related Commands

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

Command	Description
flow monitor type performance-monitor	Creates a flow monitor.
policy-map type performance-monitor	Creates a policy map.

destination

To configure an export destination for a flow exporter, use the **destination** command in flow exporter configuration mode. To remove an export destination for a 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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

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 flow exporter datagrams, use the **dscp** command in flow exporter configuration mode. To remove a DSCP value for 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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.

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.

export-protocol

To configure the export protocol for a flow exporter, use the **export-protocol** command in flow exporter configuration mode. To restore the use of the default export protocol for a flow 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 flow exporter.

Command Modes

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 Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

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 or Performance Monitor flow 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

exporter

To configure a flow exporter for a flow monitor, use the **exporter** command in the appropriate configuration mode. To remove a flow exporter for a 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

flow monitor configuration (config-flow-monitor)
Policy configuration (config-pmap-c)
Policy monitor configuration (config-pmap-c-flowmon)

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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 configuration mode and policy monitor configuration configuration mode.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor.

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.

For Performance Monitor, you can associate a flow exporter with a flow monitor while configuring either a flow monitor, policy map, or service policy.

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
```

The following example shows one of the ways to configure a flow exporter for Performance Monitor:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class class-4
Router(config-pmap-c)# flow monitor monitor-4
Router(config-pmap-c-flowmon)# exporter exporter-4
```

Related Commands

Command	Description
flow exporter	Creates a flow exporter.
flow monitor	Creates a flow monitor.
flow monitor type performance-monitor	Creates a flow monitor for Performance Monitor.
policy-map type performance-monitor	Creates a policy map for Performance Monitor
service-policy type performance-monitor	Associates policy map with an interface for Performance Monitor.

flow monitor type performance-monitor

To configure a flow monitor for Performance Monitor, use the **flow monitor type performance-monitor** command in global configuration mode. To remove flow monitor, use the **no** form of this command.

flow monitor type performance-monitor *monitor-name*

no flow monitor type performance-monitor *monitor-name*

Syntax Description

monitor-name	Specifies which flow monitor is being configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

.Before you configure flow monitor, you should first configure a flow record and an optional flow exporter.

Examples

The following example shows how to configure a flow monitor:

```
Router(config)# flow monitor type performance-monitor PM-MONITOR-4
```

Related Commands

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

flow record type performance-monitor

To configure a flow record for Performance Monitor, use the **flow record type performance-monitor** command in global configuration mode. To remove the flow record, use the **no** form of this command.

flow record type performance-monitor *record-name*

no flow record type performance-monitor *record-name*

Syntax Description

record-name	Specifies which flow record is being configured.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

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 **collect** command.

Examples

The following example shows how to configure a flow record:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
```

Related Commands

Command	Description
flow monitor type performance-monitor	Creates a flow monitor.

flows

To configure the maximum number of flows for each Performance Monitor cache, use the **flows** command in monitor parameters configuration mode. To remove the configuration, use the **no** form of this command.

flows *number*

no flows *number*

Syntax Description

number	Specifies the number of flows to collect for the policy.

Command Default

Number of flows to collect is 8000.

Command Modes

Monitor parameters configuration (config-pmap-c-mparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the number of flows to collect for a Performance Monitor policy to four:

```
Router(config)# policy-map type performance-monitor PM-POLICY-4
Router(config-pamp)# class class-6
Router(config-pmap-c)# monitor parameters
Router(config-pmap-c-mparam)# flows 4
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.

history (monitor parameters)

To configure the number of historical collections to keep for a Performance Monitor policy, use the **history** command in monitor parameters configuration mode. To remove the configuration, use the **no** form of this command.

history *number*

no history

Syntax Description

number	Specifies the number of historical collections to keep for the policy.

Command Default

Number of historical collections to keep is 10.

Command Modes

Monitor parameters configuration (config-pmap-c-mparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the number of historical collections to keep for a Performance Monitor policy to four:

```
Router(config)# policy-map type performance-monitor PM-POLICY-4
Router(config-pamp)# class class-6
Router(config-pmap-c)# monitor parameters
Router(config-pmap-c-mparam)# history 4
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.

interval duration

To configure the duration of the collection interval for a Performance Monitor policy, use the **interval duration** command in monitor parameters configuration mode. To remove the configuration, use the **no** form of this command.

interval duration *duration*

no interval duration

Syntax Description

duration	Specifies the duration of the collection interval for the policy.

Command Default

Duration of the collection interval is 30 seconds.

Command Modes

Monitor parameters configuration (config-pmap-c-mparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the collection interval for a Performance Monitor policy to twenty:

```
Router(config)# policy-map type performance-monitor PM-POLICY-4
Router(config-pamp)# class class-6
Router(config-pmap-c)# monitor parameters
Router(config-pmap-c-mparam)# interval duration 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.

match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **match any** command in policy-map inline configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

match any

no match any

Syntax Description

This command has no arguments or keywords.

Command Default

No match criteria are specified.

Command Modes

Policy-map inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
15.1(3)T	This command was introduced.

Examples

In the following configuration, all packets leaving Ethernet interface 0/0 will be matched based on the parameters specified in policy-map class configuration mode:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service policy type performance monitor inline input
Router(config-if-spolicy-inline)# match any
```

Related Commands

Command	Description
service-policy type performance-monitor inline	Associates a policy with an interface.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group {*access-group* | **name** *access-group-name*}

no match access-group *access-group*

Syntax Description

access-group	Numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
name *access-group-name*	Named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was enhanced to include matching on access lists on the Cisco 10000 series router.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(6)T	This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for policy-map inline configuration mode (config-if-spolicy-inline).

Usage Guidelines

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including ACLs, protocols, input interfaces, quality of service (QoS) labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

Note For Zone-Based Policy Firewall, this command is not applicable to CBWFQ.

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

When packets are matched to an access group, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the 'inspect' action.

Supported Platforms Other than Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

Note Zone-Based Policy Firewall supports only the **match access-group**, **match protocol**, and **match class-map** commands.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when you configure match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when you configure match criteria.

Examples

The following example specifies a class map called acl144 and configures the ACL numbered 144 to be used as the match criterion for that class:

```
class-map acl144
 match access-group 144
```

The following example pertains to Zone-Based Policy Firewall. The example defines a class map called c1 and configures the ACL numbered 144 to be used as the match criterion for that class.

```
class-map type inspect match-all c1
 match access-group 144
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
class-map	Creates a class map to be used for matching packets to a specified class.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match access-group

To configure the match criteria for a class map on the basis of the specified access control list (ACL), use the **match access-group** command in class-map configuration or policy inline configuration mode. To remove ACL match criteria from a class map, use the **no** form of this command.

match access-group {*access-group* | **name** *access-group-name*}

no match access-group *access-group*

Syntax Description

access-group	Numbered ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. An ACL number can be a number from 1 to 2699.
name *access-group-name*	Named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to this class. The name can be a maximum of 40 alphanumeric characters.

Command Default

No match criteria are configured.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was modified. This command was enhanced to include matching on access lists on the Cisco 10000 series routers.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.4(6)T	This command was modified. This command was enhanced to support Zone-Based Policy Firewall.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including ACLs, protocols, input interfaces, quality of service (QoS) labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

Note For Zone-Based Policy Firewall, this command is not applicable to CBWFQ.

The **match access-group** command specifies a numbered or named ACL whose contents are used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

When packets are matched to an access group, a traffic rate is generated for these packets. In a zone-based firewall policy, only the first packet that creates a session matches the policy. Subsequent packets in this flow do not match the filters in the configured policy, but instead match the session directly. The statistics related to subsequent packets are shown as part of the inspect action.

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.

Supported Platforms Other than Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

Note Zone-Based Policy Firewall supports only the **match access-group**, **match protocol**, and **match class-map** commands.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when you configure match criteria. For more information about the **access-list** command, refer to the *Cisco IOS IP Application Services Command Reference*.

Cisco 10000 Series Routers

To use the **match access-group** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Note The **match access-group** command specifies the numbered access list against whose contents packets are checked to determine if they match the criteria specified in the class map. Access lists configured with the optional **log** keyword of the **access-list** command are not supported when you configure match criteria.

Examples

The following example specifies a class map named acl144 and configures the ACL numbered 144 to be used as the match criterion for that class:

```
Router(config)# class-map acl144
Router(config-cmap)# match access-group 144
```

The following example pertains to Zone-Based Policy Firewall. The example defines a class map named c1 and configures the ACL numbered 144 to be used as the match criterion for that class.

```
Router(config)# class-map type inspect match-all c1
Router(config-cmap)# match access-group 144
```

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 criteria specified the ACL numbered 144 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-cmap)# match access-group 144
```

Related Commands

Command	Description
access-list (IP extended)	Defines an extended IP access list.
access-list (IP standard)	Defines a standard IP access list.
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.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match any

To configure the match criteria for a class map to be successful match criteria for all packets, use the **match any** command in class-map configuration or policy inline configuration mode. To remove all criteria as successful match criteria, use the **no** form of this command.

match any

no match any

Syntax Description

This command has no arguments or keywords.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

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.

Examples

In the following configuration, all packets traversing Ethernet interface 1/1 will be policed based on the parameters specified in policy-map class configuration mode:

```
Router(config)# class-map matchany
Router(config-cmap)# match any
Router(config-cmap)# exit

Router(config)# policy-map policy1
Router(config-pmap)# class class4
Router(config-pmap-c)# police 8100 1500 2504 conform-action transmit exceed-action
set-qos-transmit 4
Router(config-pmap-c)# exit

Router(config)# interface ethernet1/1
Router(config-if)# service-policy output policy1
```

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 all packets traversing Ethernet interface 0/0 will be matched and 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 any
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.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match cos

To match a packet on the basis of a Layer 2 class of service (CoS)/Inter-Switch Link (ISL) marking, use the **match cos** command in class-map configuration or policy inline configuration mode. To remove a specific Layer 2 CoS/ISL marking as a match criterion, use the **no** form of this command.

match cos *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]

no match cos *cos-value* [*cos-value* [*cos-value* [*cos-value*]]]

Syntax Description

Supported Platforms Other Than the Cisco 10000 Series Routers	
cos-value	Specific IEEE 802.1Q/ISL CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **match cos** statement.
Cisco 10000 Series Routers	
cos-value	Specific packet CoS bit value. Specifies that the packet CoS bit value must match the specified CoS value. The *cos-value* is from 0 to 7; up to four CoS values, separated by a space, can be specified in one **match cos** statement.

Command Default

Packets are not matched on the basis of a Layer 2 CoS/ISL marking.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.1(5)T	This command was introduced.
12.0(25)S	This command was integrated into Cisco IOS Release 12.0(25)S.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC and support for the Cisco 7600 series routers was added.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and support for the Cisco 7300 series router was added.

Release	Modification
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.

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.

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.

Examples

In the following example, the CoS values of 1, 2, and 3 are successful match criteria for the interface that contains the classification policy named cos:

```
Router(config)# class-map cos
Router(config-cmap)# match cos 1 2 3
```

In the following example, classes named voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the CoS-based-treatment policy map (in this case, the QoS treatment is priority 64 and bandwidth 512). The service policy configured in this example is attached to all packets leaving Fast Ethernet interface 0/0.1. The service policy can be attached to any interface that supports service policies.

```
Router(config)# class-map voice
Router(config-cmap)# match cos 7

Router(config)# class-map video-n-data
Router(config-cmap)# match cos 5

Router(config)# policy-map cos-based-treatment
Router(config-pmap)# class voice
Router(config-pmap-c)# priority 64
Router(config-pmap-c)# exit
Router(config-pmap)# class video-n-data
Router(config-pmap-c)# bandwidth 512
Router(config-pmap-c)# exit
Router(config-pmap)# exit

Router(config)# interface fastethernet0/0.1
Router(config-if)# service-policy output cos-based-treatment
```

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 criteria of a CoS value of 2 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 cos 2
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.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set cos	Sets the Layer 2 CoS value of an outgoing packet.
show class-map	Displays all class maps and their matching criteria.

match destination-address mac

To use the destination MAC address as a match criterion, use the **match destination-address mac** command in class-map configuration or policy inline configuration mode. To remove a previously specified destination MAC address as a match criterion, use the **no** form of this command.

match destination-address mac *address*

no match destination-address mac *address*

Syntax Description

address	Destination MAC address to be used as a match criterion.

Command Default

No destination MAC address is specified.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

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.

Examples

The following example specifies a class map named macaddress and specifies the destination MAC address to be used as the match criterion for this class:

```
Router(config)# class-map macaddress
Router(config-cmap)# match destination-address mac 00:00:00:00:00:00
```

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 specified destination MAC address 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 destination-address mac 00:00:00:00:00:00
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.

match discard-class

To specify a discard class as a match criterion, use the **match discard-class** command in class-map configuration or policy inline configuration mode. To remove a previously specified discard class as a match criterion, use the **no** form of this command.

match discard-class *class-number*

no match discard-class *class-number*

Syntax Description

class-number	Number of the discard class being matched. Valid values are 0 to 7.

Command Default

Packets will not be classified as expected.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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 discard-class value has no mathematical significance. For example, the discard-class value 2 is not greater than 1. The value simply indicates that a packet marked with discard-class 2 should be treated differently than a packet marked with discard-class 1.

Packets that match the specified discard-class value are treated differently from packets marked with other discard-class values. The discard-class is a matching criterion only, used in defining per hop behavior (PHB) for dropping traffic.

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.

Examples

The following example shows that packets in discard class 2 are matched:

