



Cisco IOS Security Configuration Guide: Securing the Control Plane

Release 12.4T

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

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

Cisco IOS Security Configuration Guide: Securing the Control Plane
© 2009 Cisco Systems, Inc. All rights reserved.



About Cisco IOS and Cisco IOS XE Software Documentation

Last Updated: March 5, 2009

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

- [Documentation Objectives, page i](#)
- [Audience, page i](#)
- [Documentation Conventions, page ii](#)
- [Documentation Organization, page iii](#)
- [Additional Resources and Documentation Feedback, page xi](#)

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 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 includes the following topics:

- [Typographic Conventions, page ii](#)
- [Command Syntax Conventions, page ii](#)
- [Software Conventions, page iii](#)
- [Reader Alert Conventions, page iii](#)

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.) |
| <i>string</i> | A string is a nonquoted set of characters shown in italics. For example, when setting a Simple Network Management Protocol (SNMP) community string to <i>public</i> , 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. |
| <i>italic</i> | 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, 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 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

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



Caution

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



Note

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



Timesaver

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

Documentation Organization

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

- [Cisco IOS Documentation Set, page iv](#)
- [Cisco IOS Documentation on Cisco.com, page iv](#)
- [Configuration Guides, Command References, and Supplementary Resources, page v](#)

Cisco IOS Documentation Set

Cisco IOS documentation consists of the following:

- Release notes and caveats provide information about platform, technology, and feature support for a release and describe severity 1 (catastrophic), severity 2 (severe), and severity 3 (moderate) defects in released Cisco IOS code. Review release notes before other documents to learn whether or not updates have been made to a feature.
- Sets of configuration guides and command references organized by technology and published for each standard Cisco IOS release.
 - Configuration guides—Compilations of documents that provide informational and task-oriented descriptions of Cisco IOS features.
 - Command references—Compilations of command pages that provide detailed information about the commands used in the Cisco IOS features and processes that make up the related configuration guides. For each technology, there is a single command reference that covers 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 documentation organization and how to access various document types.

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

New Features List

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

Feature Guides

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

Configuration Guides

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

Command References

Command reference books describe Cisco IOS commands that are supported in many different software releases and on many different platforms. The books are provided by technology. For information about 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 xi](#).

Configuration Guides, Command References, and Supplementary Resources

[Table 1](#) lists, in alphabetical order, Cisco IOS and Cisco IOS XE software configuration guides and command references, including brief descriptions of the contents of the documents. The Cisco IOS command references are comprehensive, meaning that they include commands for both Cisco IOS software and Cisco IOS XE 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.

For additional information about configuring and operating specific networking devices, go to the Product Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

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

Table 1 *Cisco IOS and Cisco IOS XE Configuration Guides and Command References*

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|--|
| <i>Cisco IOS AppleTalk Configuration Guide</i> | AppleTalk protocol. |
| <i>Cisco IOS XE AppleTalk Configuration Guide</i> | |
| <i>Cisco IOS AppleTalk Command Reference</i> | |
| <i>Cisco IOS Asynchronous Transfer Mode Configuration Guide</i> | LAN ATM, multiprotocol over ATM (MPoA), and WAN ATM. |
| <i>Cisco IOS Asynchronous Transfer Mode Command Reference</i> | |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|---|---|
| <p><i>Cisco IOS Bridging and IBM Networking Configuration Guide</i></p> <p><i>Cisco IOS Bridging Command Reference</i></p> <p><i>Cisco IOS IBM Networking Command Reference</i></p> | <ul style="list-style-type: none"> • 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. |
| <p><i>Cisco IOS Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS XE Broadband and DSL Configuration Guide</i></p> <p><i>Cisco IOS Broadband and DSL Command Reference</i></p> | <p>Point-to-Point Protocol (PPP) over ATM (PPPoA) and PPP over Ethernet (PPPoE).</p> |
| <p><i>Cisco IOS Carrier Ethernet Configuration Guide</i></p> <p><i>Cisco IOS Carrier Ethernet Command Reference</i></p> | <p>Connectivity fault management (CFM), Ethernet Local Management Interface (ELMI), IEEE 802.3ad link bundling, Link Layer Discovery Protocol (LLDP), media endpoint discovery (MED), and operations, administration, and maintenance (OAM).</p> |
| <p><i>Cisco IOS Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS XE Configuration Fundamentals Configuration Guide</i></p> <p><i>Cisco IOS Configuration Fundamentals Command Reference</i></p> | <p>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.</p> |
| <p><i>Cisco IOS DECnet Configuration Guide</i></p> <p><i>Cisco IOS XE DECnet Configuration Guide</i></p> <p><i>Cisco IOS DECnet Command Reference</i></p> | <p>DECnet protocol.</p> |
| <p><i>Cisco IOS Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS XE Dial Technologies Configuration Guide</i></p> <p><i>Cisco IOS Dial Technologies Command Reference</i></p> | <p>Asynchronous communications, dial backup, dialer technology, dial-in terminal services and AppleTalk remote access (ARA), large scale dialout, dial-on-demand routing, dialout, modem and resource pooling, ISDN, multilink PPP (MLP), PPP, virtual private dialup network (VPDN).</p> |
| <p><i>Cisco IOS Flexible NetFlow Configuration Guide</i></p> <p><i>Cisco IOS Flexible NetFlow Command Reference</i></p> | <p>Flexible NetFlow.</p> |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|--|---|
| <i>Cisco IOS H.323 Configuration Guide</i> | Gatekeeper enhancements for managed voice services, Gatekeeper Transaction Message Protocol, gateway codec order preservation and shutdown control, H.323 dual tone multifrequency relay, H.323 version 2 enhancements, Network Address Translation (NAT) support of H.323 v2 Registration, Admission, and Status (RAS) protocol, tokenless call authorization, and VoIP gateway trunk and carrier-based routing. |
| <i>Cisco IOS High Availability Configuration Guide</i> <i>Cisco IOS XE High Availability Configuration Guide</i> <i>Cisco IOS High Availability Command Reference</i> | 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. |
| <i>Cisco IOS Integrated Session Border Controller Command Reference</i> | A VoIP-enabled device that is deployed at the edge of networks. An SBC is a toolkit of functions, such as signaling interworking, network hiding, security, and quality of service (QoS). |
| <i>Cisco IOS Intelligent Services Gateway Configuration Guide</i> <i>Cisco IOS Intelligent Services Gateway Command Reference</i> | Subscriber identification, service and policy determination, session creation, session policy enforcement, session life-cycle management, accounting for access and service usage, session state monitoring. |
| <i>Cisco IOS Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS XE Interface and Hardware Component Configuration Guide</i> <i>Cisco IOS Interface and Hardware Component Command Reference</i> | LAN interfaces, logical interfaces, serial interfaces, virtual interfaces, and interface configuration. |
| <i>Cisco IOS IP Addressing Services Configuration Guide</i> <i>Cisco IOS XE Addressing Services Configuration Guide</i> <i>Cisco IOS IP Addressing Services Command Reference</i> | Address Resolution Protocol (ARP), Network Address Translation (NAT), Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Next Hop Address Resolution Protocol (NHRP). |
| <i>Cisco IOS IP Application Services Configuration Guide</i> <i>Cisco IOS XE IP Application Services Configuration Guide</i> <i>Cisco IOS IP Application Services Command Reference</i> | 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). |
| <i>Cisco IOS IP Mobility Configuration Guide</i> <i>Cisco IOS IP Mobility Command Reference</i> | Mobile ad hoc networks (MANet) and Cisco mobile networks. |
| <i>Cisco IOS IP Multicast Configuration Guide</i> <i>Cisco IOS XE IP Multicast Configuration Guide</i> <i>Cisco IOS IP Multicast Command Reference</i> | 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). |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|--|--|
| <i>Cisco IOS IP Routing Protocols Configuration Guide</i> <i>Cisco IOS XE IP Routing Protocols Configuration Guide</i> <i>Cisco IOS IP Routing Protocols Command Reference</i> | Border Gateway Protocol (BGP), multiprotocol BGP, multiprotocol BGP extensions for IP multicast, bidirectional forwarding detection (BFD), Enhanced Interior Gateway Routing Protocol (EIGRP), Interior Gateway Routing Protocol (IGRP), Intermediate System-to-Intermediate System (IS-IS), on-demand routing (ODR), Open Shortest Path First (OSPF), and Routing Information Protocol (RIP). |
| <i>Cisco IOS IP SLAs Configuration Guide</i> <i>Cisco IOS XE IP SLAs Configuration Guide</i> <i>Cisco IOS IP SLAs Command Reference</i> | Cisco IOS IP Service Level Agreements (IP SLAs). |
| <i>Cisco IOS IP Switching Configuration Guide</i> <i>Cisco IOS XE IP Switching Configuration Guide</i> <i>Cisco IOS IP Switching Command Reference</i> | Cisco Express Forwarding, fast switching, and Multicast Distributed Switching (MDS). |
| <i>Cisco IOS IPv6 Configuration Guide</i> <i>Cisco IOS XE IPv6 Configuration Guide</i> <i>Cisco IOS IPv6 Command Reference</i> | For IPv6 features, protocols, and technologies, go to the IPv6 “Start Here” document at the following URL: http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-roadmap.html |
| <i>Cisco IOS ISO CLNS Configuration Guide</i> <i>Cisco IOS XE ISO CLNS Configuration Guide</i> <i>Cisco IOS ISO CLNS Command Reference</i> | ISO connectionless network service (CLNS). |
| <i>Cisco IOS LAN Switching Configuration Guide</i> <i>Cisco IOS XE LAN Switching Configuration Guide</i> <i>Cisco IOS LAN Switching Command Reference</i> | VLANs, Inter-Switch Link (ISL) encapsulation, IEEE 802.10 encapsulation, IEEE 802.1Q encapsulation, and multilayer switching (MLS). |
| <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Gateway GPRS Support Node Command Reference</i> | 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. |
| <i>Cisco IOS Mobile Wireless Home Agent Configuration Guide</i> <i>Cisco IOS Mobile Wireless Home Agent Command Reference</i> | Cisco Mobile Wireless Home Agent, an anchor point for mobile terminals for which mobile IP or proxy mobile IP services are provided. |
| <i>Cisco IOS Mobile Wireless Packet Data Serving Node Configuration Guide</i> <i>Cisco IOS Mobile Wireless Packet Data Serving Node Command Reference</i> | 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. |
| <i>Cisco IOS Mobile Wireless Radio Access Networking Configuration Guide</i> <i>Cisco IOS Mobile Wireless Radio Access Networking Command Reference</i> | Cisco IOS radio access network products. |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|--|---|
| <p><i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS XE Multiprotocol Label Switching Configuration Guide</i></p> <p><i>Cisco IOS Multiprotocol Label Switching Command Reference</i></p> | MPLS Label Distribution Protocol (LDP), MPLS Layer 2 VPNs, MPLS Layer 3 VPNs, MPLS Traffic Engineering (TE), and MPLS Embedded Management (EM) and MIBs. |
| <p><i>Cisco IOS Multi-Topology Routing Configuration Guide</i></p> <p><i>Cisco IOS Multi-Topology Routing Command Reference</i></p> | Unicast and multicast topology configurations, traffic classification, routing protocol support, and network management support. |
| <p><i>Cisco IOS NetFlow Configuration Guide</i></p> <p><i>Cisco IOS XE NetFlow Configuration Guide</i></p> <p><i>Cisco IOS NetFlow Command Reference</i></p> | Network traffic data analysis, aggregation caches, export features. |
| <p><i>Cisco IOS Network Management Configuration Guide</i></p> <p><i>Cisco IOS XE Network Management Configuration Guide</i></p> <p><i>Cisco IOS Network Management Command Reference</i></p> | 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). |
| <p><i>Cisco IOS Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS XE Novell IPX Configuration Guide</i></p> <p><i>Cisco IOS Novell IPX Command Reference</i></p> | Novell Internetwork Packet Exchange (IPX) protocol. |
| <p><i>Cisco IOS Optimized Edge Routing Configuration Guide</i></p> <p><i>Cisco IOS Optimized Edge Routing Command Reference</i></p> | Optimized edge routing (OER) monitoring, policy configuration, routing control, logging and reporting, and VPN IPsec/generic routing encapsulation (GRE) tunnel interface optimization. |
| <p><i>Cisco IOS Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS XE Quality of Service Solutions Configuration Guide</i></p> <p><i>Cisco IOS Quality of Service Solutions Command Reference</i></p> | Class-based weighted fair queuing (CBWFQ), custom queuing, distributed traffic shaping (DTS), generic traffic shaping (GTS), IP- to-ATM class of service (CoS), low latency queuing (LLQ), modular QoS CLI (MQC), Network-Based Application Recognition (NBAR), priority queuing, Security Device Manager (SDM), Multilink PPP (MLPPP) for QoS, header compression, AutoQoS, QoS features for voice, Resource Reservation Protocol (RSVP), weighted fair queuing (WFQ), and weighted random early detection (WRED). |
| <p><i>Cisco IOS Security Configuration Guide</i></p> <p><i>Cisco IOS XE Security Configuration Guide</i></p> <p><i>Cisco IOS Security Command Reference</i></p> | 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. |

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

| Configuration Guide and Command Reference Titles | Features/Protocols/Technologies |
|--|--|
| <i>Cisco IOS Service Selection Gateway Configuration Guide</i> <i>Cisco IOS Service Selection Gateway Command Reference</i> | Subscriber authentication, service access, and accounting. |
| <i>Cisco IOS Software Activation Configuration Guide</i> <i>Cisco IOS Software Activation Command Reference</i> | An orchestrated collection of processes and components to activate Cisco IOS software feature sets by obtaining and validating Cisco software licenses. |
| <i>Cisco IOS Software Modularity Installation and Configuration Guide</i> <i>Cisco IOS Software Modularity Command Reference</i> | 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. |
| <i>Cisco IOS Terminal Services Configuration Guide</i> <i>Cisco IOS Terminal Services Command Reference</i> <i>Cisco IOS XE Terminal Services Command Reference</i> | DEC, local-area transport (LAT), and X.25 packet assembler/disassembler (PAD). |
| <i>Cisco IOS Virtual Switch Command Reference</i> | 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, refer to the product-specific software configuration information for the Cisco Catalyst 6500 series switch or for the Metro Ethernet 6500 series switch. |
| <i>Cisco IOS Voice Configuration Library</i> <i>Cisco IOS Voice Command Reference</i> | Cisco IOS support for voice call control protocols, interoperability, physical and virtual interface management, and troubleshooting. The library includes documentation for IP telephony applications. |
| <i>Cisco IOS VPDN Configuration Guide</i> <i>Cisco IOS XE VPDN Configuration Guide</i> <i>Cisco IOS VPDN Command Reference</i> | 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. |
| <i>Cisco IOS Wide-Area Networking Configuration Guide</i> <i>Cisco IOS XE Wide-Area Networking Configuration Guide</i> <i>Cisco IOS Wide-Area Networking Command Reference</i> | Frame Relay, Layer 2 Tunneling Protocol Version 3 (L2TPv3), Link Access Procedure, Balanced (LAPB), Switched Multimegabit Data Service (SMDS), and X.25. |
| <i>Cisco IOS Wireless LAN Configuration Guide</i> <i>Cisco IOS Wireless LAN Command Reference</i> | Broadcast key rotation, IEEE 802.11x support, IEEE 802.1x authenticator, IEEE 802.1x local authentication service for Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), Multiple Basic Service Set ID (BSSID), Wi-Fi Multimedia (WMM) required elements, and Wi-Fi Protected Access (WPA). |

Table 2 Cisco IOS Supplementary Documents and Resources

| Document Title | Description |
|--|--|
| <i>Cisco IOS Master Command List, All Releases</i> | Alphabetical list of all the commands documented in all Cisco IOS releases. |
| <i>Cisco IOS New, Modified, Removed, and Replaced Commands</i> | List of all the new, modified, removed, and replaced commands for a Cisco IOS release. |
| <i>Cisco IOS Software System Messages</i> | List of Cisco IOS system messages and descriptions. System messages may indicate problems with your system; be informational only; or may help diagnose problems with communications lines, internal hardware, or the system software. |
| <i>Cisco IOS Debug Command Reference</i> | 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 at the following URL: http://www.cisco.com/go/mibs |
| 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 published monthly and describes all new and revised Cisco technical documentation. The *What's New in Cisco Product Documentation* publication also provides information about obtaining the following resources:

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

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

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Using the Command-Line Interface in Cisco IOS and Cisco IOS XE Software

Last Updated: March 5, 2009

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

- [Initially Configuring a Device, page i](#)
- [Using the CLI, page ii](#)
- [Saving Changes to a Configuration, page xii](#)
- [Additional Information, page xii](#)

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 and Cisco IOS XE 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 Support area of Cisco.com at <http://www.cisco.com/web/psa/products/index.html>.

After you have performed the initial configuration and connected the device to your network, you can configure the device 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 ASR1000 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, page ii](#)
- [Using the Interactive Help Feature, page v](#)
- [Understanding Command Syntax, page vi](#)
- [Understanding Enable and Enable Secret Passwords, page viii](#)
- [Using the Command History Feature, page viii](#)
- [Abbreviating Commands, page ix](#)
- [Using Aliases for CLI Commands, page ix](#)
- [Using the no and default Forms of Commands, page x](#)
- [Using the debug Command, page x](#)
- [Filtering Output Using Output Modifiers, page x](#)
- [Understanding CLI Error Messages, page xi](#)

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 1](#) lists common command modes with associated CLI prompts, access and exit methods, and a brief description of how each mode is used.