```
Router(config)# class-map d-class-2
Router(config-cmap)# match discard-class 2
```

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 criteria specified by discard-class 2 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 discard-class 2
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.
set discard-class	Marks a packet with a discard-class value.

match dscp

To identify one or more differentiated service code point (DSCP), Assured Forwarding (AF), and Certificate Server (CS) values as a match criterion, use the **match dscp** command in class-map configuration or policy inline configuration mode. To remove a specific DSCP value from a class map, use the **no** form of this command.

match [**ip**] **dscp** *dscp-value* [*dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value dscp-value*]

no match [**ip**] **dscp** *dscp-value*

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IPv4 and IPv6 packets. **Note** For the Cisco 10000 series routers, the **ip** keyword is required.
dscp-value	The DSCP value used to identify a DSCP value. For valid values, see the "Usage Guidelines."

Command Default

No match criteria are configured.
If you do not enter the **ip** keyword, matching occurs on both IPv4 and IPv6 packets.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip dscp** command.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for support in IPv6.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and introduced on Cisco ASR 1000 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.

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.

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.

DSCP Values

You must enter one or more differentiated service code point (DSCP) values. The command may include any combination of the following:

- Numbers (0 to 63) representing differentiated services code point values
- AF numbers (for example, af11) identifying specific AF DSCPs
- CS numbers (for example, cs1) identifying specific CS DSCPs
- **default**—Matches packets with the default DSCP.
- **ef**—Matches packets with EF DSCP.

For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7 (note that only one of the IP DSCP values must be a successful match criterion, not all of the specified DSCP values), enter the **match dscp 0 1 2 3 4 5 6 7** command.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, *dscp-value* arguments are used as markings only and have no mathematical significance. For instance, the *dscp-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *dscp-value* of 2 is different than a packet marked with the *dscp-value* of 1. The treatment of these marked packets is defined by the user through the setting of Quality of Service (QoS) policies in policy-map class configuration mode.

Match Packets on DSCP Values

To match DSCP values for IPv6 packets only, the **match protocol ipv6** command must also be used. Without that command, the DSCP match defaults to match both IPv4 and IPv6 packets.

To match DSCP values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets. Alternatively, the **match protocol ip** command may be used with **match dscp** to classify only IPv4 packets.

After the DSCP bit is set, other QoS features can then operate on the bit settings.

The network can give priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain); data is then queued according to the precedence. Weighted fair queueing (WFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Random Early Detection (WRED) can ensure that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Cisco 10000 Series Routers

The Cisco 10000 series routers support DSCP matching of IPv4 packets only. You must include the **ip** keyword when specifying the DSCP values to use as match criterion.

You cannot use the **set ip dscp** command with the **set ip precedence** command to mark the same packet. DSCP and precedence values are mutually exclusive. A packet can have one value or the other, but not both.

Examples

The following example shows how to set multiple match criteria. In this case, two IP DSCP value and one AF value.

```
Router(config)# class-map map1
Router(config-cmap)# match dscp 1 2 af11
```

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 criteria specified by DSCP value 2 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 dscp 2
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.
match protocol ip	Matches DSCP values for packets.
match protocol ipv6	Matches DSCP values for IPv6 packets.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set dscp	Marks the DSCP value for packets within a traffic class.
show class-map	Displays all class maps and their matching criteria.

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**}

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.

Command Default

The use of the flow direction and the flow sampler ID number as key fields for a user-defined flow record is not enabled by default.

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.

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
```

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 for Flexible NetFlow.

match fr-de

To match packets on the basis of the Frame Relay discard eligibility (DE) bit setting, use the **match fr-de** command in class-map configuration or policy inline configuration mode. To remove the match criteria, use the **no** form of this command.

match fr-de

no match fr-de

Syntax Description

This command has no arguments or keywords.

Command Default

Packets are not matched on the basis of the Frame Relay DE bit setting.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(25)S	This command was introduced for the Cisco 7500 series router.
12.0(26)S	This command was integrated into Cisco IOS Release 12.0(26)S and implemented on the Cisco 7200 series router.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
12.2(33)SRC	This command was integrated into Cisco IOS Release 12.2(33)SRC.
12.4(15)T2	This command was integrated into Cisco IOS Release 12.4(15)T2.
12.2(33)SB	This command was integrated into Cisco IOS Release 12.2(33)SB and implemented on the Cisco 7300 series router.
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.

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.

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.

Examples

The following example creates a class named match-fr-de and matches packets on the basis of the Frame Relay DE bit setting.

```
Router(config)# class-map match-fr-de
```

```
Router(config-cmap)# match fr-de
```

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 Frame Relay DE bit setting 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 fr-de
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.
set fr-de	Changes the DE bit setting in the address field of a Frame Relay frame to 1 for all traffic leaving an interface.

match fr-dlci

To specify the Frame Relay data-link connection identifier (DLCI) number as a match criterion in a class map, use the **match fr-dlci** command in class-map configuration or policy inline configuration mode. To remove a previously specified DLCI number as a match criterion, use the **no** form of this command.

match fr-dlci *dlci-number*

no match fr-dlci *dlci-number*

Syntax Description

dlci-number	Number of the DLCI associated with the packet.

Command Default

No DLCI number is specified.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(28)SB	This command was integrated into Cisco IOS Release 12.2(28)SB.
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.

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.

This match criterion can be used in main interfaces and point-to-multipoint subinterfaces in Frame Relay networks, and it can also be used in hierarchical policy maps.

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.

Examples

In the following example a class map named “class1” has been created and the Frame Relay DLCI number of 500 has been specified as a match criterion. Packets matching this criterion are placed in class1.

```
Router(config)# class-map class1
Router(config-cmap)# match fr-dlci 500
```

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 Frame Relay DLCI number of 500 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 fr-dlci 500
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.
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match input-interface

To configure a class map to use the specified input interface as a match criterion, use the **match input-interface** command in class-map configuration or policy inline configuration mode. To remove the input interface match criterion from a class map, use the **no** form of this command.

match input-interface *interface-name*

no match input-interface *interface-name*

Syntax Description

interface-name	Name of the input interface to be used as match criteria.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.0(17)SL	This command was enhanced to include matching on the input interface.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

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.

Supported Platforms Other Than Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria including input interfaces, access control lists (ACLs), protocols, quality of service (QoS) labels, and experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match input-interface** command specifies the name of an input interface to be used as the match criterion against which packets are checked to determine if they belong to the class specified by the class map.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**
- **match protocol**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including input interfaces, ACLs, protocols, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

To use the **match input-interface** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

Examples

The following example specifies a class map named ethernet1 and configures the input interface named ethernet1 to be used as the match criterion for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match input-interface ethernet1
```

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 criteria of the input interface named ethernet1 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 input-interface ethernet 1
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.

Command	Description
match access-group	Configures the match criteria for a class map based on the specified ACL.
match mpls experimental	Configures a class map to use the specified EXP field value as a match criterion.
match protocol	Configures the match criteria for a class map on the basis of the specified protocol.

match ip dscp

The **match ip dscp** command is replaced by the **match dscp** command. See the **match dscp** command for more information.

match ip precedence

The **match ip precedence** command is replaced by the **match precedence** command. See the **match precedence** command for more information.

match ip rtp

To configure a class map to use the Real-Time Protocol (RTP) port as the match criterion, use the **match ip rtp** command in class-map configuration or policy inline configuration mode. To remove the RTP port match criterion, use the **no** form of this command.

match ip rtp *starting-port-number port-range*

no match ip rtp

Syntax Description

starting-port-number	The starting RTP port number. Values range from 2000 to 65535.
port-range	The RTP port number range. Values range from 0 to 16383.

Command Default

No match criteria are specified.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.1(2)T	This command was introduced.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

This command is used to match IP RTP packets that fall within the specified port range. It matches packets destined to all even User Datagram Port (UDP) port numbers in the range from the *starting port number* argument to the *starting port number* plus the *port range* argument.

Use of an RTP port range as the match criterion is particularly effective for applications that use RTP, such as voice or video.

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.

Examples

The following example specifies a class map named ethernet1 and configures the RTP port number 2024 and range 1000 to be used as the match criteria for this class:

```
Router(config)# class-map ethernet1
Router(config-cmap)# match ip rtp 2024 1000
```

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 criteria of RTP port number 2024 and range 1000 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 ip rtp 2024 1000
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.
ip rtp priority	Reserves a strict priority queue for a set of RTP packet flows belonging to a range of UDP destination ports.
match access-group	Configures the match criteria for a class map based on the specified ACL number.

match ipv4

To configure one or more of the IPv4 fields as a key field for a flow record, use the **match ipv4** command in flow record configuration mode. To disable the use of one or more of the IPv4 fields as a key field for a 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**}

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

match ipv4 protocol

no match ipv4 protocol

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 flow record is not enabled by default.

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.

Release	Modification
15.1(3)T	This command was integrated into Cisco IOS Release 15.1(3)T for Cisco Performance Monitor with only the **protocol** keyword.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor with only the **protocol** keyword.

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.

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 flow record, refer to the **match ipv4 ttl** command.

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

Only the **protocol** keyword is available. You must first enter the **flow record type performance-monitor** 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
```

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

The following example configures the IPv4 DSCP field as a key field for Cisco Performance Monitor:

```
Router(config)# flow record type performance-monitor FLOW-RECORD-1
Router(config-flow-record)# match ipv4 dscp
```

Related Commands

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

match ipv4 destination

To configure the IPv4 destination address as a key field for a flow record, use the **match ipv4 destination** command in flow record configuration mode. To disable the IPv4 destination address as a key field for a 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*]}

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

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

no match ipv4 destination {**address** | **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. The range is 1 to 32.

Command Default

The IPv4 destination address is not configured as a key 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.
12.0(33)S	This command was integrated into Cisco IOS Release 12.0(33)S and implemented on the Gigabit Switch Router (GSR).
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 without the **mask** keyword.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor without the **mask** keyword.

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

The **mask** keyword is not available. You must first enter the **flow record type performance-monitor** 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
```

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

The following example specifies a 16-bit IPv4 destination address mask as a key field for Cisco Performance Monitor:

```
Router(config)# flow record type performance-monitor FLOW-RECORD-1
Router(config-flow-record)# match ipv4 destination mask minimum-mask 16
```

Related Commands

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

match ipv4 source

To configure the IPv4 source address as a key field for a flow record, use the **match ipv4 source** command in flow record configuration mode. To disable the use of the IPv4 source address as a key field for a 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*]}

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

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

no match ipv4 source {**address** | **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 128.

Command Default

The IPv4 source address is not configured as a key 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 without the **mask** keyword.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE for Cisco Performance Monitor without the **mask** keyword.

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

The **mask** keyword is not available. You must first enter the **flow record type performance-monitor** 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
```

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

The following example specifies a 16-bit IPv4 source address mask as a key field for Cisco Performance Monitor:

```
Router(config)# flow record type performance-monitor FLOW-RECORD-1
Router(config-flow-record)# match ipv4 source mask minimum-mask 16
```

Related Commands

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

match mpls experimental topmost

To match the experimental (EXP) value in the topmost label header, use the **match mpls experimental topmost** command in class-map configuration or policy inline configuration mode. To remove the EXP match criterion, use the **no** form of this command.

match mpls experimental topmost *number*

no match mpls experimental topmost *number*

Syntax Description

number	Multiprotocol Label Switching (MPLS) EXP field in the topmost label header. Valid values are 0 to 7.

Command Default

No EXP match criterion is configured for the topmost label header.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
Cisco IOS XE Release 2.3	This command was integrated into Cisco IOS XE Release 2.3.
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.

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.

You can enter this command on the input interfaces and the output interfaces. It will match only on MPLS packets.

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.

Examples

The following example shows that the EXP value 3 in the topmost label header is matched:

```
Router(config)# class-map mpls exp
Router(config-cmap)# match mpls experimental topmost 3
```

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 criteria of a EXP value of 3 in the topmost label header 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 mpls experimental topmost 3
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.
set mpls experimental topmost	Sets the MPLS EXP field value in the topmost MPLS label header at the input or output interfaces.

match not

To specify the single match criterion value to use as an unsuccessful match criterion, use the **match not** command in class-map configuration or policy inline configuration mode. To remove a previously specified source value to not use as a match criterion, use the **no** form of this command.

match not *match-criterion*

no match not *match-criterion*

Syntax Description

match-criterion	The match criterion value that is an unsuccessful match criterion. All other values of the specified match criterion will be considered successful match criteria.

Command Default

No unsuccessful match criterion is configured.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.0(5)T	This command was integrated into Cisco IOS Release 12.0(5)T.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

The **match not** command is used to specify a quality of service (QoS) policy value that is not used as a match criterion. When the **match not** command is used, all other values of that QoS policy become successful match criteria.

For instance, if the **match not qos-group 4** command is issued in QoS class-map configuration mode, the specified class will accept all QoS group values except 4 as successful match criteria.

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.