Table 1 CLI Command Modes

| Command Mode | Access Method | Prompt | Exit Method | Mode Usage |
|-------------------------|---|----------------------|---|---|
| User EXEC | Log in. | Router> | Issue the logout or exit command. | <ul style="list-style-type: none"> • 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. | <ul style="list-style-type: none"> • 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 1 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. | <ul style="list-style-type: none"> 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 the Cisco ASR1000 series router) | <p>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.</p> <ul style="list-style-type: none"> 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)# | <p>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.</p> <p>If the router is in diagnostic mode because of a transport-map configuration, access the router through another port or using a method that is configured to connect to the Cisco IOS CLI.</p> <p>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.</p> | <ul style="list-style-type: none"> 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 possibly 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 2](#) describes how to use the Help feature.

Table 2 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. |
| <i>partial command?</i> | Provides a list of commands that begin with the character string (no space between the command and the question mark). |
| <i>partial command</i> <Tab> | Completes a partial command name (no space between the command and <Tab>). |
| <i>command ?</i> | Lists the keywords, arguments, or both associated with the command (space between the command and the question mark). |
| <i>command keyword ?</i> | 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 3](#) describes these conventions.

Table 3 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
Router(config)# snmp-server file-transfer access-group 10 ?
    protocol  protocol options
    <cr>

```

Understanding Enable and Enable Secret Passwords

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

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

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

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



Note

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

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

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

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

Using the Command History Feature

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

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

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

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

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

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

- Press Ctrl-P or the up arrow key—Recalls commands beginning with the most recent command. Repeat the key sequence to recall successively older commands.

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



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

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

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

Abbreviating Commands

Typing a complete command name is not always required for the command to execute. The 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 **vrp** as a keyword in addition to **version**. (Command and keyword examples from Cisco IOS Release 12.4(13)T.)

Using Aliases for CLI Commands

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

Table 4 shows the default command aliases.

Table 4 Default Command Aliases

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

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

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

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

For more information about the **alias** command, see

http://www.cisco.com/en/US/docs/ios/fundamentals/command/reference/cf_book.html.

Using the no and default Forms of Commands

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

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

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

Using the debug Command

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

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



Caution

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

Filtering Output Using Output Modifiers

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

Three output modifiers are available and are described as follows:

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

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

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

```
Router# show interface | include protocol

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

Understanding CLI Error Messages

You may encounter some error messages while using the CLI. [Table 5](#) shows the common CLI error messages.

Table 5 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 following documents:

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

Saving Changes to a Configuration

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

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

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

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

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

Additional Information

- “Using the Cisco IOS Command-Line Interface” section of the *Cisco IOS Configuration Fundamentals Configuration Guide*:
http://www.cisco.com/en/US/docs/ios/fundamentals/configuration/guide/cf_cli-basics.html
or
“Using Cisco IOS XE Software” chapter of the *Cisco ASR 1000 Series Aggregation Services Routers Software Configuration Guide*:
http://www.cisco.com/en/US/docs/routers/asr1000/configuration/guide/chassis/Using_CLI.html
- Cisco Product Support Resources
<http://www.cisco.com/web/psa/products/index.html>
- Support area on Cisco.com (also search for documentation by task or product)
<http://www.cisco.com/en/US/support/index.html>
- 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/cgi-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>

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2008–2009 Cisco Systems, Inc. All rights reserved.



Control Plane Security Overview

This chapter contains the following sections:

- [About This Guide](#)

Preview the topics in this guide.

- [Creating Effective Security Policies](#)

Learn tips and hints for creating a security policy for your organization. *Before* you configure any security features, you should make sure that your security policy is complete and up to date.

- [Identifying Security Risks and Cisco IOS Solutions](#)

Identify common security risks that might be present in your network and find the right Cisco IOS security feature to prevent security breaks.

About This Guide

The *Cisco IOS Security Configuration Guide: Securing the Control Plane* describes how to configure Cisco IOS control plane security features for your Cisco networking devices. These security features can protect your network against degradation or failure and also against data loss or compromise that is caused by intentional attacks or unintended (but damaging) mistakes by well-meaning network users.

This guide is divided into the following parts:

- [Neighbor Router Authentication](#)
- [Control Plane Policing](#)

The following sections briefly describe the security benefits and operation of the features contained in the above parts.

Neighbor Router Authentication

When neighbor authentication is configured on a router, the router authenticates its neighbor router before accepting any route updates from that neighbor. This ensures that a router always receives reliable routing update information from a trusted source.



Control Plane Policing

Control Plane Policing consists of the following features:

- [Control Plane Policing](#)
- [Control Plane Protection](#)
- [Control Plane Logging](#)

Control Plane Policing

The Control Plane Policing feature lets users configure a Quality of Service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Control Plane Protection

The Control Plane Protection feature is an extension of the policing functionality that the existing Control Plane Policing feature provides. The Control Plane Policing feature allows QoS policing of aggregate control plane traffic destined to the route processor. The Control Plane Protection feature extends this policing functionality by allowing finer policing granularity.

Control Plane Protection includes a traffic classifier, which intercepts traffic and classifies it into three control plane categories. It also includes new port filtering and queue thresholding features. Port filtering feature allows policing of packets going to closed or nonlistening TCP/UDP ports, while queue thresholding limits the number of packets for a specified protocol that is allowed in the control-plane IP input queue.

Control Plane Logging

The Control Plane Protection features let you filter and rate-limit the packets that are going to the router's control plane and discard malicious and error packets (or both). The Control Plane Logging feature enables logging of the packets that these features drop or permit. The Control Plane Logging feature provides the logging mechanism that you need to deploy, monitor, and troubleshoot Control Plane Protection features efficiently.

You can turn on logging for some or all packets that the control plane processes, without feature or class restrictions, or you can enable logging for specific Control Plane Protection features such as control plane policing, port filtering, and queue thresholding.

Creating Effective Security Policies

An effective security policy protects your network assets from sabotage and from inappropriate access (intentional or accidental).

You should configure all network security features according to your security policy. If you do not have a security policy, or it is out of date, you should ensure that a policy is created or updated before you decide how to configure security on your Cisco device.

The following sections provide guidelines to help you create an effective security policy:

- [The Nature of Security Policies](#)
- [Two Levels of Security Policies](#)
- [Tips for Developing an Effective Security Policy](#)

The Nature of Security Policies

You should recognize these aspects of security policies:

- Security policies represent tradeoffs. With all security policies, there are tradeoffs between user productivity and security measures that can be restrictive and time consuming. Any security design should provide maximum security with minimum impact on user access and productivity. Some security measures, such as network data encryption, do not restrict access and productivity. On the other hand, cumbersome or unnecessarily redundant verification and authorization systems can frustrate users and even prevent access to critical network resources.
- Security policies should be determined by business needs. A security policy should not determine how a business operates.
- Security policies are living documents. Because organizations are constantly changing, you must update security policies systematically to reflect new business directions, technological changes, and resource allocations.

Two Levels of Security Policies

A security policy has two levels: requirements and implementation.

- At the requirements level, a policy defines how much you must protect your network assets against intrusion or destruction and also estimates the consequences of a security breach. For example, the policy could state that only human resources personnel can access personnel records or that only IS personnel can configure the backbone routers. The policy could also address the consequences of a network outage (because of sabotage) and the consequences of inadvertently making sensitive information public.
- At the implementation level, a policy defines guidelines to implement the requirements-level policy by using specific technology in a predefined way. For example, the implementation-level policy could require that you configure access lists so that only traffic from human resources host computers can access the server containing personnel records.

When creating a policy, you must define security requirements before defining security implementations to avoid merely justifying particular technical solutions that you do not need.

Tips for Developing an Effective Security Policy

To develop an effective security policy, you must consider the recommendations in the following sections:

- [Identifying Your Network Assets to Protect](#)
- [Determining Points of Risk](#)
- [Limiting the Scope of Access](#)
- [Identifying Assumptions](#)
- [Determining the Cost of Security Measures](#)
- [Considering Human Factors](#)
- [Keeping a Limited Number of Secrets](#)
- [Implementing Pervasive and Scalable Security](#)
- [Understanding Typical Network Functions](#)
- [Remembering Physical Security](#)

Identifying Your Network Assets to Protect

The first step in developing a security policy is to understand and identify your network assets, which include the following:

- Networked hosts (such as PCs, which include the hosts' operating systems, applications, and data)
- Networking devices (such as routers)
- Data that travels across the network

You must identify your network's assets and determine how much you must protect each of these assets. For example, one subnetwork of hosts might contain extremely sensitive data that you must protect at all costs, while a different subnetwork of hosts might require only modest protection against security risks, because it is less costly if the subnetwork is compromised.

Determining Points of Risk

You must understand how potential intruders can enter the network or sabotage it. Special areas of consideration are network connections, dialup access points, and misconfigured hosts. Misconfigured hosts, which are frequently overlooked as points of network entry, can be systems that have unprotected login accounts (guest accounts), extensive trust in remote commands (such as rlogin and rsh), unauthorized modems attached to them, and easy-to-break passwords.

Limiting the Scope of Access

You can create multiple barriers within networks so that unlawful entry to one part of the system does not automatically grant entry to the entire infrastructure. Although maintaining high security for the entire network can be prohibitively expensive (in terms of systems and equipment as well as productivity), you can often provide higher security to the more sensitive areas of your network.

Identifying Assumptions

Every security system has underlying assumptions. For example, an organization might assume that its network is not tapped, that intruders are not very knowledgeable or are using standard software, or that a locked room is safe. You must identify, examine, and justify your assumptions, because any hidden assumption is a potential security hole.

Determining the Cost of Security Measures

In general, providing security comes at a cost. You can measure this cost in terms of increased connection times or inconveniences to legitimate users accessing the assets, increased network management requirements, and sometimes actual money spent on equipment or software upgrades.

Some security measures will inevitably inconvenience some sophisticated users. Security can delay work, create expensive administrative and educational overhead, use significant computing resources, and require dedicated hardware.

When you decide which security measures to implement, you must understand their costs and weigh these against potential benefits. If the security costs are out of proportion to the actual dangers, it is a disservice to the organization to implement them.

Considering Human Factors

If security measures interfere with essential uses of the system, users resist these measures and sometimes even circumvent them. Many security procedures fail because their designers do not take this fact into account. For example, because automatically-generated “nonsense” passwords can be difficult to remember, users often write them on the undersides of keyboards. A “secure” door that leads to a system’s only tape drive is sometimes propped open. For convenience, unauthorized modems are often connected to a network to avoid cumbersome dialin security procedures. To ensure compliance with your security measures, users must be able to get their work done as well as understand and accept the need for security.

Any user can compromise system security to some degree. For example, an intruder might learn passwords by simply calling legitimate users on the telephone claiming to be a systems administrator and asking for them. If users understand security issues and understand the reasons for them, they are far less likely to compromise security in this way.

A complete security policy must define such human factors and include corresponding policies.

At a minimum, you must teach users never to release passwords or other secrets over unsecured telephone lines (especially through cordless or cellular telephones) or electronic mail. They should be wary of questions asked by people who call them on the telephone. Some companies do not allow employees to use the network until they have completed a formal network security training program.

Keeping a Limited Number of Secrets

Most security is based on secrets (for example, passwords and encryption keys). But the more secrets there are, the harder it is to keep all of them. Therefore, you should design a security policy that relies on few secrets. An organization’s most important secret is the information that can help someone circumvent its security.

Implementing Pervasive and Scalable Security

You must use a systematic approach to security that includes multiple, overlapping security methods.

Almost any system change can affect security (especially when you create new services). Systems administrators, programmers, and users must consider the security implications of every change.

Understanding the security implications of a change takes practice and requires lateral thinking and a willingness to explore every way that a service could be manipulated. The goal of any security policy is to create an environment that is not susceptible to every minor change.

Understanding Typical Network Functions

You must understand how your network system normally functions, what is expected and unexpected behavior, and how devices are usually used. This kind of awareness helps you detect security problems. Noticing unusual events can help catch intruders before they damage the system. Software auditing tools can help detect, log, and track unusual events. In addition, you should know exactly what software you use to provide auditing trails, and your security system should not assume that all software is bug-free.

Remembering Physical Security

You cannot neglect the physical security of your network devices and hosts. For example, many facilities implement physical security by using security guards, closed-circuit television, cardkey entry systems, or other means to control physical access to network devices and hosts. Physical access to a computer or router usually gives a sophisticated user complete control over that device. Physical access to a network link usually allows a person to tap into that link, jam it, or inject traffic into it. An intruder can often circumvent software security measures when you do not control access to the hardware.

Identifying Security Risks and Cisco IOS Solutions

Cisco IOS software provides a comprehensive set of security features to guard against specific security risks. This section describes a few common security risks that might be present in your network and describes how to use Cisco IOS software to protect against each of these risks:

- [Preventing Unauthorized Access into Networking Devices](#)
- [Preventing Unauthorized Access into Networks](#)
- [Preventing Network Data Interception](#)
- [Preventing Fraudulent Route Updates](#)

Preventing Unauthorized Access into Networking Devices

If someone gains console or terminal access into a networking device (such as a router, switch, or network access server) they could significantly damage your network—perhaps by reconfiguring the device or even by simply viewing the device's configuration information.

You typically want administrators to have access to your networking device, but you do not want other users on your local-area network or those dialing in to the network to have access to the router.

Users can access Cisco networking devices by dialing in from outside the network through an asynchronous port, connecting from outside the network through a serial port, or connecting via a terminal or workstation from within the local network.

To prevent unauthorized access into a networking device, you should configure one or more of the following security features:

- At a minimum, you should configure passwords and privileges at each networking device for all device lines and ports. This is described in the “[Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices](#)” chapter in the *Cisco IOS Security Configuration Guide: Securing User Services*. The networking device stores these passwords. When users attempt to access the device through a particular line or port, they must first enter the password applied to the line or port.
- For an additional layer of security, you can also configure username and password pairs that are stored in a database on the networking device, as described in the “[Configuring Security with Passwords, Privilege Levels, and Login Usernames for CLI Sessions on Networking Devices](#)” chapter in the *Cisco IOS Security Configuration Guide: Securing User Services*. You assign these pairs to lines or interfaces, and they authenticate each user before that user can access the device. If you define privilege levels, you can also assign a specific privilege level (with associated rights and privileges) to each username and password pair.
- If you want to use username and password pairs, but you want to store them centrally instead of locally on each individual networking device, you can store them in a database on a security server. Multiple networking devices can then use the same database to obtain user authentication (and, if needed, authorization) information. Cisco supports a variety of security server protocols, such as RADIUS, TACACS+, and Kerberos. If you decide to use the database on a security server to store login username and password pairs, you must configure your router or access server to support the applicable protocol; in addition, because most supported security protocols must be administered through the AAA security services, you probably need to enable AAA. For more information about security protocols and AAA, refer to the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of the *Cisco IOS Security Configuration Guide: Securing User Services*.



Note Whenever possible, you should use AAA to implement authentication.

- To authorize individual users for specific rights and privileges, you can implement AAA’s authorization feature by using a security protocol such as TACACS+ or RADIUS. For more information about security protocol features and AAA, refer to the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of the *Cisco IOS Security Configuration Guide: Securing User Services*.
- For a backup authentication method, you must configure AAA. AAA lets you specify the main user authentication method (for example, a username-and-password database stored on a TACACS+ server) and then specify backup methods (for example, a locally-stored username-and-password database). The backup method is used if the networking device cannot access the primary method’s database. You can configure up to four sequential backup methods. To configure AAA, refer to the chapters in the “Authentication, Authorization, and Accounting (AAA)” part of the *Cisco IOS Security Configuration Guide: Securing User Services*.



Note If you have not configured backup methods, you will be denied access to the device if the username-and-password database cannot be accessed for any reason.

- To keep an audit trail of user access, you must configure AAA accounting, which is described in the “[Configuring Accounting](#)” chapter of the *Cisco IOS Security Configuration Guide: Securing User Services*.

Preventing Unauthorized Access into Networks

If someone gains unauthorized access to your internal network, they could cause damage in many ways, perhaps by accessing sensitive files from a host, planting a virus, or hindering network performance by flooding your network with illegitimate packets.

Also, someone within your network could try to access another internal network such as an R&D subnetwork that contains sensitive or critical data. That person could intentionally or inadvertently cause damage; for example, they might access confidential files or tie up a time-critical printer.

To prevent unauthorized access through a networking device into a network, you should configure one or both of these security features:

- [Traffic Filtering](#)
- [Authentication](#)

Traffic Filtering

Cisco uses access lists to filter traffic at networking devices. Basic access lists allow only specified traffic through the device; other traffic is simply dropped. You can specify individual hosts or subnets or types of traffic that should be allowed into the network. Basic access lists generally filter traffic based on source and destination addresses and the protocol type of each packet.

Advanced traffic filtering is also available to provide additional filtering capabilities; for example, the Lock-and-Key Security feature requires each user to be authenticated via a username and password before that user's traffic is allowed onto the network.

For descriptions of the Cisco IOS traffic filtering capabilities, refer to the chapters in the “Traffic Filtering, Firewalls, and Virus Detection” part of the *Cisco IOS Security Configuration Guide: Securing the Data Plane*.

Authentication

You can require users to be authenticated before they gain access into a network. When users attempt to access a service or host (such as a web site or file server) within the protected network, they must first enter certain data (such as a username and password) and possibly additional information such as their date of birth or mother's maiden name. After successful authentication (depending on the method of authentication), you assign users specific privileges, which let them access specific network assets. In most cases, this type of authentication is facilitated by CHAP or PAP over a serial PPP connection in conjunction with a specific security protocol such as TACACS+ or RADIUS.

Just as in preventing unauthorized access to specific network devices, you must decide if you want the authentication database to reside locally or on a separate security server. In this case, a local security database is useful if you have very few routers providing network access. A local security database does not require a separate (and costly) security server. A remote, centralized security database is convenient when you have numerous routers providing network access, because it prevents you from having to update each router with new or changed username authentication and authorization information for potentially hundreds of thousands of dialin users. A centralized security database also helps establish consistent remote access policies throughout a corporation.

Cisco IOS software supports a variety of authentication methods. Although AAA is the primary (and recommended) method for access control, Cisco IOS software provides additional features for simple access control that are outside the scope of AAA. For more information, refer to the “[Configuring Authentication](#)” chapter in the *Cisco IOS Security Configuration Guide: Securing User Services*.

Preventing Network Data Interception

When packets travel across a network, they might be read, altered, or “hijacked.” (Hijacking occurs when a hostile party intercepts a network traffic session and poses as one of the session endpoints.)

If the data is traveling across an unsecured network such as the Internet, the data is exposed to a fairly significant risk. Sensitive or confidential data could be exposed, critical data could be modified, and communications could be interrupted if data is altered.

To protect data as it travels across a network, you must configure network data encryption, which is described in the chapters in the “IPsec and IKE” part of the *Cisco IOS Security Configuration Guide: Secure Connectivity*.

IPSec provides the following network security services. These services are optional. In general, local security policy dictates the use of one or more of the following services:

- Data confidentiality—The IPSec sender can encrypt packets before transmitting them across a network.
- Data integrity—The IPSec receiver can authenticate packets sent by the IPSec sender to ensure that no one has altered the data during transmission.
- Data origin authentication—The IPSec receiver can authenticate the source of the IPSec packets sent. This service depends on the data integrity service.
- Anti-replay—The IPSec receiver can detect and reject replayed packets.

Cisco IPSec prevents routed traffic from being examined or tampered with as it travels across a network. This feature encrypts IP packets at a Cisco router, routes them across a network as encrypted information, and decrypts them at the destination Cisco router. Between the two routers, the packets are in encrypted form, and therefore no one can read or alter the packets’ contents. You define what traffic to encrypt between the two routers based on what data is more sensitive or critical.

To protect traffic for protocols other than IP, you can encapsulate those other protocols into IP packets using GRE encapsulation and then encrypt the IP packets.

You do not typically use IPSec for traffic that is routed through networks that are secure. You should consider using IPSec for traffic that is routed across unsecured networks, such as the Internet, if your organization could be damaged if the traffic is examined or tampered with by unauthorized individuals.

Preventing Fraudulent Route Updates

All routing devices determine where to route individual packets by using information stored in route tables. This route table information is created using route updates from neighboring routers.

If a router receives a fraudulent update, the router could be tricked into forwarding traffic to the wrong destination. This could cause sensitive data to be exposed or could cause network communications to be interrupted.

To ensure that route updates are received only from known, trusted neighbor routers, configure neighbor router authentication as described in the “[Neighbor Router Authentication: Overview and Guidelines](#)” chapter in this guide.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step,

Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



Neighbor Router Authentication



Neighbor Router Authentication: Overview and Guidelines

You can prevent your router from receiving fraudulent route updates by configuring neighbor router authentication.

This chapter describes neighbor router authentication as part of a total security plan. It describes what neighbor router authentication is, how it works, and why you should use it to increase your overall network security.

This chapter refers to neighbor router authentication as *neighbor authentication*. Neighbor router authentication is also sometimes called *route authentication*.

In This Chapter

This chapter describes the following topics:

- [About Neighbor Authentication](#)
- [How Neighbor Authentication Works](#)
- [Key Management \(Key Chains\)](#)
- [Finding Neighbor Authentication Configuration Information](#)

About Neighbor Authentication

This section contains the following subsections:

- [Benefits of Neighbor Authentication](#)
- [Protocols That Use Neighbor Authentication](#)
- [When to Configure Neighbor Authentication](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007-2009 Cisco Systems, Inc. All rights reserved.

Benefits of Neighbor Authentication

When configured, neighbor authentication occurs whenever neighbor routers exchange routing updates. This authentication ensures that a router receives reliable routing information from a trusted source.

Without neighbor authentication, unauthorized or deliberately malicious routing updates could compromise the security of your network traffic. A security compromise could occur if an unfriendly party diverts or analyzes that traffic. For example, an unauthorized router could send a fictitious routing update to convince your router to send traffic to an incorrect destination. The unfriendly party could analyze the diverted traffic to learn confidential information about your organization or merely use it to disrupt your organization's ability to communicate effectively using the network.

Neighbor authentication prevents your router from receiving any such fraudulent routing updates.

Protocols That Use Neighbor Authentication

You can configure neighbor authentication for the following routing protocols:

- Border Gateway Protocol (BGP)
- Director Response Protocol (DRP) Server Agent
- Intermediate System-to-Intermediate System (IS-IS)
- IP Enhanced Interior Gateway Routing Protocol (EIGRP)
- Open Shortest Path First (OSPF)
- Routing Information Protocol (RIP) version 2

When to Configure Neighbor Authentication

You should configure any router for neighbor authentication that

- Uses any of the routing protocols previously mentioned.
- Might conceivably receive a false route update.
- Might compromise the network if it were to receive a false route update.
- Has a neighbor that is already configured for neighbor authentication.

How Neighbor Authentication Works

When you configure a router for neighbor authentication, it authenticates the source of each routing update packet that it receives. The sending router and the receiving router accomplish this by exchanging an authenticating key (sometimes called a password) that is known to both routers.

There are two types of neighbor authentication: plain text and Message Digest Algorithm Version 5 (MD5). Both types work the same way, except that MD5 sends a *message digest* instead of the authenticating key itself. MD5 creates a message digest by using the key and a message, but the key itself is not sent, which prevents it from being read during transmission. Plain text authentication sends the authenticating key itself over the wire.

**Note**

You should not use plain text authentication as part of your security strategy. You should use it primarily to avoid accidental changes to the routing infrastructure. You should use MD5 authentication instead.

**Caution**

As with all keys, passwords, and other security secrets, you must closely guard authenticating keys used in neighbor authentication. This is because the security benefits of this feature rely on the confidentiality of authenticating keys. Also, when performing router management tasks via Simple Network Management Protocol (SNMP), do not ignore the risk associated with sending keys using non-encrypted SNMP.

This section includes the following subsections:

- [Plain Text Authentication](#)
- [MD5 Authentication](#)

Plain Text Authentication

Each participating neighbor router must share an authenticating key. You specify this key at each router during configuration. You can specify multiple keys with some protocols (if so, you must identify each by a key number).

In general, when a router sends a routing update, the following authentication sequence occurs:

- Step 1** A router sends a routing update with a key and the corresponding key number to the neighbor router. In protocols that can have only one key, the key number is always zero.
- Step 2** The receiving (neighbor) router checks the received key against the same key stored in its own memory.
- Step 3** If the two keys match, the receiving router accepts the routing update packet. If the two keys do not match, it rejects the routing update packet.

These protocols use plain text authentication:

- DRP Server Agent
- IS-IS
- OSPF
- RIP version 2

MD5 Authentication

MD5 authentication works much like plain text authentication, except that MD5 never sends the key over the wire. Instead, the router uses the MD5 algorithm to produce a message digest of the key (also called a *hash*). The router sends the message digest instead of the key itself, which ensures that no one can eavesdrop on the line and learn keys during transmission.

These protocols use MD5 authentication:

- OSPF
- RIP version 2
- BGP
- IP Enhanced IGRP

Key Management (Key Chains)

You can configure key chains for these IP routing protocols:

- RIP version 2
- IP Enhanced IGRP
- DRP Server Agent

These routing protocols offer the additional function of managing keys by using key chains. When you configure a key chain, you specify a series of keys with lifetimes, and the Cisco IOS software rotates through each of these keys. This decreases the risk that keys will be compromised.

Each key definition within the key chain must specify a time interval for which that key is activated (its *lifetime*). Then, during a key's lifetime, routing update packets are sent with this activated key.

Keys cannot be used during time periods for which they are not activated. Therefore, you should ensure that for a given key chain, key activation times overlap to avoid any period of time during which no key is activated. If a time period occurs during which no key is activated, neighbor authentication cannot occur, and therefore routing updates will fail.

You can specify multiple key chains.

Note that the router needs to know the time to be able to rotate through keys in synchronization with the other participating routers (so that all routers use the same key at the same moment). Refer to the Network Time Protocol (NTP) and calendar commands in the “*Performing Basic System Management*” chapter of the *Cisco IOS Network Management Configuration Guide* for information about configuring time at your router.

Finding Neighbor Authentication Configuration Information

To find complete configuration information for neighbor authentication, refer to the appropriate section and chapter listed in [Table 66](#).

Table 66 Location of Neighbor Authentication Information for Each Supported Protocol

| Protocol | Book | Chapter | Sections |
|------------------|--|--|---|
| BGP | <i>Cisco IOS IP Routing Protocols Configuration Guide</i> | “Configuring BGP Neighbor Session Options” | <ul style="list-style-type: none"> • “TTL Security Check for BGP Neighbor Sessions” • “Configuring the TTL Security Check for BGP Neighbor Sessions” • “Configuring the TTL-Security Check: Example” |
| DRP Server Agent | <i>Cisco IOS Network Management Configuration Guide</i> | “Configuring a DRP Server Agent” | <ul style="list-style-type: none"> • “Authentication Keys and Keychains” |
| IP Enhanced IGRP | <i>Cisco IOS IP Routing Protocols Configuration Guide</i> | “Configuring EIGRP” | <ul style="list-style-type: none"> • “Configuring EIGRP Route Authentication” |
| IS-IS | <i>Cisco IOS IP Routing Protocols Configuration Guide</i> | “Enhancing Security in an IS-IS Network” | <ul style="list-style-type: none"> • “Setting an Authentication Password for each Interface” • “Setting an Area Password for each IS-IS Area” • “Configuring IS-IS Authentication” |
| MPLS LDP | <i>Cisco IOS Multiprotocol Label Switching Configuration Guide</i> | “MPLS Label Distribution Protocol (LDP)” | <ul style="list-style-type: none"> • “Protecting Data Between LDP Peers with MD5 Authentication” |
| OSPF | <i>Cisco IOS IP Routing Protocols Configuration Guide</i> | “Configuring OSPF” | <ul style="list-style-type: none"> • “Configuring OSPF Interface Parameters” • “Configuring OSPF Area Parameters” • “Creating Virtual Links” |
| RIP version 2 | <i>Cisco IOS IP Routing Protocols Configuration Guide</i> | “Configuring Routing Information Protocol” | <ul style="list-style-type: none"> • “Enabling RIP Authentication” |

To find complete configuration information for key chains, refer to the “Managing Authentication Keys” section in the [“Configuring IP Routing Protocol-Independent Features”](#) chapter of the *Cisco IOS IP Routing Protocols Configuration Guide*.

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2007–2009 Cisco Systems, Inc. All rights reserved.



Control Plane Policing



Control Plane Policing

First Published: January 19, 2006
Last Updated: February 27, 2009

The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks. In this way, the control plane (CP) can help maintain packet forwarding and protocol states despite an attack or heavy traffic load on the router or switch.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the [“Feature Information for Control Plane Policing”](#) section on page 20.

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.

Contents

- [Prerequisites for Control Plane Policing, page 2](#)
- [Restrictions for Control Plane Policing, page 2](#)
- [Information About Control Plane Policing, page 4](#)
- [How to Use Control Plane Policing, page 10](#)
- [Configuration Examples for Control Plane Policing, page 16](#)
- [Additional References, page 17](#)
- [Command Reference, page 19](#)
- [Feature Information for Control Plane Policing, page 20](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Prerequisites for Control Plane Policing

The Modular Quality of Service (QoS) Command-Line interface (CLI) (MQC) is used to configure the packet classification and policing functionality of the Control Plane Policing feature.

Before configuring Control Plane Policing (CoPP), you should understand the procedures for using the MQC. For information about the MQC, see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions for Control Plane Policing

Aggregate and Distributed Control Plane Policing

Aggregate policing is supported in Cisco IOS Release 12.0(29)S, Cisco IOS Release 12.2(18)S, Cisco IOS Release 12.3(4)T, and later releases.

Distributed policing is supported only in Cisco IOS Release 12.0(30)S and later Cisco IOS 12.0S releases.

Output Rate-Limiting Support

Output rate-limiting is performed in silent (packet discard) mode. Silent mode enables a router to silently discard packets using policy maps applied to output control plane traffic with the **service-policy output** command. For more information, see the [“Output Rate-Limiting and Silent Mode Operation”](#) section on page 10.

Output rate-limiting (policing) in silent mode is supported only in:

- Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases
- Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases

Output rate-limiting is not supported for distributed control plane services in Cisco IOS 12.0S releases or in Cisco IOS 12.2SX releases.

Output rate-limiting is not supported on the Cisco 7500 series and Cisco 10720 Internet router.

MQC Restrictions

The Control Plane Policing feature requires the MQC to configure packet classification and policing. All restrictions that apply when you use the MQC to configure policing also apply when you configure control plane policing. Only two MQC actions are supported in policy maps—**police** and **drop**.



Note

On the Cisco 10720 Internet router, only the **police** command, not the **drop** command, is supported in policy maps. In addition, in a QoS service policy that is attached to the Cisco 10720 control plane, the **police** command does not support **set** actions as arguments in **conform-action**, **exceed-action**, and **violate-action** parameters.

Features that require Network-Based Application Recognition (NBAR) classification may not work well at the control plane level. The following classification (match) criteria are supported on all platforms:

- Standard and extended IP access lists (ACLs).
- In class-map configuration mode: **match ip dscp**, **match ip precedence**, and **match protocol arp**, and **match protocol pppoe** commands.

**Note**

In the Cisco IOS 12.2SX release, the **match protocol arp** command is not supported.

On the Cisco 10720 Internet router, the following MQC commands are also supported in class-map configuration mode: **match input-interface**, **match mpls experimental**, **match protocol ipv6**, and **match qos-group**. When using these commands for control plane policing on the Cisco 10720 Internet router, note the following restrictions:

- Packet classification using match criteria is not supported for packets that cannot be classified in the Cisco 10720 data path, such as unknown Layer 2 encapsulation and IP options.
- The following IPv6 fields are not supported in packet classification for IPv6 QoS on the Cisco 10720 Internet router and are, therefore, not supported for control plane policing:
 - IPv6 source and destination addresses
 - Layer 2 class of service (CoS)
 - IPv6 routing header flag
 - IPv6 undetermined transport flag
 - IPv6 flow label
 - IP Real-Time transport Protocol (RTP)

**Note**

Packets that are not supported for QoS packet classification on the Cisco 10720 Internet router are not policed in the default traffic class for control plane policing.

CISCO-CLASS-BASED-QOS-MIB Control Plane Support

In Cisco IOS Release 12.3(7)T and later Cisco IOS 12.3T releases, the CISCO-CLASS-BASED-QOS-MIB is extended to manage control plane QoS policies and provide information about the control plane.

Cisco IOS Release 12.2(18)SXD1

In Cisco IOS Release 12.2(18)SXD1 and later releases, Hardware Control Plane Interface for Control Plane Policing has the following restrictions:

- Supported only with Supervisor Engine 720. Not supported with Supervisor Engine 2.
- Does not support CoPP output rate-limiting (policing).
- Does not support the CoPP silent operation mode.
- Cisco IOS Release 12.2(18)SXD1 and later releases automatically install the CoPP service policy on all DFC-equipped switching modules.

For more information about control plane policing in Cisco IOS Release 12.2(18)SXD1 and later releases, see either of these publications:

- For Catalyst 6500 series switches, see the [“Configuring Control Plane Policing \(CoPP\)”](#) module.
- For Cisco 7600 series routers, see the [“Configuring Denial of Service Protection”](#) module.