Examples

In the following traffic class, all protocols except IP are considered successful match criteria:

```
Router(config)# class-map noip
Router(config-cmap)# match not protocol ip
```

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 for all protocols except IP 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 not protocol ip
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.

match packet length (class-map)

To specify the Layer 3 packet length in the IP header as a match criterion in a class map, use the **match packet length** command in class-map configuration or policy inline configuration mode. To remove a previously specified Layer 3 packet length as a match criterion, use the **no** form of this command.

match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*] | **min** *minimum-length-value* [**max** *maximum-length-value*]}

no match packet length {**max** *maximum-length-value* [**min** *minimum-length-value*] | **min** *minimum-length-value* [**max** *maximum-length-value*]}

Syntax Description

max	Indicates that a maximum value for the Layer 3 packet length is to be specified.
maximum-length-value	Maximum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.
min	Indicates that a minimum value for the Layer 3 packet length is to be specified.
minimum-length-value	Minimum length value of the Layer 3 packet length, in bytes. The range is from 1 to 2000.

Command Default

The Layer 3 packet length in the IP header is not used as a match criterion.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 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.

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.

This command considers only the Layer 3 packet length in the IP header. It does not consider the Layer 2 packet length in the IP header.

When using this command, you must at least specify the maximum or minimum value. However, you do have the option of entering both values.

If only the minimum value is specified, a packet with a Layer 3 length greater than the minimum is viewed as matching the criterion.

If only the maximum value is specified, a packet with a Layer 3 length less than the maximum is viewed as matching the criterion.

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.

Examples

In the following example a class map named "class 1" has been created, and the Layer 3 packet length has been specified as a match criterion. In this example, packets with a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes are viewed as meeting the match criteria.

```
Router(config)# class-map match-all class1
Router(config-cmap)# match packet length min 100 max 300
```

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 criteria of a minimum Layer 3 packet length of 100 bytes and a maximum Layer 3 packet length of 300 bytes 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 packet length min 100 max 300
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.
show class-map	Displays all class maps and their matching criteria.
show policy-map interface	Displays the packet statistics of all classes that are configured for all service policies either on the specified interface or subinterface or on a specific PVC on the interface.

match precedence

To identify IP precedence values to use as the match criterion, use the **match precedence** command in class-map configuration or policy inline configuration mode. To remove IP precedence values from a class map, use the **no** form of this command.

match [**ip**] **precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

no match [**ip**] **precedence** {*precedence-criteria1* | *precedence-criteria2* | *precedence-criteria3* | *precedence-criteria4*}

Syntax Description

ip	(Optional) Specifies that the match is for IPv4 packets only. If not used, the match is on both IP and IPv6 packets. **Note** For the Cisco 10000 series routers, the **ip** keyword is required.
precedence-criteria1 *precedence-criteria2* *precedence-criteria3* *precedence-criteria4*	Identifies the precedence value. You can enter up to four different values, separated by a space. See the "Usage Guidelines" for valid values.

Command Default

No match criterion is configured.
If you do not enter the **ip** keyword, matching occurs on both IPv4 and IPv6 packets.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(13)T	This command was introduced. This command replaces the **match ip precedence** command.
12.0(17)SL	This command was integrated into Cisco IOS Release 12.0(17)SL and implemented on the Cisco 10000 series routers.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB.
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.

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.

You can enter up to four matching criteria, as number abbreviation (0 to 7) or criteria names (critical, flash, and so on), in a single match statement. For example, if you wanted the precedence values of 0, 1, 2, or 3 (note that only one of the precedence values must be a successful match criterion, not all of the specified precedence values), enter the **match ip precedence 0 1 2 3** command. The *precedence-criteria* numbers are not mathematically significant; that is, the *precedence-criteria* of 2 is not greater than 1. The way that these different packets are treated depends upon quality of service (QoS) policies, set in the policy-map configuration mode.

You can configure a QoS policy to include IP precedence marking for packets entering the network. Devices within your network can then use the newly marked IP precedence values to determine how to treat the packets. For example, class-based weighted random early detection (WRED) uses IP precedence values to determine the probability that a packet is dropped. You can also mark voice packets with a particular precedence. You can then configure low-latency queueing (LLQ) to place all packets of that precedence into the priority queue.

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.

Matching Precedence for IPv6 and IPv4 Packets on the Cisco 10000 and 7600 Series Routers

On the Cisco 7600 series and 10000 series routers, you set matching criteria based on precedence values for only IPv6 packets using the **match protocol** command with the **ipv6** keyword. Without that keyword, the precedence match defaults to match both IPv4 and IPv6 packets. You set matching criteria based on precedence values for IPv4 packets only, use the **ip** keyword. Without the **ip** keyword the match occurs on both IPv4 and IPv6 packets.

Precedence Values and Names

The following table lists all criteria conditions by value, name, binary value, and recommended use. You may enter up to four criteria, each separated by a space. Only one of the precedence values must be a successful match criterion. Table 9 lists the IP precedence values.

Table 9 IP Precedence Values

Precedence Value	Precedence Name	Binary Value	Recommended Use
0	routine	000	Default marking value
1	priority	001	Data applications
2	immediate	010	Data applications
3	flash	011	Call signaling
4	flash-override	100	Video conferencing and streaming video
5	critical	101	Voice
6	internet (control)	110	Network control traffic (such as routing, which is typically precedence 6)
7	network (control)	111	

Do not use IP precedence 6 or 7 to mark packets, unless you are marking control packets.

Examples

IPv4-Specific Traffic Match

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface, matching for IPv4 traffic only. In a network where both IPv4 and IPv6 are running, you might find it necessary to distinguish between the protocols for matching and traffic segregation. In this example, the class map named ipprec5 will evaluate all IPv4 packets entering Fast Ethernet interface 1/0/0 for a precedence value of 5. If the incoming IPv4 packet has been marked with the precedence value of 5, the packet will be treated as priority traffic and will be allocated with bandwidth of 50 kbps.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match ip precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

IPv6-Specific Traffic Match

The following example shows the same service policy matching on precedence for IPv6 traffic only. Notice that the **match protocol** command with the **ipv6** keyword precedes the **match precedence** command. The **match protocol** command is required to perform matches on IPv6 traffic alone.

```
Router(config)# class-map ipprec5
Router(config-cmap)# match protocol ipv6
Router(config-cmap)# match precedence 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class ipprec5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fa1/0/0
Router(config-if)# service-policy input priority50
```

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 criteria of a match precedence of 4 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 precedence 4
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.
match protocol	Configures the match criteria for a class map on the basis of a specified protocol.

Command	Description
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set ip precedence	Sets the precedence value in the IP header.
show class-map	Displays all class maps and their matching criteria, or a specified class map and its matching criteria.

match protocol

To configure the match criterion for a class map on the basis of a specified protocol, use the **match protocol** command in class-map configuration or policy inline configuration mode. To remove the protocol-based match criterion from the class map, use the **no** form of this command.

match protocol *protocol-name*

no match protocol *protocol-name*

Syntax Description

protocol-name	Name of the protocol (for example, bgp) used as a matching criterion. See the "Usage Guidelines" for a list of protocols supported by most routers.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)T	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.0(7)S	This command was integrated into Cisco IOS Release 12.0(7)S.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(13)E	This command was integrated into Cisco IOS Release 12.1(13)E and implemented on Catalyst 6000 family switches without FlexWAN modules.
12.2(8)T	This command was integrated into Cisco IOS Release 12.2(8)T.
12.2(13)T	This command was modified to remove **apollo**, **vines**, and **xns** from the list of protocols used as matching criteria. These protocols were removed because Apollo Domain, Banyan VINES, and Xerox Network Systems (XNS) were removed in this release. The IPv6 protocol was added to support matching on IPv6 packets.
12.0(28)S	This command was integrated into Cisco IOS Release 12.0(28)S for IPv6.
12.2(14)S	This command was integrated into Cisco IOS Release 12.2(14)S.
12.2(17a)SX1	This command was integrated into Cisco IOS Release 12.2(17a)SX1.
12.2(18)SXE	This command was integrated into Cisco IOS Release 12.2(18)SXE and implemented on the Supervisor Engine 720.
12.4(6)T	This command was modified. The Napster protocol was removed because it is no longer supported.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB2	This command was integrated into Cisco IOS Release 12.2(31)SB2 and implemented on the Cisco 10000 series routers.

Release	Modification
12.2(18)ZY	This command was integrated into Cisco IOS Release 12.2(18)ZY. This command was modified to enhance Network-Based Application Recognition (NBAR) functionality on the Catalyst 6500 series switch that is equipped with the Supervisor 32/programmable intelligent services accelerator (PISA) engine.
12.4(15)XZ	This command was integrated into Cisco IOS Release 12.4(15)XZ.
12.4(20)T	This command was integrated into Cisco IOS Release 12.4(20)T and implemented on the Cisco 1700, Cisco 1800, Cisco 2600, Cisco 2800, Cisco 3700, Cisco 3800, Cisco 7200, and Cisco 7300 series routers.
Cisco IOS XE Release 2.2	This command was integrated into Cisco IOS XE Release 2.2 and implemented on the Cisco ASR 1000 Series Routers.
Cisco IOS XE Release 3.1S	This command was modified. Support for more protocols was added.
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.

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.

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.

Supported Platforms Other Than Cisco 7600 Routers and Cisco 10000 Series Routers

For class-based weighted fair queueing (CBWFQ), you define traffic classes based on match criteria protocols, access control lists (ACLs), input interfaces, quality of service (QoS) labels, and Experimental (EXP) field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **match protocol ipx** command matches packets in the output direction only.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish. After you identify the class, you can use one of the following commands to configure its match criteria:

- **match access-group**
- **match input-interface**
- **match mpls experimental**

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

To configure NBAR to match protocol types that are supported by NBAR traffic, use the **match protocol** (NBAR) command.

Cisco 7600 Series Routers

The **match protocol** command in QoS class-map configuration configures NBAR and sends all traffic on the port, both ingress and egress, to be processed in the software on the Multilayer Switch Feature Card 2 (MSFC2).

For CBWFQ, you define traffic classes based on match criteria like protocols, ACLs, input interfaces, QoS labels, and Multiprotocol Label Switching (MPLS) EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

If you want to use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class to which you want to establish the match criteria.

If you specify more than one command in a class map, only the last command entered applies. The last command overrides the previously entered commands.

This command can be used to match protocols that are known to the NBAR feature. For a list of protocols supported by NBAR, see the "Classification" part of the *Cisco IOS Quality of Service Solutions Configuration Guide*.

Cisco 10000 Series Routers

For CBWFQ, you define traffic classes based on match criteria including protocols, ACLs, input interfaces, QoS labels, and EXP field values. Packets satisfying the match criteria for a class constitute the traffic for that class.

The **match protocol** command specifies the name of a protocol to be used as the match criteria against which packets are checked to determine if they belong to the class specified by the class map.

The **match protocol ipx** command matches packets in the output direction only.

To use the **match protocol** command, you must first enter the **class-map** command to specify the name of the class whose match criteria you want to establish.

If you are matching NBAR protocols, use the **match protocol** (NBAR) command.

Match Protocol Command Restrictions (Catalyst 6500 Series Switches Only)

Policy maps contain traffic classes. Traffic classes contain one or more **match** commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application. You can create as many traffic classes as needed.

Cisco IOS Release 12.2(18)ZY includes software intended for use on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine. For this release and platform, note the following restrictions for using policy maps and **match protocol** commands:

- A single traffic class can be configured to match a maximum of 8 protocols or applications.
- Multiple traffic classes can be configured to match a cumulative maximum of 95 protocols or applications.

Supported Protocols

Table 10 lists the protocols supported by most routers. Some routers support a few additional protocols. For example, the Cisco 7600 router supports the AARP and DECnet protocols, while the Cisco 7200 router supports the directconnect and PPPOE protocols. For a complete list of supported protocols, see the online help for the **match protocol** command on the router that you are using.