Information About Control Plane Policing

To configure the Control Plane Policing feature, you should understand the following concepts:

- [Benefits of Control Plane Policing, page 4](#)
- [Terms to Understand, page 4](#)
- [Control Plane Security and Packet QoS Overview, page 6](#)
- [Aggregate Control Plane Services, page 7](#)
- [Distributed Control Plane Services, page 8](#)
- [Usage of Distributed CP Services, page 9](#)
- [Output Rate-Limiting and Silent Mode Operation, page 10](#)

Benefits of Control Plane Policing

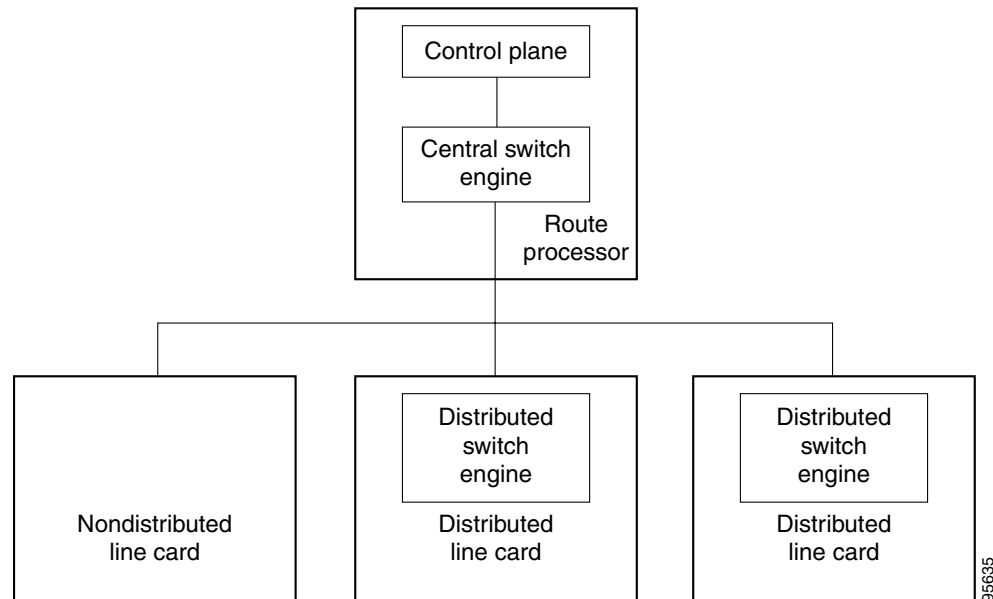
Configuring the Control Plane Policing feature on your Cisco router or switch provides the following benefits:

- Protection against DoS attacks at infrastructure routers and switches
- QoS control for packets that are destined to the control plane of Cisco routers or switches
- Ease of configuration for control plane policies
- Better platform reliability and availability

Terms to Understand

Because different platforms can have different architectures, the following set of terms is defined. [Figure 1](#) illustrates how control plane policing works.

Figure 1 *Layout of Control Plane, Central Switch Engine, Distributed Switch Engines, and Line Cards on a Router*



- Control plane (CP)—A collection of processes that run at the process level on the route processor (RP). These processes collectively provide high-level control for most Cisco IOS functions.
- Central switch engine—A device that is responsible for high-speed routing of IP packets. It also typically performs high-speed input and output services for nondistributed interfaces. (See nondistributed line cards.) The central switch engine is used to implement aggregate CP protection for all interfaces on the router.



Note

All IP packets that are destined for the CP should pass through the central switch engine before they are forwarded to the process level.

On the Cisco 10720 Internet router, control plane policing is implemented on Cisco Parallel eXpress Forwarding (PXF) in a Toaster-based architecture. PXF is a hardware-based central switch engine that can filter traffic at a higher rate than the route processor. PXF switches all data traffic separately from the route processor. PXF packet processing occurs at an intermediate step between the nondistributed line cards and the route processor shown in [Figure 1](#). In addition to the regular punting, PXF also punts certain types of packets (such as unknown Layer 2 encapsulation and packets with IP options) to the RP for further processing at interrupt level.



Note

On the Cisco 10720 Internet router, you can configure enhanced RP protection by using the **ip option drop** command to drop IPv4 packets with IP options that are punted to the RP by PXF. Tunneled IPv4 packets and IPv4 packets with an unsupported encapsulation method are not dropped. For more information, see the “[ACL IP Options Selective Drop](#)” module.

- Distributed switch engine—A device that is responsible for high-speed switching of IP packets on distributed line cards without using resources from the central switch engine. It also typically performs input and output services for the line card. Each distributed switch engine is used to implement distributed CP services for all ports on a line card. Input CP services distribute the processing load across multiple line cards and conserve vital central switch engine resources. Distributed CP services are optional; however, they provide a more refined level of service than aggregate services.
- Nondistributed line cards—Line cards that are responsible for receiving packets and occasionally performing input and output services. All packets must be forwarded to the central switch engine for a routing or switching decision. Aggregate CP services provide coverage for nondistributed line cards.

**Note**

Distributed CP services are supported only in Cisco IOS Release 12.0(30)S and later 12.0S releases.

Control Plane Security and Packet QoS Overview

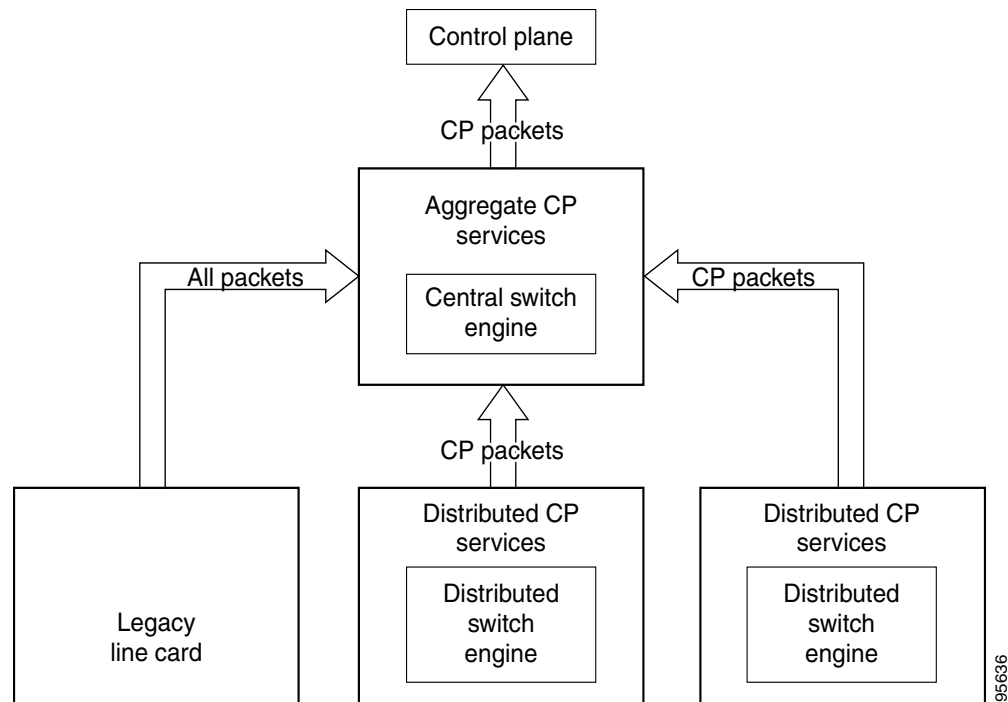
To protect the CP on a router from DoS attacks and to provide packet QoS, the Control Plane Policing feature treats the CP as a separate entity with its own ingress (input) and egress (output) ports, which are like ports on a router and switch. Because the Control Plane Policing feature treats the CP as a separate entity, a set of rules can be established and associated with the ingress and egress ports of the CP.

These rules are applied only after the packet has been determined to have the CP as its destination or when a packet exits the CP. Thereafter, you can configure a service policy to prevent unwanted packets from progressing after a specified rate limit has been reached; for example, a system administrator can limit all TCP/SYN packets that are destined for the CP to a maximum rate of 1 megabit per second.

Input CP services are executed after router input port services have been performed and after a routing decision on the input path has been made. As shown in [Figure 2](#), CP security and packet QoS are applied on:

- An aggregate level by the central switch engine and applied to all CP packets received from all line cards on the router (see the [“Aggregate Control Plane Services”](#) section on page 7).
- A distributed level by the distributed switch engine of a line card and applied to all CP packets received from all interfaces on the line card (see the [“Distributed Control Plane Services”](#) section on page 8).

Figure 2 *Input Control Plane Services: Aggregate and Distributed Services*



The following types of Layer 3 packets are forwarded to the control plane and processed by aggregate and distributed control plane policing:

- Routing protocol control packets
- Packets destined for the local IP address of the router
- Packets from management protocols (such as Simple Network Management Protocol [SNMP], Telnet, and secure shell [SSH])



Note

Ensure that Layer 3 control packets have priority over other packet types that are destined for the control plane.

Aggregate Control Plane Services

Aggregate control plane services provide control plane policing for all CP packets that are received from all line-card interfaces on the router.

The central switch engine executes normal input port services and makes routing decisions for an incoming packet: if the packet is destined for the CP, aggregate services are performed. Because CP traffic from all line cards must pass through aggregate CP services, these services manage the cumulative amount of CP traffic that reaches the CP.

Aggregate CP service steps are as follows:

1. The line card receives a packet and delivers it to the central switch engine.

**Note**

Before the packet is sent to the central switch engine, additional processing may be necessary for platforms that support hardware-level policing or platform-specific aggregate policing. It is possible that the packet may undergo multiple checks before it undergoes the generic Cisco IOS check.

2. The interfaces perform normal (interface-level) input port services and QoS.
3. The central switch engine performs Layer 3 switching or makes a routing decision, determining whether or not the packet is destined for the CP.
4. The central switch engine performs aggregate CP services for all CP packets.
5. On the basis of the results of the aggregate CP services, the central switch engine either drops the packet or delivers the packet to the CP for final processing.

Functionality Highlights of Aggregate CP Services

The following list highlights the functionality of aggregate CP services:

- Aggregate CP services are defined for a single input interface, such as the CP, and represent an aggregate for all ports on a router.
- Modular QoS is used to define CP services. Class maps and policy maps for both DoS protection and packet QoS are defined for a single aggregate CP service policy.
- Modular QoS does not prevent a single bad port from consuming all allocated bandwidth. Class maps that match an interface or subinterface may be able to constrain the contribution of each interface through an interface-specific policy map.

Distributed Control Plane Services

Distributed control plane services provide control plane policing for all CP packets that are received from the interfaces on a line card.

A distributed switch engine executes normal input port services and makes routing decisions for a packet: if the packet is destined for the CP, distributed CP services are performed. Afterwards, CP traffic from each line card is forwarded to the central switch engine where aggregate CP services are applied.

**Note**

Distributed CP services may also forward conditioned packets to the central switch engine. In this case, aggregate CP services are also performed on the conditioned CP traffic.

Distributed CP service steps are as follows:

1. A line card receives a packet and delivers it to the distributed switch engine.
2. The distributed switch engine performs normal (interface-level) input port services and QoS.
3. The distributed switch engine performs Layer 2 or Layer 3 switching or makes a routing decision, determining whether the packet is destined for the CP.
4. The distributed switch engine performs distributed CP services for all CP packets.

5. On the basis of the results of the distributed CP services, the distributed switch engine either drops the packet or marks the packet and delivers it to the central switch engine for further processing.
6. The central switch engine performs aggregate CP services and delivers the packet to the CP for final processing.

Functionality Highlights of Distributed CP Services

The following list highlights the functionality of distributed CP services:

- Distributed CP services are defined for a single input interface, such as the distributed CP, and represent an aggregate for all ports on a line card.
- The MQC is used to define CP services. Class maps and policy maps for both DoS protection and packet QoS are defined for a single distributed CP service policy. Each line card may have a unique CP service policy that applies traffic classifications, QoS policies, and DoS services to packets received from all ports on the line card in an aggregate way.
- The MQC does not prevent one bad port from consuming all allocated bandwidth on a line card. Class maps that match an interface or subinterface may be able to constrain the contribution of each interface through an interface-specific policy map.
- Distributed CP services allow you to limit the number of CP packets forwarded from a line card to the central switch engine. The total number of CP packets received from all line cards on a router may exceed aggregate CP levels.

Usage of Distributed CP Services

The purpose of CP protection and packet QoS is to apply sufficient control to the packets that reach the control plane. To successfully configure this level of CP protection, you must:

- Apply traditional QoS services using the MQC to CP packets.
- Protect the path to the control plane against indiscriminate packet dropping due to resource exhaustion. If packets are not dropped according to user-defined QoS policies, but are dropped due to a resource limitation, the QoS policy is not maintained.

Distributed CP services allow you to configure specific CP services that are enforced at the line-card level and are required for the following reasons:

- While under a DoS attack, line-card resources may be consumed. In this case, you must configure a drop policy to identify important packets. The drop policy ensures that all important packets arrive to the central switch engine for aggregate CP protection and arrive later to the CP. Distributed CP services allow routers to apply the appropriate drop policy when resources are consumed and therefore maintain the desired QoS priorities. If a line card indiscriminately drops packets, the aggregate CP filter becomes ineffective and the QoS priorities are no longer maintained.
- It is not possible to prevent one interface from consuming all aggregate CP resources. A DoS attack on one port may negatively impact CP processing of traffic from other ports. Distributed CP services allow you to limit the amount of important traffic that is forwarded by a line card to the CP. For example, you can configure a layered approach in which the combined rates of all line cards are over-subscribed compared to the aggregate rate. The rate of each individual line card would be below the aggregate rate, but combined together, the rates of all line cards exceed it. This over-subscription model is commonly used for other resource-related functions and helps limit the contribution of CP packets from any one line card.

- Distributed CP services provide for slot-level (line-card) filtering. Customer-facing interfaces may have greater security requirements (with more restrictions or for billing reasons) than network-facing interfaces to backbone devices.
- Because distributed CP protection allows you to configure packet filters on a per-line-card basis, processing cycles on line cards may offload aggregate level processing. You can configure Border Gateway Protocol (BGP) filtering at the distributed level for interfaces that use BGP, allowing the aggregate level to filter packets with the remaining filter requirements. Or you can configure identical filters for distributed and aggregate CP services with a distributed packet marking scheme that informs the aggregate filter that a packet has already been checked. Distributed CP service processing further reduces aggregate processing and can significantly reduce the load on aggregate CP services.

Output Rate-Limiting and Silent Mode Operation

A router is automatically enabled to silently discard packets when you configure output policing on control plane traffic using the **service-policy output *policy-map-name*** command.

Rate-limiting (policing) of output traffic from the CP is performed in silent mode. In silent mode, a router that is running Cisco IOS software operates without sending any system messages. If a packet that is exiting the control plane is discarded for output policing, you do not receive an error message.

When control plane policing is configured for output traffic, error messages are not generated in the following cases:

- Traffic that is being transmitted to a port to which the router is not listening
- A connection to a legitimate address and port that is rejected because of a malformed request

**Note**

The silent mode functionality and output policing on CP traffic are supported only in:

- Cisco IOS Release 12.2(25)S and later Cisco IOS 12.2S releases
- Cisco IOS Release 12.3(4)T and later Cisco IOS 12.3T releases

Silent mode and output policing on CP traffic are not supported for distributed control plane services.

How to Use Control Plane Policing

This section documents the following procedures:

- [Defining Aggregate Control Plane Services, page 11](#) (required)
- [Defining Distributed Control Plane Services, page 12](#) (required)
- [Verifying Aggregate Control Plane Services, page 13](#) (optional)
- [Verifying Distributed Control Plane Services, page 15](#) (optional)

Defining Aggregate Control Plane Services

To configure aggregate CP services, such as packet rate control and silent packet discard, for the active route processor, complete the following steps.

Prerequisites

Before you enter control-plane configuration mode to attach an existing QoS policy to the control plane, you must first create the policy using MQC to define a class map and policy map for control plane traffic.

For information about how to classify traffic and create a QoS policy, see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)

SUMMARY STEPS

- enable**
- configure terminal**
- control-plane**
- service-policy {input | output} *policy-map-name***
- end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | control-plane Example: Router(config)# control-plane | Enters control-plane configuration mode (a prerequisite for Step 4). |

| | Command or Action | Purpose |
|--------|---|---|
| Step 4 | <p>service-policy {input output} <i>policy-map-name</i></p> <p>Example: Router(config-cp)# service-policy input control-plane-policy</p> | <p>Attaches a QoS service policy to the control plane. Note the following points:</p> <ul style="list-style-type: none"> • input—Applies the specified service policy to packets received on the control plane. • output—Applies the specified service policy to packets transmitted from the control plane and enables the router to silently discard packets. • <i>policy-map-name</i>—Name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters. |
| Step 5 | <p>end</p> <p>Example: Router(config-cp)# end</p> | <p>(Optional) Returns to privileged EXEC mode.</p> |

Defining Distributed Control Plane Services

To configure distributed CP services, such as packet rate control, for packets that are destined for the CP and sent from the interfaces on a line card, complete the following steps.

Prerequisites

Before you enter control-plane configuration mode to attach an existing QoS policy for performing distributed control-plane services, you must first create the policy using MQC to define a class map and policy map for control-plane traffic.

For information about how to classify traffic and create a QoS policy, see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control plane interface.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)
- With Cisco IOS 12.2SX releases, the Supervisor Engine 720 automatically installs the service policy on all DFC-equipped switching modules.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane** [**slot** *slot-number*]

4. **service-policy input** *policy-map-name*
5. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | control-plane [slot <i>slot-number</i>] Example: Router(config)# control-plane slot 3 | Enters control-plane configuration mode, which allows you to optionally attach a QoS policy (used to manage CP traffic) to the specified slot. <ul style="list-style-type: none"> • Enter the slot keyword and the slot number, as applicable. |
| Step 4 | service-policy input <i>policy-map-name</i> Example: Router(config-cp)# service-policy input control-plane-policy | Attaches a QoS policy map to filter and manage CP traffic on a specified line card before the aggregate CP policy is applied. Note the following points: <ul style="list-style-type: none"> • input—Applies the specified policy map using the distributed switch engine to CP packets that are received from all interfaces on the line card. • <i>policy-map-name</i>—Name of a service policy map (created using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters. <p>Note The service-policy output <i>policy-map-name</i> command is not supported for applying a QoS policy map for distributed control plane services.</p> |
| Step 5 | end Example: Router(config-cp)# end | (Optional) Returns to privileged EXEC mode. |

Verifying Aggregate Control Plane Services

To display information about the service policy attached to the control plane for aggregate CP services, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map control-plane** [**all**] [**input** [*class class-name*] | **output** [*class class-name*]]

3. exit

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | show policy-map control-plane [all] [input [class <i>class-name</i>] output [class <i>class-name</i>]] Example: Router# show policy-map control-plane all | Displays information about the control plane. Note the following points: <ul style="list-style-type: none"> all—(Optional) Service policy information about all QoS policies used in aggregate and distributed CP services. input—(Optional) Statistics for the attached input policy. output—(Optional) Statistics for the attached output policy. class <i>class-name</i>—(Optional) Name of the traffic class whose configuration and statistics are displayed. |
| Step 3 | exit Example: Router(config-cp)# exit | (Optional) Exits privileged EXEC mode. |

Examples

The following example shows that the policy map TEST is associated with the control plane. This policy map polices traffic that matches the class map TEST, while allowing all other traffic (that matches the class map “class-default”) to go through as is.

```
Router# show policy-map control-plane

Control Plane

Service-policy input:TEST

Class-map:TEST (match-all)
  20 packets, 11280 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:access-group 101
  police:
    8000 bps, 1500 limit, 1500 extended limit
    conformed 15 packets, 6210 bytes; action:transmit
    exceeded 5 packets, 5070 bytes; action:drop
    violated 0 packets, 0 bytes; action:drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map:class-default (match-any)
  105325 packets, 11415151 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any
```

Verifying Distributed Control Plane Services

To display information about the service policy attached to the control plane to perform distributed CP services, complete the following steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map control-plane** [**all** | **slot** *slot-number*] [**input** [**class** *class-name*] | **output** [**class** *class-name*]]
3. **exit**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show policy-map control-plane [all][slot <i>slot-number</i>] [input [class <i>class-name</i>] output [class <i>class-name</i>]] Example: Router# show policy-map control-plane slot 2 | Displays information about the service policy used to apply distributed CP services on the router. Note the following points: <ul style="list-style-type: none"> • all—(Optional) Service policy information about all QoS policies used in aggregate and distributed CP services. • slot <i>slot-number</i>—(Optional) Service policy information about the QoS policy map used to perform distributed CP services on the specified line card. • input—(Optional) Statistics for the attached input policy map. • output—(Optional) Statistics for the attached output policy map. • class <i>class-name</i>—(Optional) Name of the traffic class whose configuration and statistics are displayed. |
| Step 3 | exit Example: Router# exit | (Optional) Exits privileged EXEC mode. |

Examples

The following example shows how to display information about the classes of CP traffic received from all interfaces on the line card in slot 1 to which the policy map TESTII is applied for distributed CP services. This policy map polices traffic that matches the traffic class TESTII, while allowing all other traffic (that matches the class map “class-default”) to go through as is.

```
Router# show policy-map control-plane slot 1
```

```

Control Plane - slot 1

Service-policy input: TESTII (1048)

Class-map: TESTII (match-all) (1049/4)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: protocol arp (1050)
  police:
    cir 8000 bps, bc 4470 bytes, be 4470 bytes
    conformed 0 packets, 0 bytes; actions:
      transmit
    exceeded 0 packets, 0 bytes; actions:
      drop
    violated 0 packets, 0 bytes; actions:
      drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map: class-default (match-any) (1052/0)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any (1053)

```

Configuration Examples for Control Plane Policing

This section contains examples that shows how to configure aggregate control plane services on both an input and an output interface:

- [Configuring Control Plane Policing on Input Telnet Traffic: Example, page 16](#)
- [Configuring Control Plane Policing on Output ICMP Traffic: Example, page 17](#)

Configuring Control Plane Policing on Input Telnet Traffic: Example

The following example shows how to apply a QoS policy for aggregate CP services to Telnet traffic that is received on the control plane. Trusted hosts with source addresses 10.1.1.1 and 10.1.1.2 forward Telnet packets to the control plane without constraint, while allowing all remaining Telnet packets to be policed at the specified rate.

```

! Allow 10.1.1.1 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Router(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate-limit all other Telnet traffic.
Router(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-in
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police 80000 conform transmit exceed drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Define aggregate control plane service for the active route processor.
Router(config)# control-plane
Router(config-cp)# service-policy input control-plane-in
Router(config-cp)# end

```

Example: Configuring Control Plane Policing on Output ICMP Traffic

The following example shows how to apply a QoS policy for aggregate CP services to Telnet traffic transmitted from the control plane. Trusted networks with source addresses 10.0.0.0 and 10.0.0.1 receive Internet Control Management Protocol (ICMP) port-unreachable responses without constraint, while allowing all remaining ICMP port-unreachable responses to be dropped:

```
! Allow 10.0.0.0 trusted network traffic.
Router(config)# access-list 141 deny icmp 10.0.0.0 0.0.0.255 any port-unreachable
! Allow 10.0.0.1 trusted network traffic.
Router(config)# access-list 141 deny icmp 10.0.0.1 0.0.0.255 any port-unreachable
! Rate-limit all other ICMP traffic.
Router(config)# access-list 141 permit icmp any any port-unreachable
Router(config)# class-map icmp-class
Router(config-cmap)# match access-group 141
Router(config-cmap)# exit
Router(config)# policy-map control-plane-out
! Drop all traffic that matches the class "icmp-class."
Router(config-pmap)# class icmp-class
Router(config-pmap-c)# drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
Router(config)# control-plane
! Define aggregate control plane service for the active route processor.
Router(config-cp)# service-policy output control-plane-out
Router(config-cp)# end
```

Additional References

The following sections provide references related to the Control Plane Policing feature.

Related Documents

| Related Topic | Document Title |
|---|---|
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | Cisco IOS Quality of Service Solutions Command Reference |
| QoS features overview | “Quality of Service Overview” module |
| MQC | “Applying QoS Features Using the MQC” module |
| Security features overview | “Control Plane Security Overview” module in the <i>Cisco IOS Security Configuration Guide: Securing the Control Plane</i> |
| Control plane policing in Cisco IOS Release 12.2(18)SXD1 and later releases | For Catalyst 6500 series switches, see the “Configuring Control Plane Policing (CoPP)” module. For Cisco 7600 series routers, see the “Configuring Denial of Service Protection” module. |
| Enhanced RP protection | “ACL IP Options Selective Drop” module |

Standards

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

MIBs

| MIB | MIBs Link |
|--|--|
| <ul style="list-style-type: none"> CISCO-CLASS-BASED-QOS-MIB <p>Note Supported only in Cisco IOS Release 12.3(7)T.</p> | <p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator, found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p> |

RFCs

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

Technical Assistance

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

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html. 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.

- **control-plane**
- **service-policy** (control-plane)
- **show policy-map control-plane**

Feature Information for Control Plane Policing

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS, Catalyst OS, and Cisco IOS XE software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.

**Note**

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 **Feature Information for Control Plane Policing**

| Feature Name | Releases | Feature Information |
|------------------------|--|---|
| Control Plane Policing | 12.2(18)S 12.3(4)T 12.3(7)T 12.0(29)S 12.2(18)SXD1 12.0(30)S 12.2(27)SBC 12.0(32)S 12.3(31)SB2 | <p>The Control Plane Policing feature allows users to configure a quality of service (QoS) filter that manages the traffic flow of control plane packets to protect the control plane of Cisco IOS routers and switches against reconnaissance and denial-of-service (DoS) attacks.</p> <p>For Release 12.2(18)S, this feature was introduced.</p> <p>For Release 12.3(4)T, this feature was integrated into Cisco IOS Release 12.3(4)T, and the output rate-limiting (silent mode operation) feature was added.</p> <p>For Release 12.3(7)T, the CISCO-CLASS-BASED-QOS-MIB was extended to manage control plane QoS policies, and the police rate command was introduced to support traffic policing on the basis of packets per second for control plane traffic.</p> <p>For Release 12.0(29)S, this feature was integrated into Cisco IOS Release 12.0(29)S.</p> <p>For Release 12.2(18)SXD1, this feature was integrated into Cisco IOS Release 12.2(18)SXD1.</p> <p>For Release 12.0(30)S, this feature was modified to include support for distributed control plane services on the Cisco 12000 series Internet router.</p> <p>For Release 12.2(27)SBC, this feature was integrated into Cisco IOS Release 12.2(27)SBC.</p> <p>For Release 12.0(32)S, this feature was modified to include support for aggregate control plane services on the Cisco 10720 Internet router.</p> <p>For Release 12.3(31)SB2, this feature was implemented on the Cisco 10000 series router for the PRE3.</p> |

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2006–2009 Cisco Systems, Inc. All rights reserved.



Control Plane Protection

The Control Plane Protection feature is an extension of the policing functionality provided by the existing Control-Plane Policing feature. The Control-Plane Policing feature allows Quality of Service (QoS) policing of aggregate control-plane traffic destined to the route processor. The Control Plane Protection feature extends this policing functionality by allowing finer policing granularity.

The functionality added with Control Plane Protection includes a traffic classifier, which intercepts traffic and classifies it into three control-plane categories. New port-filtering and queue-thresholding features have also been added. The port-filtering feature provides for policing of packets going to closed or nonlistened TCP/UDP ports, while queue-thresholding limits the number of packets for a specified protocol that will be allowed in the control-plane IP input queue.

History for the Control Plane Protection Feature

| Release | Modification |
|----------|------------------------------|
| 12.4(4)T | This feature was introduced. |

Finding Support Information for Platforms and Cisco IOS Software Images

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

Contents

- [Prerequisites for Control Plane Protection, page 2](#)
- [Restrictions for Control Plane Protection, page 2](#)
- [Information About Control Plane Protection, page 3](#)
- [How to Configure Control Plane Protection, page 6](#)
- [Additional References, page 24](#)
- [Command Reference, page 26](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

Prerequisites for Control Plane Protection

- You understand the principles of Control-Plane Policing and how to classify control-plane traffic.
- You understand the concepts and general configuration procedure (class map and policy map) for applying QoS policies on a router.

For information about control plane policing and its capabilities, see the [“Control Plane Policing”](#) module.

For information about Cisco IOS QoS and the procedure for configuring QoS in your network using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions for Control Plane Protection

Control Plane Protection for IPv4

Control Plane Protection is restricted to IPv4 input path only.

No Support for Direct ACL Configuration

The current release of Control Plane Protection does not support direct access control list (ACL) configuration in the control-plane subinterfaces, but rather can be configured using Modular QoS CLI (MQC) policies.

Requires CEF

Control Plane Protection depends on Cisco Express Forwarding (CEF) for IP packet redirection. If you disable CEF globally, this will remove all active protect and policing policies configured on the control-plane subinterfaces. Aggregate control-plane interface policies will continue to function as normal.

Control-plane Feature Policy Restriction

Policies applicable on the control-plane host subinterface are subject to the following restrictions:

- The port-filter feature policy supports only TCP/UDP-based protocols.
- The queue-thresholding feature policy supports only TCP/UDP-based protocols.

No Support for Distributed or Hardware Switching Platforms

This release does not provide support for distributed or hardware switching platforms.

Control-plane IP Traffic Classification Restrictions

The control-plane host subinterface only supports TCP/UDP-based host traffic. All IP packets entering the control-plane matching any of the following conditions are not classified any further and are redirected to the cef-exception subinterface:

- IP Packets with IP options.
- IP Packets with TTL less than or equal to 1.

Protocols Auto-detected by the Port-filter

Some Cisco IOS TCP/UDP-based services, when configured, may not be auto-detected by the port-filter. That is, they do not get listed under the **show control-plane host open ports** output and they are not classified as an open port. This type of port must be manually added to the active port-filter class-map to be unblocked.

Control-plane Policing Subinterface Restrictions

There are no restrictions on existing aggregate control-plane policing policies. New control-plane policing policies that are configured on host subinterface will not process ARP traffic since ARP traffic is processed at the cef-exception and aggregate interfaces.

Information About Control Plane Protection

To configure the Control-plane Policing feature, you should understand the following concepts:

- [Benefits of Control Plane Protection, page 3](#)
- [Control Plane Protection Architecture, page 3](#)
- [Control-plane Interface and Subinterfaces, page 4](#)

Benefits of Control Plane Protection

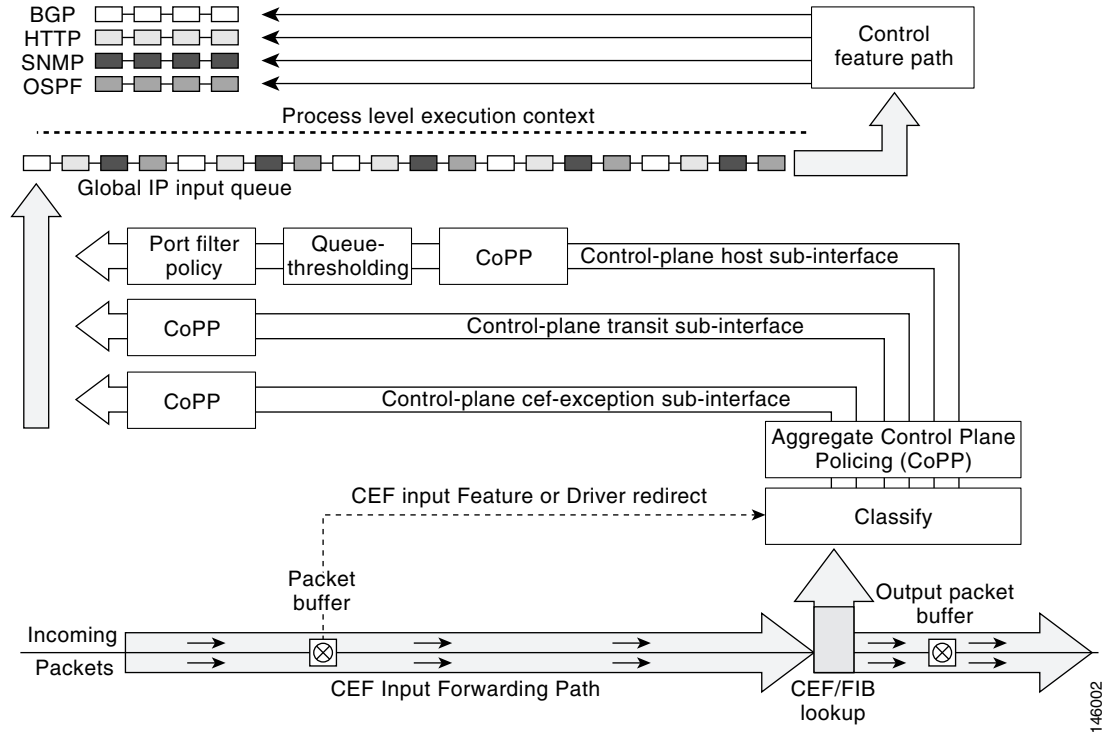
Configuring the Control Plane Protection feature on your Cisco router provides the following benefits:

- Extends protection against DoS attacks at infrastructure routers by providing mechanism for finer policing granularity for control-plane traffic that allows you to rate-limit each type individually.
- Provides a mechanism for early dropping of packets that are directed to closed or nonlistened IOS TCP/UDP ports.
- Provides ability to limit protocol queue usage such that no single protocol flood can overwhelm the input interface.
- Provides QoS control for packets that are destined to the control-plane of Cisco routers.
- Provides ease of configuration for control plane policies using MQC Infrastructure.
- Provides better platform reliability, security and availability.
- Provides dedicated control-plane subinterface for aggregate, host, transit and cef-exception control-plane traffic processing.
- Is highly flexible: permit, deny, rate-limit.
- Provides CPU protection so it can be used for important jobs, such as routing.

Control Plane Protection Architecture

[Figure 1](#) shows control-plane architecture with the Control Plane Protection feature.

Figure 1 Control-plane Architecture with Control Plane Protection



The following sections describe the components of the Control Plane Protections feature.

Control-plane Interface and Subinterfaces

Control Plane Policing (CoPP) introduced the concept of early rate-limiting protocol specific traffic destined to the processor by applying QoS policies to the aggregate control-plane interface. Control Plane Protection extends this control plane functionality by providing three additional control-plane subinterfaces under the top-level (aggregate) control-plane interface. Each subinterface receives and processes a specific type of control-plane traffic. The three subinterfaces are:

- Control-plane host subinterface.** This interface receives all control-plane IP traffic that is directly destined for one of the router interfaces. Examples of control-plane host IP traffic include tunnel termination traffic, management traffic or routing protocols such as SSH, SNMP, BGP, OSPF, and EIGRP. All host traffic terminates on and is processed by the router. Most control plane protection features and policies operate strictly on the control-plane host subinterface. Since most critical router control plane services, such as routing protocols and management traffic, is received on the control-plane host subinterface, it is critical to protect this traffic through policing and protection policies. CoPP, port-filtering and per-protocol queue thresholding protection features can be applied on the control-plane host subinterface.