Table 10 Supported Protocols

Protocol Name	Description
802-11-iapp	IEEE 802.11 Wireless Local Area Networks Working Group Internet Access Point Protocol
ace-svr	ACE Server/Propagation
aol	America-Online Instant Messenger
appleqtc	Apple QuickTime
arp*	IP Address Resolution Protocol (ARP)
bgp	Border Gateway Protocol
biff	Biff mail notification
bootpc	Bootstrap Protocol Client
bootps	Bootstrap Protocol Server
bridge*	bridging
cddbp	CD Database Protocol
cdp*	Cisco Discovery Protocol
cifs	CIFS
cisco-fna	Cisco FNATIVE
cisco-net-mgmt	cisco-net-mgmt
cisco-svcs	Cisco license/perf/GDP/X.25/ident svcs
cisco-sys	Cisco SYSMAINT
cisco-tdp	cisco-tdp
cisco-tna	Cisco TNATIVE
citrix	Citrix Systems Metaframe
citriximaclient	Citrix IMA Client
clns*	ISO Connectionless Network Service
clns_es*	ISO CLNS End System
clns_is*	ISO CLNS Intermediate System
clp	Cisco Line Protocol
cmns*	ISO Connection-Mode Network Service
cmp	Cluster Membership Protocol
compressedtcp*	Compressed TCP
creativepartnr	Creative Partner
creativeserver	Creative Server
cuseeme	CU-SeeMe desktop video conference
daytime	Daytime (RFC 867)
dbase	dBASE Unix
dbcontrol_agent	Oracle Database Control Agent
ddns-v3	Dynamic DNS Version 3

Table 10 Supported Protocols (continued)

Protocol Name	Description
dhcp	Dynamic Host Configuration
dhcp-failover	DHCP Failover
directconnect	Direct Connect
discard	Discard port
dns	Domain Name Server lookup
dnsix	DNSIX Security Attribute Token Map
echo	Echo port
edonkey	eDonkey
egp	Exterior Gateway Protocol
eigrp	Enhanced Interior Gateway Routing Protocol
entrust-svc-handler	Entrust KM/Admin Service Handler
entrust-svcs	Entrust sps/aaas/aams
exec	Remote Process Execution
exchange	Microsoft RPC for Exchange
fasttrack	FastTrack Traffic (KaZaA, Morpheus, Grokster, and so on)
fcip-port	FCIP
finger	Finger
ftp	File Transfer Protocol
ftps	FTP over TLS/SSL
gdoi	Group Domain of Interpretation
giop	Oracle GIOP/SSL
gnutella	Gnutella Version 2 Traffic (BearShare, Shareeza, Morpheus, and so on)
gopher	Gopher
gre	Generic Routing Encapsulation
gtpv0	GPRS Tunneling Protocol Version 0
gtpv1	GPRS Tunneling Protocol Version 1
h225ras	H225 RAS over Unicast
h323	H323 Protocol
h323callsigalt	H323 Call Signal Alternate
hp-alarm-mgr	HP Performance data alarm manager
hp-collector	HP Performance data collector
hp-managed-node	HP Performance data managed node
hsrp	Hot Standby Router Protocol
http	Hypertext Transfer Protocol
https	Secure Hypertext Transfer Protocol
ica	ica (Citrix)

Table 10 Supported Protocols (continued)

Protocol Name	Description
icabrowser	icabrowser (Citrix)
icmp	Internet Control Message Protocol
ident	Authentication Service
igmpv3lite	IGMP over UDP for SSM
imap	Internet Message Access Protocol
imap3	Interactive Mail Access Protocol 3
imaps	IMAP over TLS/SSL
ip*	IP (version 4)
ipass	IPASS
ipinip	IP in IP (encapsulation)
ipsec	IP Security Protocol (ESP/AH)
ipsec-msft	Microsoft IPsec NAT-T
ipv6*	IP (version 6)
ipx	IPX
irc	Internet Relay Chat
irc-serv	IRC-SERV
ircs	IRC over TLS/SSL
ircu	IRCU
isakmp	ISAKMP
iscsi	iSCSI
iscsi-target	iSCSI port
kazaa2	Kazaa Version 2
kerberos	Kerberos
l2tp	Layer 2 Tunnel Protocol
ldap	Lightweight Directory Access Protocol
ldap-admin	LDAP admin server port
ldaps	LDAP over TLS/SSL
llc2*	llc2
login	Remote login
lotusmtap	Lotus Mail Tracking Agent Protocol
lotusnote	Lotus Notes
mgcp	Media Gateway Control Protocol
microsoft-ds	Microsoft-DS
msexch-routing	Microsoft Exchange Routing
msnmsgr	MSN Instant Messenger
msrpc	Microsoft Remote Procedure Call

Table 10 Supported Protocols (continued)

Protocol Name	Description
ms-cluster-net	MS Cluster Net
ms-dotnetster	Microsoft .NETster Port
ms-sna	Microsoft SNA Server/Base
ms-sql	Microsoft SQL
ms-sql-m	Microsoft SQL Monitor
mysql	MySQL
n2h2server	N2H2 Filter Service Port
ncp	NCP (Novell)
net8-cman	Oracle Net8 Cman/Admin
netbios	Network Basic Input/Output System
netbios-dgm	NETBIOS Datagram Service
netbios-ns	NETBIOS Name Service
netbios-ssn	NETBIOS Session Service
netshow	Microsoft Netshow
netstat	Variant of systat
nfs	Network File System
nntp	Network News Transfer Protocol
novadigm	Novadigm Enterprise Desktop Manager (EDM)
ntp	Network Time Protocol
oem-agent	OEM Agent (Oracle)
oracle	Oracle
oracle-em-vp	Oracle EM/VP
oraclenames	Oracle Names
orasrv	Oracle SQL*Net v1/v2
ospf	Open Shortest Path First
pad*	Packet assembler/disassembler (PAD) links
pcanywhere	Symantec pcANYWHERE
pcanywheredata	pcANYWHEREdata
pcanywherestat	pcANYWHEREstat
pop3	Post Office Protocol
pop3s	POP3 over TLS/SSL
pppoe	Point-to-Point Protocol over Ethernet
pptp	Point-to-Point Tunneling Protocol
printer	Print spooler/ldp
pwdgen	Password Generator Protocol
qmtp	Quick Mail Transfer Protocol

Table 10 Supported Protocols (continued)

Protocol Name	Description
radius	RADIUS & Accounting
rcmd	Berkeley Software Distribution (BSD) r-commands (rsh, rlogin, rexec)
rdb-dbs-disp	Oracle RDB
realmedia	RealNetwork's Realmedia Protocol
realsecure	ISS Real Secure Console Service Port
rip	Routing Information Protocol
router	Local Routing Process
rsrb*	Remote Source-Route Bridging
rsvd	RSVD
rsvp	Resource Reservation Protocol
rsvp-encap	RSVP ENCAPSULATION-1/2
rsvp_tunnel	RSVP Tunnel
rtc-pm-port	Oracle RTC-PM port
rtelnet	Remote Telnet Service
rtp	Real-Time Protocol
rtsp	Real-Time Streaming Protocol
r-winsock	remote-winsock
secure-ftp	FTP over Transport Layer Security/Secure Sockets Layer (TLS/SSL)
secure-http	Secured HTTP
secure-imap	Internet Message Access Protocol over TLS/SSL
secure-irc	Internet Relay Chat over TLS/SSL
secure-ldap	Lightweight Directory Access Protocol over TLS/SSL
secure-nntp	Network News Transfer Protocol over TLS/SSL
secure-pop3	Post Office Protocol over TLS/SSL
secure-telnet	Telnet over TLS/SSL
send	SEND
shell	Remote command
sip	Session Initiation Protocol
sip-tls	Session Initiation Protocol-Transport Layer Security
skinny	Skinny Client Control Protocol
sms	SMS RCINFO/XFER/CHAT
smtp	Simple Mail Transfer Protocol
snapshot	Snapshot routing support
snmp	Simple Network Protocol
snmptrap	SNMP Trap
socks	Sockets network proxy protocol (SOCKS)

Table 10 Supported Protocols (continued)

Protocol Name	Description
sqlnet	Structured Query Language (SQL)*NET for Oracle
sqlserv	SQL Services
sqlsrv	SQL Service
sqlserver	Microsoft SQL Server
ssh	Secure shell
sshell	SSLshell
ssp	State Sync Protocol
streamwork	Xing Technology StreamWorks player
stun	cisco Serial Tunnel
sunrpc	Sun remote-procedure call (RPC)
syslog	System Logging Utility
syslog-conn	Reliable Syslog Service
tacacs	Login Host Protocol (TACACS)
tacacs-ds	TACACS-Database Service
tarantella	Tarantella
tcp	Transport Control Protocol
telnet	Telnet
telnets	Telnet over TLS/SSL
tftp	Trivial File Transfer Protocol
time	Time
timed	Time server
tr-rsrb	cisco RSRB
tto	Oracle TTC/SSL
udp	User Datagram Protocol
uucp	UUCPD/UUCP-RLOGIN
vdolive	VDOLive streaming video
vofr*	Voice over Frame Relay
vqp	VLAN Query Protocol
webster	Network Dictionary
who	Who’s service
wins	Microsoft WINS
x11	X Window System
xdmcp	XDM Control Protocol
xwindows*	X-Windows remote access
ymsgr	Yahoo! Instant Messenger

* This protocol is not supported on the Catalyst 6500 series switch that is equipped with a Supervisor 32/PISA engine.

Examples

The following example specifies a class map named ftp and configures the FTP protocol as a match criterion:

```
Router(config)# class-map ftp
Router(config-cmap)# match protocol ftp
```

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 for the IP protocol 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 protocol ip
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.
match access-group	Configures the match criteria for a class map based on the specified ACL.
match input-interface	Configures a class map to use the specified input interface as a match criterion.
match mpls experimental	Configures a class map to use the specified value of the experimental field as a match criterion.
match precedence	Identifies IP precedence values as match criteria.
match protocol (NBAR)	Configures NBAR to match traffic by a protocol type known to NBAR.
match qos-group	Configures a class map to use the specified EXP field value as a match criterion.

match qos-group

To identify a specific quality of service (QoS) group value as a match criterion, use the **match qos-group** command in class-map configuration or policy inline configuration mode. To remove a specific QoS group value from a class map, use the **no** form of this command.

match qos-group *qos-group-value*

no match qos-group *qos-group-value*

Syntax Description

qos-group-value	The exact value from 0 to 99 used to identify a QoS group value.

Command Default

No match criterion is specified.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
11.1CC	This command was introduced.
12.0(5)XE	This command was integrated into Cisco IOS Release 12.0(5)XE.
12.2(13)T	This command was integrated into Cisco IOS Release 12.2(13)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series routers.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
Cisco IOS XE Release 2.1	This command was integrated into Cisco IOS XE Release 2.1 and implemented on Cisco ASR 1000 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.

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.

The **match qos-group** command is used by the class map to identify a specific QoS group value marking on a packet. This command can also be used to convey the received Multiprotocol Label Switching (MPLS) experimental (EXP) field value to the output interface.

The *qos-group-value* argument is used as a marking only. The QoS group values have no mathematical significance. For instance, the *qos-group-value* of 2 is not greater than 1. The value simply indicates that a packet marked with the *qos-group-value* of 2 is different than a packet marked with the *qos-group-value* of 1. The treatment of these packets is defined by the user through the setting of QoS policies in QoS policy-map class configuration mode.

The QoS group value is local to the router, meaning that the QoS group value that is marked on a packet does not leave the router when the packet leaves the router. If you need a marking that resides in the packet, use IP precedence setting, IP differentiated services code point (DSCP) setting, or another method of packet marking.

This command can be used with the **random-detect discard-class-based** 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.

Examples

The following example shows how to configure the service policy named priority50 and attach service policy priority50 to an interface. In this example, the class map named qosgroup5 will evaluate all packets entering Fast Ethernet interface 1/0/0 for a QoS group value of 5. If the incoming packet has been marked with the QoS group value of 5, the packet will be treated with a priority level of 50.

```
Router(config)# class-map qosgroup5
Router(config-cmap)# match qos-group 5
Router(config)# exit
Router(config)# policy-map priority50
Router(config-pmap)# class qosgroup5
Router(config-pmap-c)# priority 50
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# interface fastethernet1/0/0
Router(config-if)# service-policy output priority50
```

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 criteria of a QoS value of 4 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 qosgroup 4
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.
policy-map	Creates or modifies a policy map that can be attached to one or more interfaces to specify a service policy.
random-detect discard-class-based	Bases WRED on the discard class value of a packet.

Command	Description
service-policy	Attaches a policy map to an input interface or VC, or an output interface or VC, to be used as the service policy for that interface or VC.
set precedence	Specifies an IP precedence value for packets within a traffic class.
set qos-group	Sets a group ID that can be used later to classify packets.

match source-address mac

To use the source MAC address as a match criterion, use the **match source-address mac** command in class-map configuration or policy inline configuration mode. To remove a previously specified source MAC address as a match criterion, use the **no** form of this command.

match source-address mac *address-source*

no match source-address mac *address-source*

Syntax Description

address-source	The source source MAC address to be used as a match criterion.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.0(5)XE	This command was introduced.
12.1(1)E	This command was integrated into Cisco IOS Release 12.1(1)E.
12.1(5)T	This command was integrated into Cisco IOS Release 12.1(5)T.
12.2(33)SRA	This command was integrated into Cisco IOS Release 12.2(33)SRA.
12.2(31)SB	This command was integrated into Cisco IOS Release 12.2(31)SB and implemented on the Cisco 10000 series.
12.2SX	This command is supported in the Cisco IOS Release 12.2SX train. Support in a specific 12.2SX release of this train depends on your feature set, platform, and platform hardware.
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.

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.

This command can be used only on an input interface with a MAC address; for example, Fast Ethernet and Ethernet interfaces.

This command cannot be used on output interfaces with no MAC address, such as serial and ATM interfaces.

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.