Note Non-IP based Layer 2 protocol packets such as ARP or CDP do not fall within the control-plane host subinterface. These packets are currently classified in the control-plane CEF-exception subinterface traffic.

- **Control-plane transit subinterface.** This subinterface receives all control-plane IP traffic that is software switched by the route processor. This means packets that are not directly destined to the router itself but rather traffic traversing through the router. Nonterminating tunnels handled by the router is an example of this type of control-plane traffic. Control Plane Protection allows specific aggregate policing of all traffic received at this subinterface.
- **Control-plane CEF-exception subinterface.** This control-plane subinterface receives all traffic that is either redirected as a result of a configured input feature in the CEF packet forwarding path for process switching or directly enqueued in the control plane input queue by the interface driver (i.e. ARP, L2 Keepalives and all non-IP host traffic). Control Plane Protection allows specific aggregate policing of this type of control plane traffic.

QoS policies attached on any of the control-plane interfaces or subinterfaces execute at interrupt level prior to packets being enqueued to the IP input queue and sent to the processor.

The transit and CEF-exception control plane subinterfaces exist in parallel to the control plane host subinterface. This release of Control Plane Protection allows for rate-limiting policies to be configured on these paths as Control Plane Policing extensions. The port-filtering and per-protocol queue thresholding features are not available on these control-plane subinterfaces.

All protection features in the control plane are implemented as MQC policies that operate using the control plane class-maps and policy-maps. New class-map and policy-map types have been created for the control plane port-filter and per-protocol queue-threshold features.

Port-filtering

The control-plane Port-filtering feature enhances control plane protection by providing for early dropping of packets directed toward closed or nonlistened IOS TCP/UDP ports on the router. The port-filter feature policy can be applied only to the control-plane host subinterface.

The port-filter maintains a global database of all open TCP and UDP ports on the router, including random ephemeral ports created by applications. The port database is dynamically populated with entries provided by the registered applications as they start listening on their advertised ports either by configuration of an application (that is SNMP) or initiation of an application (that is, TFTP transfer). An MQC class-map using the list of open ports can be configured and a simple drop policy can be applied to drop all packets destined to closed or nonlistened ports. Port-filter class-maps also support direct match of any user configured TCP/UDP port numbers.

Queue-thresholding

Control-plane protocol Queue-thresholding feature provides a mechanism for limiting the number of unprocessed packets a protocol can have at process-level. This feature can only be applied to the control-plane host subinterface. The intent of this feature is to prevent the input queue from being overwhelmed by any single protocol traffic. Per-protocol thresholding follows a protocol charge model. Each protocol's queue usage is limited such that no single mis-behaving protocol process can jam the interface hold queue. In this release, only a subset of TCP/UDP protocols can be configured for thresholding. Non-IP and Layer 2 protocols such as ARP and CDP cannot be configured. You can set queue limits for the following protocols:

- bgp—Border Gateway Protocol
- dns—Domain Name Server lookup
- ftp—File Transfer Protocol
- http—World Wide Web traffic
- igmp— Internet Group Management Protocol

- snmp—Simple Network Management Protocol
- ssh—Secure Shell Protocol
- syslog—Syslog Server
- telnet—Telnet
- tftp—Trivial File Transfer Protocol
- host-protocols—A wild card for all TCP/UDP protocol ports open on the router not specifically matched/configured

Aggregate Control-plane Services

Control-plane Policing is an existing Cisco IOS feature that allows QoS policing of aggregate control-plane traffic destined to the route processor. The Control Plane Protection feature enhances protection for the router's control-plane by providing finer granularity of policing of traffic destined to the router's processor entering through any of the three control-plane subinterfaces. The CoPP feature is intended to be the first Control Plane Protection feature encountered by packets before any other features/policies. Existing (aggregate) Control-plane Policing policies will not be affected when the Control Plane Protection functionality is enabled. The aggregate Control-plane Policing policy will be applied on all control-plane traffic types. However, Control Plane Protection allows for additional and/or separate Control-plane Policing policies to be configured and applied on the different types of control-plane subinterfaces (host, transit, CEF-exception).

How to Configure Control Plane Protection

The CLI for control-plane (introduced with the Control Plane Policing feature) has been extended to allow for CoPP policies to be applied to individual control-plane subinterfaces (host, transit, CEF-exception). The command syntax for creating CoPP Service Policies remains the same. In addition, the MQC class-map and policy-map CLI was modified to allow for additional types. The port-filter and queue-threshold policy features available in the host subinterface uses these new class-map and policy-map "types".

CoPP leverages MQC to define traffic classification criteria and to specify configurable policy actions for the classified traffic. Traffic of interest must first be identified via class-maps, which are used to define packets for a particular traffic class. Once classified, enforceable policy actions for the identified traffic are created with policy-maps. The **control-plane** global command allows the control-plane service policies to be attached to the aggregate control-plane interface itself.

The CLI for configuring Control-plane Policing policies on the new control-plane subinterfaces remains basically the same as the CLI introduced for Control-plane Policing. The only difference is in how you apply or attach the CoPP policy to the different control-plane subinterfaces.

- [Defining Packet Classification Criteria for CoPP, page 7](#) (required)
- [Defining a CoPP Service Policy, page 8](#) (required)
- [Entering Control Plane Configuration Mode, page 9](#) (required)
- [Applying CoPP Service Policy, page 10](#) (required)
- [Configuring Port-filter Policy, page 12](#) (optional)
- [Configuring Queue-threshold Policy, page 17](#) (optional)
- [Verifying Control Plane Protection, page 22](#) (optional)

Defining Packet Classification Criteria for CoPP

Perform this task to define the packet classification criteria for CoPP.

Prerequisites

Before you attach an existing QoS policy to the control-plane subinterface, you must first create the policy using the MQC to define a class map and policy map for control-plane traffic.

For information about how to classify traffic and create a QoS policy, see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions

- The Control-plane Policing feature requires the MQC to configure packet classification and policing. Thus, restrictions that apply to MQC also apply to control-plane policing.
- Only the following classification (match) criteria are supported: standard and extended IP access lists (named or numbered) and the **match ip dscp** command, the **match ip precedence** command, and the **match protocol arp** command.
- The control-plane policing CLI does not support “type” extensions available with other protection features. This is to preserve backward-compatibility.

SUMMARY STEPS

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

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|--------|---|--|
| Step 3 | <pre>class-map [match-any match-all] class-map-name</pre> <p>Example: Router(config)# class-map match-any control-plane-class </p> | <p>Enables class map global configuration <i>command mode</i> used to create a traffic class.</p> <ul style="list-style-type: none"> match-any—Specifies that one of the match criterion must be met for traffic entering the traffic class to be classified as part of the traffic class. match-all—Specifies that all match criterion must be met for traffic entering the traffic class to be classified as part of the traffic class. <i>class-map-name</i>—Specifies the user-defined name of the traffic class. Names can be a maximum of 40 alphanumeric characters. |
| Step 4 | <pre>match {access-group name access-group-name}</pre> <p>Example: Router(config-cmap)# match access-group name cpp-igp-acl </p> | <p>Specifies the match criteria for the class-map.</p> |

Defining a CoPP Service Policy

To define a service policy, use the **policy-map** global configuration command to specify the service policy name, and use the configuration commands to associate a traffic class that was configured with the **class-map** command, with the QoS action. The traffic class is associated with the service policy when the **class** command is used. You must issue the **class** command after entering policy-map configuration mode. After entering the **class** command, you are automatically in policy-map class configuration mode.

For information about how to classify traffic and create a QoS policy, see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control-plane interface.
- The Control-plane Policing feature requires the modular QoS command-line interface (CLI) (MQC) to configure packet classification and policing. Thus, restrictions that apply to MQC also apply to control-plane policing. Also, only two MQC actions are supported in policy maps - police and drop.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases, and only on the aggregate control-plane interface. Only input policing is available on the new control-plane host, transit and CEF-exception subinterfaces. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)

SUMMARY STEPS

- enable**
- configure terminal**
- policy-map** *policy-map-name*

4. **class** *class-name*
5. **police** rate [*burst-normal*] [*burst-max*] conform-action *action* exceed-action *action* [violate-action *action*]

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | policy-map <i>policy-map-name</i> Example: Router(config)# policy-map control-plane-policy | Enters policy map configuration mode to define a policy. <ul style="list-style-type: none"> • <i>policy-map-name</i>—Name of a service policy map. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | class <i>class-name</i> Example: Router(config-pmap)# class control-plane-class | Enters class map configuration mode, which is used to associate a service policy with a class. <ul style="list-style-type: none"> • <i>class-name</i> —Name of a service policy class. The name can be a maximum of 40 alphanumeric characters. |
| Step 5 | police rate [<i>burst-normal</i>] [<i>burst-max</i>] conform-action <i>action</i> exceed-action <i>action</i> [violate-action <i>action</i>] Example: Router(config-pmap-c)# police rate 50000 pps conform-action transmit exceed-action drop | To configure traffic policing, use the police command in policy-map class configuration mode or policy-map class police configuration mode. <ul style="list-style-type: none"> • rate—Specifies the police rate. If the police rate is specified in pps, the valid value range is 1 to 2000000. If the police rate is specified in bps, the valid range of values is 8000 to 10000000000. • pps—(Optional) Packets per second (pps) will be used to determine the rate at which traffic is policed. • conform-action action—Action to take on packets that conform to the rate limit. • exceed-action action—Action to take on packets that exceed the rate limit. |

Entering Control Plane Configuration Mode

After you have created a class of traffic and defined the service policy for the control-plane, apply the policy to either the aggregate control-plane interface or one of the subinterfaces.

Restrictions

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control-plane interface.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases, and only on the aggregate control-plane interface. Only input policing is available on the new control-plane host, transit and CEF-exception subinterfaces. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane [host |transit | cef-exception]**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | control-plane [host transit cef-exception] Example: Router(config)# control-plane | Enters control-plane configuration mode to attach a QoS policy that manages CP traffic to specified control-plane subinterface: <ul style="list-style-type: none"> • host—enters control-plane host subinterface configuration mode. • transit—enters control-plane transit subinterface configuration mode. • cef-exception—enters control-plane cef-exception subinterface configuration mode. |

Applying CoPP Service Policy

Perform this task to apply CoPP service policies to a control-plane interface.

Prerequisites

Before you attach an existing QoS policy to the control-plane, you must first create the policy by using MQC to define a class map and policy map for control-plane traffic.

For information about how to classify traffic and create a QoS policy, see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions

- Platform-specific restrictions, if any, are checked when the service policy is applied to the control-plane interface.
- Support for output policing is available only in Cisco IOS Release 12.3(4)T and later T-train releases, and only on the aggregate control-plane interface. Only input policing is available on the new control-plane host, transit and CEF-exception subinterfaces. (Note that output policing does not provide any performance benefits. It simply controls the information that is leaving the device.)

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane [host | transit | cef-exception]**
4. **service-policy {input | output} *policy-map-name***

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|--------|---|---|
| Step 3 | <p><code>control-plane [host transit cef-exception]</code></p> <p>Example: <pre>Router(config)# control-plane host</pre></p> | <p>Attaches a QoS policy that manages CP traffic to a specified subinterface, and enters the control-plane configuration mode.</p> <ul style="list-style-type: none"> • host—applies policies to host control-plane traffic • transit— applies policies to transit control-plane traffic • cef-exception—applies policies to CEF-exception control-plane traffic |
| Step 4 | <p><code>service-policy {input output} policy-map-name</code></p> <p>Example: <pre>Router(config-cp)# service-policy input control-plane-policy</pre></p> | <p>Attaches a QoS service policy to the control-plane.</p> <ul style="list-style-type: none"> • input—Applies the specified service policy to packets received on the control-plane. • output—Applies the specified service policy to packets transmitted from the control-plane and enables the router to silently discard packets. • <i>policy-map-name</i>—Name of a service policy map (created by using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters. |

Configuring Port-filter Policy

You can apply the port-filter policy feature to the control-plane host subinterface to block traffic destined to closed or nonlistened TCP/UDP ports. New class-map and service-policy types have been created to accommodate the port-filter configuration. The classification and match criteria for the new port-filter class-maps supports only a constrained subset of the overall global MQC match criteria. Also, the actions supported by the new port-filter service policy is limited as well. that is only the drop action is supported

Restrictions

- The classification and match criteria for the new port-filter class-maps support only a constrained subset of the overall global MQC match criteria.
- The actions supported by the new port-filter service policy is limited. Only the drop action is supported.
- The port-filter feature policy can only be attached on the control-plane host subinterface.
- Some IOS TCP/UDP-based services, when configured, may not be auto-detected by the port filter. That is, they do not get listed under the "show control plane host open ports" output and are not classified as an open port. This type of port must be manually added to the active port filter class-map to be unblocked when using the 'closed-port' match criteria.

There are three required steps to configure a port-filter policy:

- [Defining Port-filter Packet Classification Criteria, page 13](#)
- [Defining Port-filter Service Policy, page 14](#)
- [Applying Port-filter Service Policy to the Host Subinterface, page 15.](#)

Defining Port-filter Packet Classification Criteria

Before you can attach a port-filter service policy to the control-plane host subinterface, you must first create the policy using the modified MQC to define a port-filter class-map and policy-map type for control-plane traffic.

A new MQC class-map type called *port-filter* was created for the port-filter feature. You must first create one or more port-filter class-map(s) before you can create your port-filter service policy. Your port-filter class-maps will separate your traffic into “classes” of traffic in which your service policy will define actions on.

Restrictions

- The classification and match criteria for the new port-filter class-maps supports only a constrained subset of the overall global MQC match criteria. That is, only a subset of match protocol criteria is supported.
- Some IOS TCP/UDP-based services, when configured, may not be auto-detected by the port filter. That is, they do not get listed under the "show control plane host open ports" output and are not classified as an open port. This type of port must be manually added to the active port filter class-map to be unblocked when using the 'closed-port' match criteria.

SUMMARY STEPS

1. **enable**
2. **class-map type port-filter [match-all | match-any] *class-name***
3. **match {closed-ports | not | ports}**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | <pre>enable</pre> <p>Example: Router> enable</p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <pre>class-map type port-filter [match-all match-any] class name</pre> <p>Example: Router(config)# class-map type port-filter match-all pf-class</p> | <p>Creates a class map used to match packets to a specified class and enables the port-filter class-map configuration mode.</p> <ul style="list-style-type: none"> match-all—performs a logical AND on the match criteria match-any—performs a logical OR on the match criteria class-name—Name of a service policy class. The name can be a maximum of 40 alphanumeric characters. |
| Step 3 | <pre>match {closed-ports not port} {TCP UDP} 0-65535</pre> <p>Example: Router(config-cmap)# match closed-ports</p> | <p>Specifies the TCP/UDP match criteria for the class-map</p> <ul style="list-style-type: none"> Closed-ports—matches automatically on all closed-ports on the router Port—allows you to manually specify a TCP/UDP port to match on. TCP—specifies a TCP port to match on UDP—specifies an UDP port to match on |

Defining Port-filter Service Policy

You can define a port-filter service policy that provides additional control-plane protection. Defining this policy supports early dropping of packets that are directed toward closed on nonlistened TCP/UDP ports on the router.

To configure a Port-filter service policy, use the new policy-map type port-filter global configuration command to specify the port-filter service policy name, and use the following configuration commands to associate a port-filter traffic class that was configured with the class-map type port-filter command, with the port-filter drop action command. The port-filter traffic class is associated with the service policy when the class command is used. The class command must be issued after entering policy-map configuration mode. After entering the class command, you are automatically in policy-map class configuration mode.

Restrictions

The actions supported by the new port-filter service policy is limited. Only the drop action is supported.

SUMMARY STEPS

- enable
- configure terminal

3. **policy-map type port-filter** *policy-map-name*
4. **class** *class-name*
5. **drop**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | policy-map type port-filter <i>policy-map-name</i> Example: Router(config- pcmap)# policy-map type port-filter cpr-pf-policy | Creates the port-filter service policy and enters the policy-map configuration mode. <ul style="list-style-type: none"> • <i>policy-map-name</i>—Name of a service policy map. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | class <i>class name</i> Example: Router (config-cmap)# class <i>pf-class</i> | Associates a service policy with a class and enters class map configuration mode. <ul style="list-style-type: none"> • <i>class-name</i>—Name of a service policy class. The name can be a maximum of 40 alphanumeric characters. |
| Step 5 | drop Example: Router (config-cmap)# drop | Applies the port-filter service policy action on the class. |

Applying Port-filter Service Policy to the Host Subinterface

Perform this task to apply port-filter service policies to a subinterface.

Prerequisites

Before you attach a port-filter service policy to the control-plane host subinterface, you must first create the policy using MQC to define a class map and policy map for the required control-plane traffic.

Restrictions

The port-filter feature can only be applied on the control-plane host subinterface and only as input policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane [host | transit | cef-exception]]**
4. **service-policy type port-filter {input} *port-filter-policy-map-name***

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters the global configuration mode. |
| Step 3 | control-plane [host transit cef-exception] Example: Router(config)# control-plane host | Attaches a QoS policy that manages traffic to the control-plane host subinterface and enters the control-plane configuration mode. Note Port-filter can only be applied to the host subinterface. <ul style="list-style-type: none"> • host—enters the control-plane host subinterface configuration mode |
| Step 4 | service-policy type port-filter {input} <i>port-filter-policy-map-name</i> Example: Router(config-cp)# service-policy input <i>cpr-pf-policy</i> | Attaches a QoS service policy to the control-plane host subinterface. <ul style="list-style-type: none"> • input—Applies the specified service policy to packets received on the control-plane. • port-filter-policy-map-name—Name of a port-filter service policy map (created using the policy-map type port-filter command) to be attached. The name can be a maximum of 40 alphanumeric characters. |

Examples

The following example shows how to configure a port-filter policy to drop all traffic destined to closed or “nonlistened” TCP/UDP ports:

```
Router(config)# class-map type port-filter pf-class
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
Router#
```

The following example shows how to configure a port-filter policy to drop all traffic destined to closed or “nonlistening” ports except NTP.

```
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
Router#
```

Configuring Queue-threshold Policy

The Control Plane Protection feature includes a new queue-threshold policy feature that can be applied to the control-plane host subinterface. The queue-threshold feature allows you to limit the number of packets for a given higher level protocol allowed in the control-plane IP input queue. Much like the port-filter feature, new class-map and policy-map types have been created to accommodate the queue-threshold feature. As with the port-filter feature, the queue-threshold feature supports a very specific class-map and policy-map capabilities.

Restrictions

- The classification and match criteria for the new queue-threshold class-maps supports only a constrained subset of the overall global MQC match criteria. That is, only a subset of match protocol option.
- The actions supported by the new queue-threshold service policy is limited. Only the queue-limit action is supported.
- The queue-threshold feature is supported only on the control-plane host subinterface as an input policy.

There are three steps required to configure a Queue-threshold policy:

- [Defining Queue-threshold Packet Classification Criteria, page 17](#)
- [Defining a Queue-threshold Service Policy, page 19](#)
- [Applying a Queue-threshold policy to the Host Subinterface, page 20](#)

Defining Queue-threshold Packet Classification Criteria

You can define a queue-threshold service policy when you want to limit the number of unprocessed packets that a protocol can have at process level.

Before you can attach a queue-threshold service policy to the control-plane host subinterface, you must first create the policy using the modified MQC to define a queue-threshold class-map and policy-map type for control-plane traffic.

A new MQC class-map type called *queue-threshold* was created for the queue-threshold feature. You must first create one or more queue-threshold class-map(s) before you can create your queue-threshold service policy. Your queue-threshold class-maps will separate your traffic into “classes” of traffic in which your service policy will define actions on.

Restrictions

The classification and match criteria for the new queue-threshold class-map supports only a constrained subset of the overall global MQC match criteria. That is, only a subset of the match protocol criteria is supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map type *queue-threshold* [match-all | match-any] class name**
4. **match protocol [bgp | dns | ftp | http | igmp | snmp | ssh | syslog | telnet | tftp] [cr]**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters the global configuration mode. |

| | Command or Action | Purpose |
|--------|---|--|
| Step 3 | <pre>class-map type queue-threshold [match-all match-any] class name</pre> <p>Example: Router(config)#class-map type queue-threshold match-all cppr-pf</p> | <p>Applies a class map for the queue-threshold and enables the queue-threshold class-map configuration mode.</p> <ul style="list-style-type: none"> • match-all—performs a logical AND on the match criteria • match-any—performs a logical OR on the match criteria • <i>class-name</i>—Name of a service policy class. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | <pre>match protocol [bgp dns ftp http igmp snmp ssh syslog telnet tftp host-protocols]</pre> <p>Example: Router(config-cmap)# match protocol bgp</p> | <p>Specifies the upper layer protocol match criteria for the class-map.</p> <ul style="list-style-type: none"> • bgp—Border Gateway Protocol • dns—Domain Name Server lookup • ftp—File Transfer Protocol • http—World Wide Web traffic • igmp—Internet Group Management Protocol • snmp—Simple Network Management Protocol • ssh—Secure Shell Protocol • syslog—Syslog Server • telnet—Telnet • tftp—Trivial File Transfer Protocol • host-protocols—any open TCP/UDP port on the router. |

Defining a Queue-threshold Service Policy

To configure a queue-threshold service policy, use the new policy-map type called queue-threshold global configuration command to specify the queue-threshold service policy name, and use the following configuration commands to associate a queue-threshold traffic class that was configured with the class-map type queue-threshold command, with the queue-threshold queue-limit action command. The queue-threshold traffic class is associated with the service policy when the class command is used. The class command must be issued after entering policy-map configuration mode. After entering the class command, you are automatically in policy-map class configuration mode.

Restrictions

The actions supported by the new queue-threshold service policy is limited. Only the queue-limit action is supported.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **policy-map type queue-threshold** *policy-name*
4. **class** *class name*
5. **queue-limit** *number*

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|---|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters the global configuration mode. |
| Step 3 | policy-map type queue-threshold <i>policy name</i> Example: Router(config)# policy-map type queue-threshold <i>cppr-qt-policy</i> | Enables the queue-threshold service policy configuration mode. <ul style="list-style-type: none"> • <i>policy-name</i>—Name of a service policy map. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | class <i>class name</i> Example: Router(config-pcmap)# class qt-class | Enters class map configuration mode used to associate a service policy with a class. <ul style="list-style-type: none"> • <i>class-name</i>—Name of a service policy class. The name can be a maximum of 40 alphanumeric characters. |
| Step 5 | queue-limit <i>number</i> Example: Router(config-cmap) #queue-limit 75 | Applies the queue-threshold service policy action on the class. Note Queue limit range is 0 to 255. |

Applying a Queue-threshold policy to the Host Subinterface

Perform this task to apply queue-threshold service policies to the control-plane host subinterface.

Prerequisites

Before you attach a queue-threshold service policy to the control-plane host subinterface, you must first create the policy by using MQC to define a class map and policy map for the required control-plane traffic.

Restrictions

The queue-threshold feature can only be applied on the control-plane host subinterface as an input policy.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane [host | transit | cef-exception]**
4. **service-policy type queue-threshold {input} *queue-threshold-policy-map-name***

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters the global configuration mode. |
| Step 3 | control-plane [host transit cef-exception] Example: Router(config)# control-plane host | Attaches a QoS queue-threshold policy that manages traffic to the host subinterface and enters control-plane configuration mode. Note queue-threshold can only be applied to the host subinterface. <ul style="list-style-type: none"> • host—Enters the control-plane host subinterface configuration mode. |
| Step 4 | service-policy type queue-threshold {input} <i>queue-threshold-policy-map-name</i> Example: Router(config-cp)# service-policy input <i>cpr-qt-policy</i> | Attaches a QoS service policy to the control-plane. <ul style="list-style-type: none"> • input—Applies the specified service policy to packets received on the control-plane. • <i>queue-threshold-policy-map-name</i> —Name of a queue-threshold service policy map (created using the policy-map type queue-threshold command) to be attached. The name can be a maximum of 40 alphanumeric characters. |

Examples

The following example shows how to configure a queue-threshold policy to set the queue limit for SNMP protocol traffic to 50, telnet traffic to 50, and all other protocols to 150.

```
Router(config)# class-map type queue-threshold qt-snmpp-class
Router(config-cmap)# match protocol snmp
Router(config-cmap)# class-map type queue-threshold qt-telnet-class
Router(config-cmap)# match protocol telnet
Router(config-cmap)# class-map type queue-threshold qt-other-class
Router(config-cmap)# match host-protocols
Router(config-cmap)# exit
Router(config)# policy-map type queue-threshold qt-policy
Router(config-pmap)# class qt-snmpp-class
```

```
Router(config-pmap-c)# queue-limit 50
Router(config-pmap-c)# class qt-telnet-class
Router(config-pmap-c)# queue-limit 50
Router(config-pmap-c)# class qt-other-class
Router(config-pmap-c)# queue-limit 150
Router(config-pmap-c)# end
Router#
```

Verifying Control Plane Protection

Use the **show policy-map control-plane command** to verify Control Plane Protection configurations and to view statistics for control-plane service policies.

To display information about the service policy attached to the control-plane, perform the following optional steps.

SUMMARY STEPS

1. **enable**
2. **show policy-map [type *policy-type*] control-plane [pfx | slot *slot number*] [all] [host | transit | cef-exception] [{input | output}] [class *class-name*]**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | show policy-map [<i>type policy-type</i>] control-plane [<i>pxfx</i> <i>slot slot number</i>] [<i>all</i>] [<i>host</i> <i>transit</i> <i>cef-exception</i>] [{ <i>input</i> <i>output</i> }] [<i>class class-name</i>] Example: Router# show policy-map control-plane all | Displays information about the control-plane. <ul style="list-style-type: none"> • policy-type— Specifies policy-map type that you want statistics for (i.e. port-filter or queue-threshold) • pxfx— Does not apply to Control Plane Protection feature. • slot— Does not apply to Control Plane Protection feature • all—Information for all control plane interfaces. • host—Policy-map and class-map statistics for the host path. • transit—Policy-map and class-map statistics for transit path. • cef-exception—Policy-map and class-map statistics for CEF-exception path. • input—Statistics for the attached input policy will be displayed. • output—Statistics for the attached output policy will be displayed. • class class name—Name of class whose configuration and statistics are to be displayed. |

Examples

The following example shows that the aggregate CoPP policy map named “copp-transit-policy” is associated with the control-plane transit subinterface and displays the statistics for that policy:

```
Router# show policy-map control-plane transit
control-plane Transit

Service-policy input: copp-transit-policy

Class-map: copp-transit-class (match-all)
  8 packets, 592 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any
  police:
    rate 2000 pps, burst 488 packets
    conformed 8 packets; actions:
      transmit
    exceeded 0 packets; actions:
      drop
    conformed 0 pps, exceed 0 pps
```

```

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match: any

```

The following example shows that the policy map “TEST” is associated with the aggregate control-plane interface. This policy map polices traffic that matches the class map “TEST,” while allowing all other traffic (that matches the class map “class-default”) to go through as is.

```

Router# show policy-map control-plane

control-plane

Service-policy input:TEST

Class-map:TEST (match-all)
  20 packets, 11280 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:access-group 101
  police:
    8000 bps, 1500 limit, 1500 extended limit
    conformed 15 packets, 6210 bytes; action:transmit
    exceeded 5 packets, 5070 bytes; action:drop
    violated 0 packets, 0 bytes; action:drop
    conformed 0 bps, exceed 0 bps, violate 0 bps

Class-map:class-default (match-any)
  105325 packets, 11415151 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
  Match:any

```

Additional References

The following sections provide references related to Control-Plane Protection.

Related Documents

| Related Topic | Document Title |
|---|--|
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | Cisco IOS Quality of Service Solutions Command Reference |
| QoS feature overview | “Quality of Service Overview” module |

Standards

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

MIBs

| MIB | MIBs Link |
|---|---|
| <ul style="list-style-type: none">CISCO-CLASS-BASED-QOS-MIB Note Supported only in Cisco IOS Release 12.3(7)T. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator, found at the following URL: http://www.cisco.com/go/mibs |

RFCs

| RFC | Title |
|------|-------|
| None | — |

Technical Assistance

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

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **class-map**
- **control-plane**
- **show policy-map control-plane**

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.



Control Plane Logging

First Published: February 27, 2006

Last Updated: February 27, 2006

The Cisco IOS Control Plane Protection features allow you to filter and rate-limit the packets that are going to the router's control plane, and discard malicious and or error packets. The addition of the Control Plane Logging feature enables logging of the packets that are dropped or permitted by these features. You can turn on logging for all or some packets that are processed by the control plane, without feature or class restrictions, or you can enable logging for specific Control Plane Protection features such as control plane policing, port-filtering, and queue-thresholding. The Control Plane Logging feature provides the logging mechanism that is needed to efficiently deploy, monitor, and troubleshoot Control Plane Protection features.

Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To reach links to specific feature documentation in this module and to see a list of the releases in which each feature is supported, use the [Feature Information for Control Plane Logging, page 21](#).

Finding Support Information for Platforms and Cisco IOS and Catalyst OS Software Images

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.

Contents

- [Prerequisites for Control Plane Logging, page 2](#)
- [Restrictions for Control Plane Logging, page 2](#)
- [Information About Control Plane Logging, page 3](#)
- [How to Configure Logging on a Control Plane Interface, page 4](#)
- [Configuration Examples for Control Plane Logging, page 13](#)
- [Additional References, page 18](#)



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

© 2007 Cisco Systems, Inc. All rights reserved.

- [Command Reference, page 20](#)
- [Feature Information for Control Plane Logging, page 21](#)

Prerequisites for Control Plane Logging

- You understand the principles of control plane policing and how to classify control-plane traffic.
- You understand the concepts and general configuration procedures for control plane protection, including control plane policing, port-filtering, and queue-threshold.
- You understand the concepts and general configuration procedure for applying QoS policies on a router (class map and policy map).

For information about control plane policing and its capabilities, see the [“Control Plane Policing”](#) module.

For information about control plane protection and its capabilities, see the [“Control Plane Protection”](#) module.

For information about Cisco IOS QoS and the procedure for configuring QoS in your network using the Modular Quality of Service (QoS) Command-Line Interface (CLI) (MQC), see the [“Applying QoS Features Using the MQC”](#) module.

Restrictions for Control Plane Logging

- The Control Plane Logging feature logs control-plane packets only. This feature does not log data-plane traffic that traverses the router on non-control-plane interfaces.
- The Control Plane Logging feature logs IPv4 packets only. IPv6 packet logging is not supported.
- Control plane logging is supported only on platforms that support control plane protection.
- Packets permitted or dropped by the Management Plane Protection (MPP) feature can be logged only via the Global Control Plane Logging mechanism. Feature-specific or class-specific control plane logging cannot be used to log MPP traffic.
- Global control plane logging can log only dropped or error packets on the aggregate control-plane interface as a result of a control plane policing policy applied to the aggregate interface. To log allowed packets, you must apply the global control-plane logging policy to the host, transit, or cef-exception control-plane subinterface, or you must use feature-specific or class-specific logging.
- A packet that passes through the control plane can be logged only once using this feature. The state printed in the log message (PERMIT or DROP) is the final state of the packet on the control plane. For example, if there is a control-plane protection policy on the aggregate control-plane interface and another on the host control-plane subinterface, with logging enabled on both, a packet that is allowed by both features will be logged only once (with a state of PERMIT). So a state of PERMIT when logged for a packet means that the packet was allowed by all control-plane protection features.
- Although logging control-plane traffic provides valuable insight into the details of control-plane traffic, logging excessive control-plane traffic might result in an overwhelming number of log entries and possibly high router CPU usage. Use control plane logging for short periods of time and only when needed to help classify, monitor, and troubleshoot control-plane traffic and features.

Information About Control Plane Logging

To configure the Control Plane Logging feature, you should understand the following concepts:

- [Global Control Plane Logging, page 3](#)
- [Feature-Specific or Class-Specific Logging, page 3](#)

Global Control Plane Logging

Global Control Plane Logging is a feature that allows logging of all or some packets processed by the control plane, without feature or class restrictions. This can be used to log all, or a subset of, traffic permitted or dropped by the Control Plane Protection Features. Packets to be logged can be filtered based on the basis of multiple match criteria (that is input interface, source IP address, or destination IP address). The list of supported match criteria can be found in the [“How to Configure Logging on a Control Plane Interface”](#) section on page 4.

Logging policies can also log packets on the basis of the action taken on them (that is, dropped or permitted) by control plane features (that is, control plane policing, port-filtering or per-protocol queue-thresholding). Packets that are dropped by the control-plane infrastructure because of checksum errors can also be filtered and logged. If you have not specified the kind of packet to be logged via the “permitted,” “dropped,” or “error” action match criteria, all packets (permitted, dropped, and error) will be considered for logging.

By default, the log messages contain source IP address, destination IP address, protocol name (IP/TCP/UDP), action (permit, drop, error), and port number. Additionally, there are options that can be configured with the log action that can enable logging of other fields in the IP header as well, such as TTL and packet length. There is also an option to configure the rate-limit interval for which log messages are created; that is, the interval between the logging of two messages.

The Global Control Plane Logging feature is configured using new MQC class-map, policy-map, and service-policy types and can be applied on the aggregate control-plane interface or on a specific control-plane subinterface (that is, host, transit, or cef-exception).

Feature-Specific or Class-Specific Logging

Feature-specific or class-specific logging tracks only packets that match a specific class and that are acted upon by a specific control plane protection feature (that is, control plane policing, port-filtering, or per-protocol queue-thresholding). This type of logging differs from global logging, which allows you to log all packets on a control-plane interface. With global logging, traffic that matches individual classes within a control plane protection feature policy cannot be distinguished. Global logging, for example, can log only all packets dropped on a control-plane interface as a whole. However, with feature-specific or class-specific logging, packets that match a specific class and that are acted upon by a specific control plane protection feature will be separated out. Feature-specific or class-specific logging may be most valuable during the initial stages of control plane protection deployment, when there is a need to know details about packets that match a specific class. For example, knowing what traffic is hitting your class-default class would help in modifying your class maps or policy maps to account for stray packets or for determining characteristics of an attack.