Examples

The following example uses the MAC address mac 0.0.0 as a match criterion:

```
Router(config)# class-map matchsrcmac
Router(config-cmap)# match source-address mac 0.0.0
```

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 specified MAC source address 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 source-address mac 0.0.0
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.

match transport destination-port

To configure the destination port as a key field for a flow record, use the **match transport destination-port** command in flow record configuration mode. To disable the use of the destination port as a key field for a flow record, use the **no** form of this command.

match transport destination-port

no match transport destination-port

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the destination port as a key field for a user-defined flow record is not enabled by default.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

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 type performance-monitor PM-RECORD-4
Router(config-flow-record)# match transport destination-port
```

Related CommandsC

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

match transport rtp ssrc

To configure the SSRC field in RTP packet header as a key field for a flow record, use the **match transport rtp ssrc** command in flow record configuration mode. To disable the use of the SSRC field as a key field for a flow record, use the **no** form of this command.

match transport rtp ssrc

no match transport rtp ssrc

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the SSRC field in RTP packet header as a key field for a user-defined flow record is not enabled by default.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

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.

The SSRC field in RTP packet header is used to identify a different stream source which is using the same protocol and source and destination IP address and port.

Examples

The following example configures the SSRC field in RTP packet header as a key field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# match transport rtp ssrc
```

Related Commands

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

match transport source-port

To configure the source port as a key field for a flow record, use the **match transport source-port** command in flow record configuration mode. To disable the use of the source port as a key field for a flow record, use the **no** form of this command.

match transport source-port

no match transport source-port

Syntax Description

This command has no arguments or keywords.

Command Default

The use of the source port as a key field for a user-defined flow record is not enabled by default.

Command Modes

flow record configuration (config-flow-record)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

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 source port as a key field:

```
Router(config)# flow record type performance-monitor PM-RECORD-4
Router(config-flow-record)# match transport source-port
```

Related Commands

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

match vlan

To define the VLAN match criteria, use the **match vlan** command in class-map configuration or policy inline configuration mode. To remove the match criteria, use the **no** form of this command.

match vlan {*vlan-id* | *vlan-range* | *vlan-combination*}

no match vlan

Syntax Description

vlan-id	The VLAN identification number. Valid range is from 1 to 4094; do not enter leading zeros.
vlan-range	A VLAN range. For example, 1 - 3.
vlan-combination	A combination of VLANs. For example, 1 - 3 5 - 7.

Command Default

No match criterion is configured.

Command Modes

Class-map configuration (config-cmap)
Policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
12.2(4)JA	This command was introduced.
12.4(2)T	This command was integrated into Cisco IOS Release 12.4(2)T.
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.

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.

Use the **match vlan** command to specify which fields in the incoming packets are examined to classify the packets. Only the IP access group or the MAC access group matching the Ether Type/Len field are supported.

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.

Examples

The following example uses the VLAN ID as a match criterion:

```
Router(config)# class-map matchsrcmac
Router(config-cmap)# match vlan 2
```

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 criteria of a VLAN ID of 2 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 vlan 2
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.

max-dropout (policy RTP)

To configure the maximum dropout metric for a Performance Monitor policy, use the **max-dropout** command in policy RTP configuration mode. To remove the configuration, use the **no** form of this command.

max-dropout *number*

no max-dropout *number*

Syntax Description

number	Specifies the maximum number of packets to ignore ahead of the current packet in terms of sequence number.

Command Default

Maximum number of dropouts is 5.

Command Modes

policy RTP configuration (config-pmap-c-mrtp)
policy inline RTP configuration (config-spolicy-inline-mrtp)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the maximum RTP dropout, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric rtp
Router(config-pmap-c-mrtp)# max-dropout 20
```

The following example shows how to set the maximum RTP dropout, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric rtp
Router(config-spolicy-inline-mrtp)# max-dropout 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

max-reorder (policy RTP)

To configure the maximum reorder metric for a Performance Monitor policy, use the **max-reorder** command in policy RTP configuration mode. To remove the configuration, use the **no** form of this command.

max-reorder *number*

no max-reorder *number*

Syntax Description

number	Specifies the maximum number of packets to ignore ahead of the current packet in terms of sequence number.

Command Default

Maximum number of reorders is 5.

Command Modes

policy RTP configuration (config-pmap-c-mrtp)
policy inline RTP configuration (config-spolicy-inline-mrtp)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the maximum RTP reorder, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric rtp
Router(config-pmap-c-mrtp)# max-reorder 20
```

The following example shows how to set the maximum RTP reorder, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric rtp
Router(config-spolicy-inline-mrtp)# max-reorder 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

min-sequential (policy RTP)

To configure the mimimum number of packets in a sequence used to classify an RTP flow, use the **min-sequential** command in policy RTP configuration mode. To remove the configuration, use the **no** form of this command.

min-sequential *number*

no min-sequential *number*

Syntax Description

number	Specifies the mimimum number of sequental packets required to identify a stream as being an RTP flow.

Command Default

min-sequential is 5.

Command Modes

policy RTP configuration (config-pmap-c-mrtp)
policy inline RTP configuration (config-spolicy-inline-mrtp)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the mimimum number of packets in a sequence used to classify an RTP flow, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric rtp
Router(config-pmap-c-mrtp)# min-sequential 20
```

The following example shows how to set the mimimum number of packets in a sequence used to classify an RTP flow, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric rtp
Router(config-spolicy-inline-mrtp)# min-sequential 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

monitor metric ip-cbr

To configure IP-CBR monitor metrics for a Performance Monitor policy, use the **monitor metric ip-cbr** command in policy configuration mode. To remove the configuration, use the **no** form of this command.

monitor metric ip-cbr

no monitor metric ip-cbr

Syntax Description

This command has no arguments or keywords.

Command Modes

policy RTP configuration (config-pmap-c)
policy inline RTP configuration (config-if-spolicy-inline)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the layer 3 transmission rate to 10 gbps, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric ip-cbr
Router(config-pmap-c-mipcbr)# rate layer3 10 gbps
```

The following example shows how to set the layer 3 transmission rate to 10 gbps, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric ip-cbr
Router(config-spolicy-inline-mipcbr)# rate layer3 10 gbps
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

monitor metric rtp

To configure RTP monitor metrics for a Performance Monitor policy, use the **monitor metric rtp** command in policy configuration mode. To remove the configuration, use the **no** form of this command.

monitor metric rtp

no monitor metric rtp

Syntax Description

This command has no arguments or keywords.

Command Modes

policy configuration (config-pmap-c)
policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the RTP monitor metrics, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric rtp
```

The following example shows how to set the RTP monitor metrics, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric rtp
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

monitor parameters

To configure monitor parameters for a Performance Monitor policy, use the **monitor parameters** command in policy configuration mode. To remove the configuration, use the **no** form of this command.

monitor parameters

no monitor parameters

Syntax Description

This command has no arguments or keywords.

Command Modes

Policy configuration (config-pmap-c)
Policy inline configuration (config-if-spolicy-inline))

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the amount of time wait for a response when collecting data to 20 seconds, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor parameters
Router(config-pmap-c-mparam)# timeout 20
```

The following example shows how to set the amount of time wait for a response when collecting data to 20 seconds, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor parameters
Router(config-spolicy-inline-mparam)# timeout 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

option (Flexible NetFlow)

To configure options data parameters for a flow exporter for Flexible NetFlow or Performance Monitor, use the **option** command in flow exporter configuration mode. To remove options for a 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 timeout is 600 seconds. All other options data parameters are not configured.

Command Modes

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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 Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor.

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 export packets for Flexible NetFlow or Performance Monitor using quality of service (QoS) or encryption, use the **output-features** command in 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 or Performance Monitor export packets.

Command Modes

flow exporter configuration (config-flow-exporter)

Command History

Release	Modification
12.4(20)T	This command was introduced.
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.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor.

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 or Performance Monitor export packets.

Examples

The following example configures the use of QoS or encryption on Flexible NetFlow or Performance Monitor 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.

policy-map type performance-monitor

To configure a policy for Performance Monitor, use the **policy-map type performance-monitor** command in global configuration mode. To remove the policy, use the **no** form of this command.

policy-map type performance-monitor *policy-name*

no policy-map type performance-monitor *policy-name*

Syntax Description

policy-name	Specifies the name of the Performance Monitor policy to create or edit.

Command Modes

Global configuration (config)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If you do not have an existing flow monitor, you can still configure a flow policy by using the **flow monitor inline** command to create a new flow monitor.

Examples

The following example shows how to configure a Performance Monitor policy.

```
Router(config)# policy-map type performance-monitor PM-POLICY-4
```

Related Commands

Command	Description
flow monitor type performance-monitor	Creates a flow monitor.
flow record type performance-monitor	Creates a flow record for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

rate layer3

To configure a Layer 3 transmission rate for a Performance Monitor policy, use the **rate layer3** command in policy IP-CBR configuration mode. To remove the configuration, use the **no** form of this command.

rate layer3 {*rate-byte* {**bps** | **kbps** | **mbps** | **gbps**} | **packet**}

no rate layer3 {*rate-byte* {**bps** | **kbps** | **mbps** | **gbps**} | **packet**}

Syntax Description

rate-byte	Rate in Bps, kBps, mBps, or gBps. The range is from 1 to 65535.
bps	Specifies that the rate is in bytes per second.
kbps	Specifies that the rate is in kilobytes per second.
mbps	Specifies that the rate is in megabytes per second. The default is 100.
gbps	Specifies that the rate is in gigabytes per second.
packet	Use the rate specified in the packet.

Command Default

The Layer 3 transmission rate is 100 mbps.

Command Modes

Policy IP-CBR configuration (config-pmap-c-mipcbr)
Policy inline IP-CBR configuration (config-spolicy-inline-mipcbr)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the Layer 3 transmission rate to 10 gbps, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric ip-cbr
Router(config-pmap-c-mipcbr)# rate layer3 10 gbps
```

The following example shows how to set the Layer 3 transmission rate to 10 gbps, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric ip-cbr
Router(config-spolicy-inline-mipcbr)# rate layer3 10 gbps
```

Related CommandsR

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

react (policy)

To configure threshold parameters for a Performance Monitor policy, use the **react** command in policy configuration mode. To disable all threshold monitoring or to disable individual monitored elements, use the **no** form of this command.

react *ID* {**media-stop** | **mrv** | **rtp-jitter-average | transport-packets-lost-rate**}

no react *ID* {**media-stop** | **mrv** | **rtp-jitter-average | transport-packets-lost-rate**}

Syntax Description

ID	ID for react configuration. The range is 1 to 65535.
media-stop	A reaction occurs when no traffic is found for the flow.
mrv	A reaction occurs when the MRV value violates the threshold. MRV is a fixed-point percentage, calculated by dividing the difference between the actual rate and the expected rate, by the expected rate.
rtp-jitter-average	A reaction occurs when the average jitter value violates the threshold.
transport-packets-lost-rate	A reaction occurs when the rate at which transport packets are lost violates the threshold. This rate is calculated by dividing the number of lost packets by the expected packet count.

Command Default

Service policy threshold monitoring is disabled.

Command Modes

policy configuration (config-pmap-c)
policy inline configuration (config-if-spolicy-inline)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can configure multiple **react** commands for a Performance Monitor policy.

Examples

The following example shows how to specify that SNMP MIB variables will receive an alarm or notification, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# react 2000 rtp-jitter-average
Router(config-pmap-c-react)# action snmp
```

The following example shows how to specify that SNMP MIB variables will receive an alarm or notification, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# react 2000 rtp-jitter-average
Router(config-spolicy-inline-react)# action snmp
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

record (Performance Monitor)

To associate a flow record with a flow monitor for Performance Monitor, use the **record** command in the appropriate Performance Monitor configuration mode. To remove the association, use the **no** form of this command.

record {*record-name* | **default-rtp** | **default-tcp**}

no record {*record-name* | **default-rtp** | **default-tcp**}

Syntax Description

record-name	Specifies which flow record is being associated.
default-rtp	Specifies that the default RTP flow record is being associated.
default-tcp	Specifies that the default TCP flow record is being associated.

Command Modes

Flow monitor configuration (config-flow-monitor)
Monitor configuration (config-pmap)
Policy monitor configuration (config-pmap-c-flowmon)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can associate a flow record with a flow monitor for Performance Monitor while configuring either a flow monitor, policy map, or service policy.

Examples

The following example shows how to configure a flow record:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class class-4
Router(config-pmap-c)# flow monitor inline
Router(config-pmap-c-flowmon)# record record-4
```

Related Commands

Command	Description
flow monitor type performance-monitor	Creates a flow monitor.
policy-map type performance-monitor	Creates a policy map.
service-policy type performance-monitor	Associates policy map with an interface.

rename (policy)

To rename a policy for Performance Monitor, use the **rename** command in the policy configuration mode.

rename *policy-name*

Syntax Description

policy-name	The new name for the policy.

Command Modes

Policy configuration (config-pmap)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to rename a policy:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# rename policy-20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy map.

service-policy type performance-monitor

To configure the association of a Performance Monitor policy to an interface, use the **service-policy type performance-monitor** command in interface configuration mode. To remove the association, use the **no** form of this command.

service-policy type performance-monitor {{**input** | **output**} *policy-name* | **inline** {**input** | **output**}}

no service-policy type performance-monitor {{**input** | **output**} *policy-name* | **inline** {**input** | **output**}}

Syntax Description

input	Assocate the Performance Monitor policy to the incoming interface.
output	Assocate the Performance Monitor policy to the outgoing interface.
policy-name	Specifies which Performance Monitor policy to assocate to an interface.
inline	Enters inline mode to configure a new flow monitor for the Performance Monitor policy.

Command Modes

interface configuration (config-if)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If you do not have an existing flow policy, you can still association a flow policy to an interface by using the **inline** option to create a new flow policy.

Examples

The following example shows how to configure an association of a Performance Monitor policy to an interface for the input direction.

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor input PM-POLICY-4
```

Related Commands

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

show performance monitor cache

To display the contnet of the cache for Performance Monitor, use the **show performance monitor cache** command in privileged EXEC mode.

show performance monitor cache [**policy** *policy map name* **class** *class map name*] [**interface** *interface name*]

Syntax Description

policy *policy map name*	Show statistics only for the specified policy.
class *class map name*	Show statistics only for the specified class.
interface *interface name*	Show statistics for the specified interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no flow policy or interface is specified, all for all flow policies and interfaces are shown.

Examples

The following example shows the output for this command:

```
Router # show performance monitor cache

MMON Metering Layer Stats:
  static pkt cnt: 3049
  static cce sb cnt: 57
  dynamic pkt cnt: 0

  Cache type:                               Permanent
  Cache size:                                    2000
  Current entries:                                  8
  High Watermark:                                   9

  Flows added:                                      9
  Updates sent            (  1800 secs)             0

IPV4 SRC ADDR    IPV4 DST ADDR    IP PROT  TRNS SRC PORT  TRNS DST PORT

ipv4 ttl ipv4 ttl min ipv4 ttl max  ipv4 dscp bytes long perm pktslong perm  user space vm

==============================================================================================
10.1.1.1         10.1.2.3              17           4000           1967
0             0             0  0x00                          80
1 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
```

```
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000

10.1.1.1         10.1.2.3              17           6000           1967
0             0              0  0x00                          80
1  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000

10.1.1.1         10.1.2.3              17           4000           2000
0             0              0  0x00                          44
1  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1         10.1.2.3               6           6000           3000
0             0              0  0x00                          84
2  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1         10.1.2.3              17           1967           6001
0             0              0  0x00                          36
1  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1         10.1.2.3              17           1967           4001
0             0              0  0x00                          36
1  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1         10.1.2.3               6           3001           6001
0             0              0  0x00                         124
3  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
10.1.1.1         10.1.2.3              17           2001           4001
0             0              0  0x00                          44
1  0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
```

```
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000 0x00000000
0x00000000
```

Table 11 describes the significant fields shown in the display.

Table 11 show performance monitor cache Field Descriptions

Field	Description
static pkt cnt	Number static packets collected in this cache.
static cce sb cnt	Number of CCE SBs.
dynamic pkt cnt	Number of dynamic packets in this cache
Cache type	Type fo cache.
Cache size	Maximum number of entries that can be collected in this cache.
Current entries	Current number of entries collected in this cache.
High Watermark	Highest number of entries collected in this cache.
Flows added	Number of flows added for this cache.
Updates sent	Number of updates sent for this cahe.
IPV4 SRC ADDR	IP address of the source of the flow.
IPV4 DST ADDR	IP addres of the destiation of the flow.
IP PROT	IP protocil used by the flow.
TRNS SRC PORT	Port number used by the source of the flow.
TRNS DST PORT	Port number used by the destiantion of flow.
ipv4 ttl	IPv4 time-to-live (TTL).
ipv4 ttl min	Miniumum IPv4 time-to-live (TTL).
ipv4 ttl max	Maximum IPv4 time-to-live (TTL).
ipv4 dscp	IPv4 differentiated services code point (DCSP).
bytes long perm	Number of long perm bytes.
pkts long perm	Number of long perm packets.
user space vm	User space VM.

Related CommandsR

Command	Description
show performance monitor historical	Displays historical sets of statistics collected by Performance Monitor.

show performance monitor clock rate

To display information about clock rates for performance monitor classes, use the **show performance monitor clock rate** command in privileged EXEC mode.

show performance monitor clock rate [**policy** *policy map name* **class** *class map name*]

Syntax Description

policy *policy map name*	Show statistics only for the specified policy.
class *class map name*	Show statistics only for the specified class.

Command Modes

privileged EXEC

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You must have at least one active session before clock information can be displayed.

Examples

The following example displays performance monitor clock rate information:

```
Router# show performance monitor clock rate

Load for five secs: 6%/2%; one minute: 5%; five minutes: 5% Time source is NTP,
17:41:35.508 EST Wed Feb 16 2011

RTP clock rate for Policy: all-apps-w-mask, Class: IPTV
     Payload type     Clock rate(Hz)

     pcmu     (0  )      8000
     gsm      (3  )      8000
     g723     (4  )      8000
     dvi4     (5  )      8000
     dvi4-2   (6  )      16000
     lpc      (7  )      8000
     pcma     (8  )      8000
     g722     (9  )      8000
     l16-2    (10 )      44100
     l16      (11 )      44100
     qcelp    (12 )      8000
     cn       (13 )      8000
     mpa      (14 )      90000
     g728     (15 )      8000
     dvi4-3   (16 )      11025
     dvi4-4   (17 )      22050
     g729     (18 )      8000
     celb     (25 )      90000
     jpeg     (26 )      90000
     nv       (28 )      90000
     h261     (31 )      90000
```

```
     mpv     (32 )     90000
     mp2t    (33 )     90000
     h263    (34 )     90000
     default           90000

RTP clock rate for Policy: all-apps, Class: telepresence-CS4
     Payload type     Clock rate(Hz)

     pcmu    (0  )     8000
     gsm     (3  )     8000
     g723    (4  )     8000
     dvi4    (5  )     8000
     dvi4-2  (6  )     16000
     lpc     (7  )     8000
     pcma    (8  )     8000
     g722    (9  )     8000
     l16-2   (10 )     44100
     l16     (11 )     44100
     qcelp   (12 )     8000
     cn      (13 )     8000
     mpa     (14 )     90000
     g728    (15 )     8000
     dvi4-3  (16 )     11025
     dvi4-4  (17 )     22050
     g729    (18 )     8000
     celb    (25 )     90000
     jpeg    (26 )     90000
     nv      (28 )     90000
     h261    (31 )     90000
     mpv     (32 )     90000
     mp2t    (33 )     90000
     h263    (34 )     90000
             (96 )     48000
             (112)     90000
     default           90000


RTP clock rate for Policy: all-apps, Class: IPVS-traffic-rtp
     Payload type     Clock rate(Hz)

     pcmu    (0  )     8000
     gsm     (3  )     8000
     g723    (4  )     8000
     dvi4    (5  )     8000
     dvi4-2  (6  )     16000
     lpc     (7  )     8000
     pcma    (8  )     8000
     g722    (9  )     8000
     l16-2   (10 )     44100
     l16     (11 )     44100
     qcelp   (12 )     8000
     cn      (13 )     8000
     mpa     (14 )     90000
     g728    (15 )     8000
     dvi4-3  (16 )     11025
     dvi4-4  (17 )     22050
     g729    (18 )     8000
     celb    (25 )     90000
     jpeg    (26 )     90000
     nv      (28 )     90000
     h261    (31 )     90000
     mpv     (32 )     90000
     mp2t    (33 )     90000
     h263    (34 )     90000
```

```
            (96 )      30000
    default            90000
```

Table 12 describes the significant fields shown in the display.

Table 12 show performance monitor clock Field Descriptions

Field	Description
Payload type	The values for the payload type and their associated type numbers are celb (25), cn (13), dvi4 (5) (8000 Hz as described in RFC 3551, *RTP Profile for Audio and Video Conferences with Minimal Control*), dvi4-2 (6) (8000 Hz as described in RFC 3551), dvi4-3 (16) (DVI4 Dipol 11025 Hz), dvi4-4 (17) DVI4 Dipol 22050 Hz), g722 (9), g723 (4), g728 (15), g729 (18), gsm (3), h261 (31), h263 (34), jpeg (26), l16 (11) (L16 channel 1), l16-2 (10) (L16 channel 2), lpc (7), mp2t (33), mpa (14), mpv (32), nv (28), pcma (8), pcmu (0), qcelp (12).
Clock rate(Hz)	Clock rate in cycles per sec (Hz).

Related Commands

Command	Description
clock-rate	Configure the rate for the RTP packet time-stamp clock.

show performance monitor clients

To display information about clients for performance monitor, use the **show performance monitor clients** command in privileged EXEC mode.

show performance monitor clients {**detail {***client-ID* | **all}** | **list**}

Syntax Description

detail *client-ID*	Show detailed information for the specified clients.
detail all	Show detailed information for all clients.
list	Show a list of clients.

Command Modes

privileged EXEC

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You must have Cisco Mediatrace configured and at least one active session before client information can be displayed.

Examples

The following example displays a list of performance monitor clients:

```
Router# show performance monitor clients list

Dynamic Video Monitor Client database list:
Total number of active clients: 1
ID name age(secs) flow(src,dst,src-port, dst-port)

1 Mediatrace-158244661 7498 10.10.10.1 1000 10.10.12.2 2000 17
```

Table 13 describes the significant fields shown in the display.

The following example displays details for all performance monitor clients:

```
Router# show performance monitor clients detail all

Client name for ID 1 : Mediatrace-131419052
   Type: Mediatrace
   Age: 443 seconds
   Monitor Object: _MMON_DYN_-class-map-69
        Flow spec: (dvmc-acl#47) 10.10.130.2 1000 10.10.132.2 2000 17
        monitor parameters
                interval duration 60
                timeout 2
                history 1
                flows 100
        monitor metric rtp
                min-sequential 10
```

```
        max-dropout 5
        max-reorder 5
        clock-rate 112 90000
        clock-rate default 90000
        ssrc maximum 20
monitor metric ip-cbr
        rate layer3 packet 20
Flow record: dvmc_fnf_fdef_47
        Key fields:
                ipv4 source address
                ipv4 destination address
                transport source-port
                transport destination-port
                ip protocol
        Non-key fields:
                monitor event
                application media event
                routing forwarding-status
                ip dscp
                ip ttl
                counter bytes rate
                application media bytes rate
                transport rtp jitter mean
                transport packets lost counter
                transport packets expected counter
                transport event packet-loss counter
                transport packets lost rate
                timestamp interval
                counter packets dropped
                counter bytes
                counter packets
                application media bytes counter
                application media packets counter
Monitor point: _MMON_DYN_-policy-map-70 GigabitEthernet0/3 output
Classification Statistic:
        matched packet: 545790
        matched byte: 64403220
```

Table 14 describes the significant fields shown in the display.

Table 13 show performance monitor clients list Field Descriptions

Field	Description
Total number of active clients	Number of active clients.
ID	ID of the client.
Name	Name of the client.
Age(secs)	Number seconds the client has been active.
Flow (src)	IP address of the source of the flow.
Flow(dst)	IP address of the destination of the flow.
Flow(src-port)	Port number of the source of the flow.
Flow(dst-port)	Port number of the destination of the flow.

Table 14 show performance monitor clients detail all Field Descriptions

Field	Description
Client name for ID *number*	Name and ID of the client.
Type	Type of client
Age	Number seconds the client has been active.
Monitor Object: _MMON_DYN_-class-map-69	Name of flow monitor and class map used by this client.
Flow spec: (dvmc-acl#47) 10.10.130.2 1000 10.10.132.2 2000 17	Source and destination IP addresses and ports of the flow and the code for flow protocol.
monitor parameters	Settings for the monitor parameters.
monitor metric rtp	Settings for the monitor metric RTP parameters.
monitor metric ip-cbr	Settings for the monitor metric IP-CBR parameters.
Flow record: dvmc_fnf_fdef_47	Name of the flow used by the client.
Key fields:	Key fields defined for the flow used by the client.
Non-key fields:	Non-key fields defined for the flow used by the client.
Monitor point: _MMON_DYN_-policy-map-70 GigabitEthernet0/3 output	Name of the policy map and interface used by this client.
Matched packet:	Number of packets matched to criteria defined by the flow record for the client.
Matched byte:	Number of bytes matched to criteria defined by the flow record for the client.

Related Commands

Command	Description
show performance monitor historical	Displays historical sets of statistics collected by Performance Monitor.

show performance monitor history

To display the statistics collected by Performance Monitor during the current or past intervals, use the **flow performance monitor history** command in privileged EXEC mode.

show performance monitor history [**interval** {**all** | *number* [**start** *number*]} | **interface** *interface name* [*filter*] | **policy** *policy map name* **class** *class map name* [*filter*]} | *filter*]

where *filter* = {**ip** {*source-addr source-prefix* | **any**} {*dst-addr dst-prefix* | **any**} | {**tcp** | **udp**} {*source-addr source-prefix* | **any**} {[**eq** | **lt** | **gt** *number* | **range** *min max* | **ssrc** {*ssrc-number* | **any**} | {{*dst-addr dst-prefix* | **any**} **eq** | **lt** | **gt** *number* | **range** *min max* | **ssrc** {*ssrc-number* | **any**}}

Syntax Description

interval	Show statistics only for the specified intervals.
all	Show statistics for all intervals.
number	Show statistics only for the specified number of intervals.
start *number*	Show statistics starting at the specified interval number.
interface *interface name*	Show statistics for the specified interface. If no interface is specified, show statistics for all interfaces associated with a performance-monitor policy-map.
policy *policy map name*	Show statistics only for the specified policy.
class *class map name*	Show statistics only for the specified class.
ip	Show statistics for an IP flow.
tcp	Show statistics for a TCP flow.
udp	Show statistics for a UDP flow.
source-addr source-prefix	Show statistics for the specified flow source.
any	Show statistics for any flow source.
dst-addr dst-prefix	Show statistics for the specified flow destination.
any	Show statistics for any flow destination.
eq	Show statistics only for the specified source port number.
lt	Show statistics only for source port numbers less than the specified number.
gt	Show statistics only for source port numbers greater than the specified number.
range	Show statistics only for source port number. within the specified range.
min	Minimum value for the range for which to show statistics.
max	Maximum value for the range for which to show statistics.
any	Show statistics for any destination IP address.
ssrc *ssrc-number*	Show statistics for the specified Synchronization Source.
ssrc any	Show statistics for all Synchronization Sources (SSRCs).

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

You can display the statistics collected by Performance Monitor during any or all intervals, including the current one. The duration of collection intervals is specified by the **interval duration** command.

If no flow policy or interface is specified, statistics for all flow policies and interfaces are shown.

Examples

The following example shows the output for this command:

```
Router # show performance monitor history

Codes: *    - field is not configurable under flow record
       NA   - field is not applicable for configured parameters

Match: ipv4 src addr = 1.1.1.1, ipv4 dst addr = 7.7.7.2, ipv4 prot = udp, trns src port =
20001, trns dst port = 10000, SSRC = 4294967291
 Policy: RTP_POL, Class: RTP_CLASS, Interface: GigabitEthernet0/4, Direction: input

  start time                                              14:57:34
                                                          ============
 *history bucket number                                 : 1
 *counter flow                                          : 1
  counter bytes                                         : 0
  counter bytes rate                              (Bps) : NA
 *counter bytes rate per flow                     (Bps) : NA
 *counter bytes rate per flow min                 (Bps) : NA
 *counter bytes rate per flow max                 (Bps) : NA
  counter packets                                       : 0
 *counter packets rate per flow                         : 0
  counter packets dropped                               : 0
  routing forwarding-status reason                      : Unknown
  interface input                                       : NA
  interface output                                      : NA
  monitor event                                         : true
  ipv4 dscp                                             : 0
  ipv4 ttl                                              : 57
  application media bytes counter                       : 0
  application media packets counter                     : 0
  application media bytes rate                    (Bps) : NA
 *application media bytes rate per flow           (Bps) : NA
 *application media bytes rate per flow min       (Bps) : NA
 *application media bytes rate per flow max       (Bps) : NA
  application media packets rate                  (pps) : 0
  application media event                               : Stop
 *transport rtp flow count                              : 0
  transport rtp jitter mean                      (usec) : NA
  transport rtp jitter minimum                   (usec) : NA
  transport rtp jitter maximum                   (usec) : NA
 *transport rtp payload type                            : 0
  transport event packet-loss counter                   : NA
 *transport event packet-loss counter min               : NA
 *transport event packet-loss counter max               : NA
  transport packets expected counter                    : NA
  transport packets lost counter                        : NA
 *transport packets lost counter minimum                : NA
 *transport packets lost counter maximum                : NA
```

```
 transport packets lost rate                    ( % ) : NA
*transport packets lost rate min                ( % ) : NA
*transport packets lost rate max                ( % ) : NA
*transport tcp flow count                             : 1
*transport round-trip-time sum                 (msec) : 32
*transport round-trip-time samples                    : 1
 transport round-trip-time                     (msec) : 32
*transport round-trip-time min                 (msec) : 32
*transport round-trip-time max                 (msec) : 32
```

Table 15 describes the significant fields shown in the display.

Table 15 show performance monitor history Field Descriptions

Field	Description
history bucket number	Number of the bucket of historical data collected.
counter flow	Number of flows collected.
counter bytes	Total number of bytes collected for all flows.
counter bytes rate	Average number of packets or bits (as configured) processed by the monitoring system per second during the monitoring interval for all flows.
counter bytes rate per flow	Average number of packets or bits (as configured) processed by the monitoring system per second during the monitoring interval for each flow.
counter bytes rate per flow min	Minimum threshold for the average number of packets or bits processed per second for each flow.
counter bytes rate per flow max	Maximum threshold for the average number of packets or bits processed per second for each flow.
counter packets	Total number of IP packets sent for all flows.
counter packets rate per flow	Number of IP packets sent for each flow.
counter packets dropped	IP packet drops by any intermediate system in any of the mionitored flows.

Table 15 show performance monitor history Field Descriptions (continued)

Field	Description
routing forwarding-status reason	Forwarding status is encoded using eight bits with the two most significant bits giving the status and the six remaining bits giving the reason code. Status is either unknown (00), Forwarded (10), Dropped (10) or Consumed (11). The following list shows the forwarding status values for each status category. **Unknown** • 0 **Forwarded** • Unknown 64 • Forwarded Fragmented 65 • Forwarded not Fragmented 66 **Dropped** • Unknown 128, • Drop ACL Deny 129, • Drop ACL drop 130, • Drop Unroutable 131, • Drop Adjacency 132, • Drop Fragmentation & DF set 133, • Drop Bad header checksum 134, • Drop Bad total Length 135, • Drop Bad Header Length 136, • Drop bad TTL 137, • Drop Policer 138, • Drop WRED 139, • Drop RPF 140, • Drop For us 141, • Drop Bad output interface 142, • Drop Hardware 143, **Consumed** • Unknown 192, • Terminate Punt Adjacency 193, • Terminate Incomplete Adjacency 194, • Terminate For us 195
interface out	Outgoing interface index.

Table 15 show performance monitor history Field Descriptions (continued)

Field	Description
interface in	Incoming interface index.
monitor event	Bit 1 indicates that one of the thresholds specified by a react statement for the flow was crossed at least once in the monitoring interval. Bit 2 indicates that there was a loss-of-confidence in measurement.
ipv4 dscp	IPv4 differentiated services code point (DCSP).
ipv4 ttl	IPv4 time-to-live (TTL).
application media bytes counter	Number of IP bytes from by media applications received for a specific media stream.
application media packets counter	Number of IP packets produced from media applications received for a specific media stream.
application media bytes rate	Average media bit rate (bps) for all flows during the monitoring interval.
application media bytes rate per flow	Average media bit rate (bps) for each flow during the monitoring interval.
application media bytes rate per flow min	Minimum threshold for the rate of application media bytes, in Bps, collected per flow.
application media bytes rate per flow max	Maximum threshold for the rate of application media bytes, in Bps, collected per flow.
application media event	Bit 1 is not used. Bit 2 indicates that no media application packets were seen, in other words, a Media Stop Event occured.
transport rtp flow count	Number of RTP flows collected.
transport rtp jitter mean	Mean deviation of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
transport rtp jitter minimum	Minimum threshold for the deviation of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
transport rtp jitter maximum	Maximum threshold for the deviation of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
transport rtp payload type	Code for the payload format. Payload type codes can be defined dynamically or codes for default audio and video format can be used as defined in RFC 3551. An RTP source can change the payload type during a session, but a receiver MUST ignore packets with payload types that it does not understand. Therefore, some measurements taken during monitoring may not be accurate.
transport event packet-loss counter	Number of loss events (number of contiguous sets of lost packets).
transport event packet-loss counter min	Minimum threshold for the number of packet loss events.
transport event packet-loss counter max	Maximum threshold for the number of packet loss events.
transport packets expected counter	Number of packets expected.

Table 15 show performance monitor history Field Descriptions (continued)

Field	Description
transport packets lost counter	Number of packets lost.
transport packets lost counter minimum	Minimum threshold for the number of packets lost.
transport packets lost counter maximum	Maximum threshold for the number of packets lost.
transport packets lost rate	Rate of packets lost, in percent.
transport packets lost rate min	Minimum threshold for the percent of packets lost.
transport packets lost rate max	Maximum threshold for the percent of packets lost.
transport tcp flow count	Number of the flow collected.
transport round-trip-time sum	Total of all round-trip-times.
transport round-trip-time samples	Number of round-trip-time samples
transport round-trip-time	Average of all round-trip-times.
transport round-trip-time min	Smallest of all round-trip-times.
transport round-trip-time max	Largest of all round-trip-times.

Related Commands

Command	Description
show performance monitor status	Displays statistics collected by Performance Monitor.

show performance monitor status

To display the cumulative statistics collected by Performance Monitor during the specified number of most recent intervals, use the **show performance monitor status** command in privileged EXEC mode.

show performance monitor status [**interface** *interface name* [*filter*] | **policy** *policy map name* **class** *class map name* [*filter*]} | *filter* | **sort** {*bitrate-max* | *loss-event* | *rtt-max*}]

where *filter* = {**ip** {*source-addr source-prefix* | **any**} {*dst-addr dst-prefix* | **any**} | {**tcp** | **udp**} {*source-addr source-prefix* | **any**} {[**eq** | **lt** | **gt** *number* | **range** *min max* | **ssrc** {*ssrc-number* | **any**} | {{*dst-addr dst-prefix* | **any**} **eq** | **lt** | **gt** *number* | **range** *min max* | **ssrc** {*ssrc-number* | **any**}}

Syntax Description

interface *interface name*	Show statistics for the specified interface. If no interface is specified, show statistics for all interfaces associated with a performance-monitor policy-map.
policy *policy map name*	Show statistics only for the specified policy.
class *class map name*	Show statistics only for the specified class.
sort	Sort the statistics output.
bitrate-max	Sort the statistics output by the maximum bite rate.
loss-event	Sort the statistics output by the loss event count.
rtt-max	Sort the statistics output by the maximum Round Trip Time (RRT).
ip	Show statistics for an IP flow.
tcp	Show statistics for a TCP flow.
udp	Show statistics for a UDP flow.
source-addr source-prefix	Show statistics for the specified flow source.
any	Show statistics for any flow source.
dst-addr dst-prefix	Show statistics for the specified flow destination.
any	Show statistics for any flow destination.
eq	Show statistics only for the specified source port number.
lt	Show statistics only for source port numbers less than the specified number.
gt	Show statistics only for source port numbers greater than the specified number.
range	Show statistics only for source port number. within the specified range.
min	Minimum value for the range for which to show statistics.
max	Maximum value for the range for which to show statistics.
any	Show statistics for any destination IP address.
ssrc *ssrc-number*	Show statistics for the specified Synchronization Source.
ssrc any	Show statistics for all Synchronization Sources (SSRCs).
network *mask*	Show statistics for the specified network.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

This command displays the cumulative statistics for the specified number of most recent intervals. The number of intervals is configured using the **history** command. The default settings for this commands is 10 of the most recent collection intervals. The duration of collection intervals is specified by the **interval duration** command.

If no flow policy or interface is specified, statistics for all flow policies and interfaces are shown.

Examples

The following example shows the output for this command:

```
Router # show performance monitor status
Codes: *   - field is not configurable under flow record
       NA  - field is not applicable for configured parameters

Match: ipv4 src addr = 1.1.1.1, ipv4 dst addr = 7.7.7.2, ipv4 prot = udp, trns src port =
20001, trns dst port = 10000, SSRC = 4294967291
 Policy: RTP_POL, Class: RTP_CLASS, Interface: GigabitEthernet0/4, Direction: input


 *counter flow                                    : 7
  counter bytes                                   : 43560
  counter bytes rate                       (Bps)  : 311
 *counter bytes rate per flow              (Bps)  : 44
 *counter bytes rate per flow min          (Bps)  : 0
 *counter bytes rate per flow max          (Bps)  : 442
  counter packets                                 : 990
 *counter packets rate per flow                   : 1
  counter packets dropped                         : 0
  routing forwarding-status reason                : NA
  interface input                                 : NA
  interface output                                : NA
  monitor event                                   : NA
  ipv4 dscp                                       : NA
  ipv4 ttl                                        : NA
  application media bytes counter                 : 0
  application media packets counter               : 0
  application media bytes rate             (Bps)  : 169
 *application media bytes rate per flow    (Bps)  : 24
 *application media bytes rate per flow min (Bps) : 0
 *application media bytes rate per flow max (Bps) : 241
  application media packets rate           (pps)  : 7
  application media event                         : Stop
 *transport rtp flow count                        : 6
  transport rtp jitter mean                (usec) : 457
  transport rtp jitter minimum             (usec) : 3
  transport rtp jitter maximum             (usec) : 2031
 *transport rtp payload type                      : 31
  transport event packet-loss counter             : 0
 *transport event packet-loss counter min         : 0
 *transport event packet-loss counter max         : 0
  transport packets expected counter              : 990
  transport packets lost counter                  : 0
 *transport packets lost counter minimum          : 0
 *transport packets lost counter maximum          : 0
  transport packets lost rate               ( % ) : 0.00
```

```
*transport packets lost rate min              ( % ) : 0.00
*transport packets lost rate max              ( % ) : 0.00
*transport tcp flow count                           : 1
*transport round-trip-time sum               (msec) : 32
*transport round-trip-time samples                  : 1
 transport round-trip-time                   (msec) : 32
*transport round-trip-time min               (msec) : 32
*transport round-trip-time max               (msec) : 32
```

Table 16 describes the significant fields shown in the display.

Table 16 show performance monitor status Field Descriptions

Field	Description
counter flow	Number of flows collected.
counter bytes	Total number of bytes collected for all flows.
counter bytes rate	Average number of packets or bits (as configured) processed by the monitoring system per second during the monitoring interval for all flows.
counter bytes rate per flow	Average number of packets or bits (as configured) processed by the monitoring system per second during the monitoring interval for each flow.
counter bytes rate per flow min	Minimum threshold for the average number of packets or bits processed per second for each flow.
counter bytes rate per flow max	Maximum threshold for the average number of packets or bits processed per second for each flow.
counter packets	Total number of IP packets sent for all flows.
counter packets rate per flow	Number of IP packets sent for each flow.
counter packets dropped	IP packet drops by any intermediate system in any of the mionitored flows.

Table 16 show performance monitor status Field Descriptions (continued)

Field	Description
routing forwarding-status reason	Forwarding status is encoded using eight bits with the two most significant bits giving the status and the six remaining bits giving the reason code. Status is either unknown (00), Forwarded (10), Dropped (10) or Consumed (11). The following list shows the forwarding status values for each status category. **Unknown** • 0 **Forwarded** • Unknown 64 • Forwarded Fragmented 65 • Forwarded not Fragmented 66 **Dropped** • Unknown 128, • Drop ACL Deny 129, • Drop ACL drop 130, • Drop Unroutable 131, • Drop Adjacency 132, • Drop Fragmentation & DF set 133, • Drop Bad header checksum 134, • Drop Bad total Length 135, • Drop Bad Header Length 136, • Drop bad TTL 137, • Drop Policer 138, • Drop WRED 139, • Drop RPF 140, • Drop For us 141, • Drop Bad output interface 142, • Drop Hardware 143, **Consumed** • Unknown 192, • Terminate Punt Adjacency 193, • Terminate Incomplete Adjacency 194, • Terminate For us 195
interface out	Outgoing interface index.

Table 16 show performance monitor status Field Descriptions (continued)

Field	Description
interface in	Incoming interface index.
monitor event	Bit 1 indicates that one of the thresholds specified by a react statement for the flow was crossed at least once in the monitoring interval. Bit 2 indicates that there was a loss-of-confidence in measurement.
ipv4 dscp	IPv4 differentiated services code point (DCSP).
ipv4 ttl	IPv4 time-to-live (TTL).
application media bytes counter	Number of IP bytes from by media applications received for a specific media stream.
application media packets counter	Number of IP packets produced from media applications received for a specific media stream.
application media bytes rate	Average media bit rate (bps) for all flows during the monitoring interval.
application media bytes rate per flow	Average media bit rate (bps) for each flow during the monitoring interval.
application media bytes rate per flow min	Minimum threshold for the rate of application media bytes, in Bps, collected per flow.
application media bytes rate per flow max	Maximum threshold for the rate of application media bytes, in Bps, collected per flow.
application media event	Bit 1 is not used. Bit 2 indicates that no media application packets were seen, in other words, a Media Stop Event occured.
transport rtp flow count	Number of RTP flows collected.
transport rtp jitter mean	Mean deviation of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
transport rtp jitter minimum	Minimum threshold for the deviation of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
transport rtp jitter maximum	Maximum threshold for the deviation of the difference in packet spacing at the receiver compared to the sender for a pair of packets.
transport rtp payload type	Code for the payload format. Payload type codes can be defined dynamically or codes for default audio and video format can be used as defined in RFC 3551. An RTP source can change the payload type during a session, but a receiver MUST ignore packets with payload types that it does not understand. Therefore, some measurements taken during monitoring may not be accurate.
transport event packet-loss counter	Number of loss events (number of contiguous sets of lost packets).
transport event packet-loss counter min	Minimum threshold for the number of packet loss events.
transport event packet-loss counter max	Maximum threshold for the number of packet loss events.
transport packets expected counter	Number of packets expected.

Table 16 show performance monitor status Field Descriptions (continued)

Field	Description
transport packets lost counter	Number of packets lost.
transport packets lost counter minimum	Minimum threshold for the number of packets lost.
transport packets lost counter maximum	Maximum threshold for the number of packets lost.
transport packets lost rate	Rate of packets lost, in percent .
transport packets lost rate min	Minimum threshold for the percent of packets lost.
transport packets lost rate max	Maximum threshold for the percent of packets lost.
transport tcp flow count	Number of the flow collected.
transport round-trip-time sum	Total of all round-trip-times.
transport round-trip-time samples	Number of round-trip-time samples
transport round-trip-time	Average of all round-trip-times.
transport round-trip-time min	Smallest of all round-trip-times.
transport round-trip-time max	Largest of all round-trip-times.

Related Commands

Command	Description
show performance monitor history	Displays historical sets of statistics collected by Performance Monitor.

show policy-map type performance-monitor

To display policy-map statistics for Performance Monitor, use the **show policy-map type performance-monitor** command in privileged EXEC mode.

show policy-map type performance-monitor[**interface** *interface-name*] [**class** *class-name*] [**input** | **output**]

Syntax Description

interface *interface-name*	Show statistics for the specified interface. If no interface is specified, show statistics for all interface associated with a performance-monitor policy-map.
class *class-name*	Show statistics only for the specified class.
input	Show input statistics for the interface.
output	Show output statistics for the interface.

Command Modes

Privileged EXEC (#)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

If no interface or class is specified, statistics for all interfaces and classes associated with a performance-monitor policy-map are shown.

Examples

The following example shows the output for this command for one Flow Policy::

```
Router # show policy-map type performance-monitor
Policy Map type performance-monitor PM-POLICY-4
    Class PM-CLASS-4
      flow monitor PM-MONITOR-4
        record PM-RECORD-4
        exporter PM-EXPORTER-4
      monitor parameters
        interval duration 30
        timeout 10
        history 10
        flows 8000
      monitor metric rtp
        min-sequential 5
        max-dropout 5
        max-reorder 5
        clock-rate default 90000
        ssrc maximum 5
```

Table 17 describes the significant fields shown in the display.

Table 17 show policy-map type performance-monitor Field Descriptions

Field	Description
Policy Map type performance-monitor	Name of the Performance Monitor Flow Policy.
flow monitor	Name of the Performance Monitor Flow Monitor.
record	Name of the Performance Monitor Flow Record.
exporter	Name of the Performance Monitor Flow Exporter.
monitor parameter	Parameters for the Flow Policy.
interval duration	The configured duration of the collection interval for the policy.
timeout	The configured amount of time wait for a response when collecting data for the policy.
history	The configured number of historical collections to keep for the policy.
flows	The configured number of flows to collect for the policy.
monitor metric rtp	RTP metrics for the Flow Policy.
min-sequential	The configured mimimum number of packets in a sequence used to classify an RTP flow.
max-dropout	The configured maximum number of packets to ignore ahead of the current packet in terms of sequence number.
max-reorder	The configured maximum number of packets to ignore behind the current packet in terms of sequence number.
clock-rate default	The configured clock rate for the RTP packet timestamp clock that is used to calculate the packet arrival latency.
ssrc maximum	The configured maximum number of SSRCs that can be monitored within same flow (as defined by the protocol, source/destination address, source/destination port). The range is from 1 to 50.

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.

source (Flexible NetFlow)

To configure the source IP address interface for all of the packets sent by a flow exporter for Flexible NetFlow or Performance Monitor, use the **source** command in flow exporter configuration mode. To remove the source IP address interface for all of the packets sent by a 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 flow exporter.
interface-number	Interface number whose IP address you want to use for the source IP address of the packets sent by a flow exporter.

Command Default

The IP address of the interface over which the Flexible NetFlow or Performance Monitor datagram is transmitted is used as the source IP address.

Command Modes

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor.

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 or Performance Monitor is used by the destination system to determine from which router the Flexible NetFlow or Performance Monitor data is arriving. If your network has two or more paths that can be used to send Flexible

NetFlow or Performance Monitor 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 or Performance Monitor datagrams from the same router, but with different source IP addresses. When the destination system receives Flexible NetFlow or Performance Monitor datagrams from the same router with different source IP addresses, the destination system treats the datagrams as if they were being sent from different routers. To avoid having the destination system treat the datagrams as if they were being sent from different routers, you must configure the destination system to aggregate the datagrams it receives from all of the possible source IP addresses in the router into a single 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 or Performance Monitor 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 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 or Performance Monitor 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 or Performance Monitor 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.

ssrc maximum

To configure the SSRC maximum metrics for a Performance Monitor policy, use the **ssrc maximum** command in policy RTP configuration mode. To remove the configuration, use the **no** form of this command.

ssrc maximum *number*

no monitor ssrc maximum *number*

Syntax Description

number	Specifies the maximum number of SSRCs that can be monitored within same flow (as defined by the protocol, source/destination address, source/destination port). The range is from 1 to 50.

Command Default

Maximum number of SSRC sessions is 10.

Command Modes

Policy RTP configuration (config-pmap-c-mrtp)
Policy inline RTP configuration (config-spolicy-inline-mrtp)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Usage Guidelines

It is not recommended that you limit the maximum number of SSRCs that can be monitored within same flow by using the **ssrc maximum** keyword**.** The flow engine will not learn new SSRC sessions once the maximum number is meet until a discovered flow is removed. Setting the value high will help to avoid the unexpected denial-of-service attacks.

Examples

The following example shows how to set the SSRC maximum, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor metric rtp
Router(config-pmap-c-mrtp)# ssrc maximum 40
```

The following example shows how to set the SSRC maximum, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor metric rtp
Router(config-spolicy-inline-mrtp)# ssrc maximum 40
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

template data timeout

To configure the template resend timeout for a flow exporter, use the **template data timeout** command in flow exporter configuration mode. To remove the template resend timeout for a 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 flow exporter is 600 seconds.

Command Modes

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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 Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor.

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.

threshold value (policy react and policy inline react)

To configure the threshold that determines whether alarms are sent for a Performance Monitor policy, use the **threshold value** command in policy configuration mode and policy inline react configuration mode. To remove the threshold setting, use the **no** form of this command.

threshold value {**ge** *number* | **gt** *number* | **le** *number* | **lt** *number* **| range** *rng-start rng-end*}

no threshold value {**ge** *number* | **gt** *number* | **le** *number* | **lt** *number* **| range** *rng-start rng-end*}

Syntax Description

ge *number*	Send alarms if the value is greater than or equal to threshold.
gt *number*	Send alarms if the value is greater than threshold.
le *number*	Send alarms if the value is less than or equal to threshold.
lt *number*	Send alarms if the value is less than threshold.
range *rng-start rng-end*	Send alarms if the value is within the specified range of the threshold.

Command Default

no thresholds are set.

Command Modes

Policy react configuration (config-pmap-c-react)
Policy inline react configuration (config-spolicy-inline-react)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to specify that alarms are sent if a value exceeds a threshold of 20, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# react 2000 rtp-jitter-average
Router(config-pmap-c-react)# threshold gt 20
```

The following example shows how to specify that alarms are sent if a value exceeds a threshold of 20, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# react 2000 rtp-jitter-average
Router(config-spolicy-inline-react)# threshold gt 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
service-policy type performance-monitor	Associates a policy with an interface.

timeout (monitor parameters)

To configure the amount of time to wait before a stopped flow is removed from the Performance Monitor database, use the **monitor parameters** command in monitor parameters configuration mode. To remove the configuration, use the **no** form of this command.

timeout *number*

no timeout

Syntax Description

timeout *number*	Specifies the number of intervals before a stopped flow is removed from the database.

Command Default

Timeout is 10 intervals.

Command Modes

Monitor parameters configuration (config-pmap-c-mparam)
Inline monitor parameters configuration (config-spolicy-inline-mparam)

Command History

Release	Modification
15.1(3)T	This command was introduced.
12.2(58)SE	This command was integrated into Cisco IOS Release 12.2(58)SE.

Examples

The following example shows how to set the amount of time wait for a response when collecting data to 20 intervals, while configuring a policy-map:

```
Router(config)# policy-map type performance-monitor policy-4
Router(config-pmap)# class PM-CLASS-4
Router(config-pmap-c)# monitor parameters
Router(config-pmap-c-mparam)# timeout 20
```

The following example shows how to set the amount of time wait for a response when collecting data to 20 intervals, while associating a service-policy with an interface:

```
Router(config)# interface ethernet 0/0
Router(config-if)# service-policy type performance-monitor inline input
Router(config-if-spolicy-inline)# monitor parameters
Router(config-spolicy-inline-mparam)# timeout 20
```

Related Commands

Command	Description
policy-map type performance-monitor	Creates a policy for Performance Monitor.
policy-map type performance-monitor	Creates a policy for Performance Monitor.

transport (Flexible NetFlow)

To configure the transport protocol for a flow exporter for Flexible NetFlow or Performance Monitor, use the **transport** command in flow exporter configuration mode. To remove the transport protocol for a 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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor.

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 flow exporter for Flexible NetFlow or Performance Monitor, use the **ttl** command in flow exporter configuration mode. To remove the TTL value for a flow exporter, use the **no** form of this command.

ttl *ttl*

no ttl

Syntax Description

ttl	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

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.
12.0(33)S	This command was implemented on the Cisco 12000 series routers.
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.
Cisco IOS XE Release 3.1S	This command was integrated into Cisco IOS XE Release 3.1S.
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.

Usage Guidelines

This command can be used with both Flexible NetFlow and Performance Monitor.

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.