Feature-specific or class-specific logging provides feature-specific logging, making it possible to log packets for a specific feature on a specific control-plane interface (for example, port-filtering on the control-plane host interface).

Feature-specific or class-specific logging allows logging of packets that pass through a class map in a control plane protection feature service policy applied to a control-plane interface. When a feature, such as control plane policing, is applied on a control-plane interface, feature-specific or class-specific logging can be added as one of the actions to be performed on a class defined in the feature policy map. When logging is added as an action for a class inside a policy map, all packets that match that class will be logged. The only packets filtered are those that the feature class map supports. There is no further classification done for logging specifically. The **log** action keyword can be added by itself without any other policing actions defined in the class, or it can be added in addition to the police or drop action defined in the class. When the **log** keyword is added as an action for a class inside a policy map, all packets (permitted and/or dropped) that match the class will be logged.

By default, the log messages contain source IP address, destination IP address, protocol name (IP/TCP/UDP), action (permit, drop, error), and port number. Additionally, there are options that can be configured with the log action that can enable logging of other fields in the IP header as well, such as TTL and packet length. There is also an option to configure the rate-limit interval for which log messages are created; that is, the interval between the logging of two messages.

How to Configure Logging on a Control Plane Interface

You can configure control plane logging for global logging and/or for feature-specific or class-specific logging.

- [Configuring Global Logging, page 4](#)
- [Configuring Feature-Specific or Class-Specific Logging, page 9](#)
- [Verification Examples for Control Plane Logging, page 11](#)

Configuring Global Logging

To support global control plane logging, new MQC class-map, policy-map, and service-policy types were created. Policy-map type logging is used only for global control plane logging policies. Class-map type logging is used to classify what type of control-plane traffic you want to log. The logging type class maps support a subset of generic QoS match criteria and some control-plane-specific match criteria. The supported match criteria are as follows:

- input-interface
- IPv4 source IP address
- IPv4 destination IP address
- packets dropped
- packets permitted
- packets error

If one of the packet-action filters, packets dropped, packets permitted, or packets error, is not specified, all matching packets will be logged irrespective of the action taken on them (permitted or dropped).

Also, in a logging type policy map, the only action supported is log. The configuration and behavior of the **log** action keyword are the same in global logging and feature-specific or class-specific logging. The available options for the **log** action keyword are as follows:

- **interval**—Sets packet logging interval.
- **ttl**—Logs ttl for IPv4 packets.
- **total-length**—Logs packet length for IPv4 packets.

The tasks for configuring global logging include the following:

- [Defining Packet Logging Classification Criteria, page 5](#) (required)
- [Defining the Logging Policy Map, page 6](#) (required)
- [Creating a Logging Service Policy on a Control Plane Interface, page 7](#) (required)



Note

Logging policies can be applied to the control plane, control-plane host, control-plane transit, and control-plane cef-exception interfaces.

Defining Packet Logging Classification Criteria

When configuring global logging, you must first define the packet logging classification criteria.

Restrictions

You can apply global logging policies on control plane interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **class-map** [type {stack | access-control | port-filter | queue-threshold | logging}] [match-all | match-any] *class-map-name*
4. **match** [input-interface | ipv4 source-address | ipv4 destination-address | not input-interface | packets permitted | packets dropped | packets error]
5. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|--|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |

| | Command or Action | Purpose |
|--------|---|---|
| Step 3 | <pre>class-map [type {stack access-control port-filter queue-threshold logging}] [match-all match-any] class-map-name</pre> <p>Example: Router(config)# class-map type logging match-all log-class</p> | <p>Creates a class map used to match packets to a specified class and enters class-map configuration mode. The following keywords and arguments can be used for control plane logging:</p> <ul style="list-style-type: none"> • type—(Optional) Identifies the class-map type. Use the logging keyword for control plane logging configurations. • match-all—(Optional) Performs a logical AND on the match criteria. • match-any—(Optional) Performs a logical OR on the match criteria. • <i>class-map name</i>—Name of a class. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | <pre>match [input-interface ipv4 source-address ipv4 destination-address not input-interface packets permitted packets dropped packets error]</pre> <p>Example: Router(config-cmap)# match packets dropped</p> | <p>Defines the match criteria for the logging class map.</p> |
| Step 5 | <pre>end</pre> <p>Example: Router(config-cmap)# end</p> | <p>Exits class-map configuration mode and returns to privileged EXEC mode.</p> |

Defining the Logging Policy Map

After you define packet logging criteria for global logging, you must define the logging policy map.

To configure global logging policy maps, use the new **policy-map type logging** configuration command. Then, use the **class** command, to associate a logging class-map that was configured with the **class-map type logging** command, with the logging policy map. Use the **log** keyword to configure the log action for the class that you associated with the policy map. The **class** command must be issued after entering the policy-map configuration mode. After entering the **class** command, you are automatically in policy-map class configuration mode. The action **log** can be configured while in policy-map class configuration mode.

Restrictions

You can apply global logging policies on control plane interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map [type {stack | access-control | port-filter | queue-threshold | logging}]
policy-map-name**
4. **class class-name**

5. `log [interval seconds | total-length | ttl]`
6. `end`

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | <code>enable</code> Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <code>configure terminal</code> Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | <code>policy-map [type {stack access-control port-filter queue-threshold logging}] policy-map-name</code> Example: Router(config)# policy-map type logging log-policy | Creates the logging service policy and enters policy-map configuration mode. <ul style="list-style-type: none"> type—(Optional) Identifies the policy-map type. Use the logging keyword for control plane logging configurations. policy-map-name—Name of a policy map. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | <code>class class-name</code> Example: Router(config-pmap)# class log-class | Associates a class with a policy map and enters class-map configuration mode. <ul style="list-style-type: none"> class-name—Name of a class of type logging. The name can be a maximum of 40 alphanumeric characters. |
| Step 5 | <code>log [interval <i>seconds</i> total-length ttl]</code> Example: Router(config-pmap-c)# log interval 1000 | Applies the log action to the logging class. With this command, you can enter the following optional parameters: <ul style="list-style-type: none"> interval <i>seconds</i>—(Optional) Sets packet logging interval. total-length—(Optional) Logs packet length for IPv4 packets. ttl—(Optional) Logs ttl for IPv4 packets. |
| Step 6 | <code>end</code> Example: Router(config-pmap-c)# end | Exits from class-map configuration mode and returns to privileged EXEC mode. |

Creating a Logging Service Policy on a Control Plane Interface

After you define the logging service policy, you must apply the policy to a specific control plane interface.

Restrictions

You can apply global logging policies on control plane interfaces only.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **control-plane** [host | transit | cef-exception | cr]
4. **service-policy** type logging input *logging-policy-map-name*
5. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | enable Example: Router> enable | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | configure terminal Example: Router# configure terminal | Enters global configuration mode. |
| Step 3 | control-plane [host transit cef-exception cr] Example: Router(config)# control-plane host | Enters control-plane configuration mode. <ul style="list-style-type: none"> • host—(Optional) Applies policies to control-plane host subinterface. • transit—(Optional) Applies policies to control-plane transit subinterface. • cef-exception—(Optional) Applies policies to control-plane cef-exception subinterface. • cr—(Optional) Applies policies to all control-plane interfaces. |
| Step 4 | service-policy type logging input logging-policy-map-name Example: Router(config-cp)# service-policy type logging input log-policy | Applies a logging policy to a control-plane interface. <ul style="list-style-type: none"> • input—Applies the specified service policy to packets received on the control plane. • logging-policy-map-name—Name of a logging policy map (created by using the policy-map command) to be attached. The name can be a maximum of 40 alphanumeric characters. |
| Step 5 | end Example: Router(config-cp)# end | Exits control-plane configuration mode and returns to privileged EXEC mode. |

Configuring Feature-Specific or Class-Specific Logging

Feature-specific or class-specific control plane logging is implemented as an integrated part of Cisco's Control Plane Protection features, such as per-protocol queue-thresholding, port-filter, or control plane policing, as an action within their respective policy maps. To enable feature-specific or class-specific control plane logging, the log action should be added to the existing Control Plane Protection feature policy map.

The default behavior for a policy with the log action is to log matching packets. By default, the log messages contain source IP address, destination IP address, protocol name (IP/TCP/UDP), action (permit, drop, error), and port number. Additionally, there are options that can be configured with the log action that can enable logging of other fields in the IP header as well, such as TTL and packet length. There is also an option to configure the rate-limit interval for which log messages are created, that is the interval between the logging of two messages.

The additional options for the **log** action keyword are as follows:

- **interval**—Sets packet logging interval.
- **ttl**—Logs ttl for Ipv4 packets.
- **total-length**—Logs packet length for IPv4 packets.

Restrictions

The log action can be added only to policy maps of control-plane protection features, which are control plane policing, port-filtering, and queue-thresholding.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **policy-map** [type {stack | access-control | port-filter | queue-threshold | logging}]
policy-map-name
4. **class** *class-name*
5. **log** [interval *seconds* | total-length | ttl]
6. **end**

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|---|
| Step 1 | <pre>enable</pre> <p>Example: Router> enable </p> | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted. |
| Step 2 | <pre>configure terminal</pre> <p>Example: Router# configure terminal </p> | <p>Enters global configuration mode.</p> |
| Step 3 | <pre>policy-map [type {stack access-control port-filter queue-threshold logging}] policy-map-name</pre> <p>Example: Router(config)# policy-map type queue-threshold qt-policy </p> | <p>Creates a policy map and enters policy-map configuration mode.</p> <ul style="list-style-type: none"> type—(Optional) Specifies the service policy type. port-filter—(Optional) Enters the policy map for the port-filter feature. queue-threshold—(Optional) Enters the policy map for the queue-threshold feature. logging—(Optional) Enters policy-map configuration mode for the control plane logging feature. policy-map-name—Name of the policy map. The name can be a maximum of 40 alphanumeric characters. |
| Step 4 | <pre>class class-name</pre> <p>Example: Router(config-pmap)# class qt-host </p> | <p>Associates a class with a policy and enters class map configuration mode.</p> |
| Step 5 | <pre>log [interval seconds total-length ttl]</pre> <p>Example: Router(config-pmap-c)# log interval 1000 </p> | <p>Applies the log action to the service-policy class. You can configure the following additional parameters:</p> <ul style="list-style-type: none"> interval seconds—(Optional) Sets packet logging interval. total-length—(Optional) Logs packet length for IPv4 packets. ttl—(Optional) Logs ttl for IPv4 packets. |
| Step 6 | <pre>end</pre> <p>Example: Router(config-pmap-c)# end </p> | <p>Exits class-map configuration mode and returns to privileged EXEC mode.</p> |

Verifying Control Plane Logging Information

You can verify control plane logging for both global logging configurations and feature-specific or class-specific configurations.

To display active control plane logging information for global logging, perform the following optional steps.

SUMMARY STEPS

1. `enable`
2. `show policy-map type logging control-plane [host | transit | cef-exception | cr]`
3. `show policy-map [type policy-type] control-plane [host | transit | cef-exception | all | cr]`

DETAILED STEPS

| | Command or Action | Purpose |
|--------|---|--|
| Step 1 | <pre><code>enable</code></pre> <p>Example: Router> <code>enable</code></p> | Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted. |
| Step 2 | <pre><code>show policy-map type logging control-plane [host transit cef-exception cr]</code></pre> <p>Example: Router# <code>show policy-map type logging control-plane host</code></p> | Display information for global control plane logging. |
| Step 3 | <pre><code>show policy-map [type <i>policy-type</i>] control-plane [host transit cef-exception all cr]</code></pre> <p>Example: Router# <code>show policy-map type logging control-plane host</code></p> | Display information for feature-specific or class-specific control plane logging. <p>Note The example shows feature-specific or class-specific logging enabled on a port-filter policy.</p> |

Verification Examples for Control Plane Logging

This section provides the following examples:

- [Sample Output for a Global Logging Configuration: Example, page 11](#)
- [Sample Output for a Feature-Specific or Class-Specific Configuration: Example, page 12](#)
- [Sample Log Output: Example, page 12](#)

Sample Output for a Global Logging Configuration: Example

The following output displays the global logging service policy that was just added to the control-plane host feature path interface:

```
Router# show policy-map type logging control-plane host
```

```
Control Plane Host
Service-policy logging input: cpplog-host-policy
Class-map: cpplog-host-map (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match:  packets dropped
  0 packets, 0 bytes
  5 minute rate 0 bps
Match:  packets permitted
```

```

    0 packets, 0 bytes
    5 minute rate 0 bps

Class-map: class-default (match-any)
  0 packets, 0 bytes
  5 minute offered rate 0 bps, drop rate 0 bps
Match: any

```

Sample Output for a Feature-Specific or Class-Specific Configuration: Example

The following output displays the logging policy map that was just added to the control-plane host feature path interface:

```

Router# show policy-map cpp-policy
Policy Map cpp-policy
  Class cppclass-igp
  Class cppclass-management
    police rate 250 pps burst 61 packets
    conform-action transmit
    exceed-action drop
  Class cppclass-monitoring
    police rate 100 pps burst 24 packets
    conform-action transmit
    exceed-action drop
  Class cppclass-undesirable
    drop
    log interval 5000
  Class class-default
    police rate 50 pps burst 12 packets
    conform-action transmit
    exceed-action drop

```

Sample Log Output: Example

The following example shows log output for a configuration that sends IP traffic to the router:

```

Router#
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254
%CP-6-IP: PERMIT ttl=59 length=20 209.165.200.225 -> 209.165.200.254

```

The following is a description of the log information displayed in the preceding example:

- IP denotes the kind of traffic received.
- PERMIT means that no control-plane feature dropped the packet.
- ttl gives the ttl value in the IP header.
- length gives the total-length field in the IP header.

- 209.165.200.225 is the source IP address.
- 209.165.200.254 is the destination IP address.

The following example shows log output for a configuration that sends TCP traffic to the router:

Router#

```
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
%CP-6-TCP: PERMIT ttl=59 length=40 209.165.200.225(18611) -> 209.165.200.254(23)
```

The following is a description of the log information displayed in the preceding example:

- TCP denotes the kind of traffic received.
- PERMIT means that no control-plane feature dropped the packet.
- ttl gives the ttl value in the IP header.
- length gives the total-length field in the IP header.
- 209.165.200.225 is the source IP address.
- 18611 is the source TCP port.
- 209.165.200.254 is the destination IP address.
- 23 is the destination TCP port.

Configuration Examples for Control Plane Logging

This section provides the following configuration examples:

- [Configuring Global Control Plane Logging for Dropped and Permitted Packets: Example, page 13](#)
- [Configuring Global Control Plane Logging for Dropped Packets: Example, page 14](#)
- [Configuring Logging for a Specific Class: Example, page 15](#)
- [Configuring Logging for a Port-Filter Policy Map: Example, page 17](#)

Configuring Global Control Plane Logging for Dropped and Permitted Packets: Example

The following example shows how to configure a global control-plane logging service policy to log all dropped and permitted packets that hit the control-plane host feature path only, regardless of the interface from which the packets enter the router. Also, the router rate-limits the log messages to one every 5 seconds.

```
! Define a class map of type logging to specify what packets will be logged.
```

```
Router# configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
Router(config)# class-map type logging match-any cpplog-host-map
```

```
Router(config-cmap)# match packets dropped
```

```
Router(config-cmap)# match packets permitted
```

```
Router(config-cmap)# exit
```

```

! Define a policy map of type logging using your logging class map and rate-limit log
messages to one every 5 seconds.
Router(config)# policy-map type logging cpplog-host-policy
Router(config-pmap)# class cpplog-host-map
Router(config-pmap-c)# log interval 5000
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Apply the new logging policy map to the control-plane host feature path interface.
Router(config)# control-plane host
Router(config-cp)# service-policy type logging input cpplog-host-policy
Router(config-cp)# end
Router#
Aug  8 17:57:57.359: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#

```

The following output displays the logging policy map that was just added to the control-plane host feature path interface:

```

Router# show policy-map type logging control-plane host
Control Plane Host
  Service-policy logging input: cpplog-host-policy
    Class-map: cpplog-host-map (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: packets dropped
        0 packets, 0 bytes
        5 minute rate 0 bps
      Match: packets permitted
        0 packets, 0 bytes
        5 minute rate 0 bps
      log interval 5000
    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any

```

Configuring Global Control Plane Logging for Dropped Packets: Example

The following example shows how to configure a global control-plane logging service policy to log all dropped packets that come from GigabitEthernet interface 0/3 that hit the aggregate control-plane interface.

```

! Define a class map of type logging to specify what packets will be logged.
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.

```

```

Router(config)# class-map type logging match-all cpplog-gig
Router(config-cmap)# match input-interface gigabitethernet 0/3
Router(config-cmap)# match packets dropped
Router(config-cmap)# exit
! Define a policy map of type logging using your logging type class map.
Router(config)# policy-map type logging cpplog-gig-policy
Router(config-pmap)# class cpplog-gig
Router(config-pmap-c)# log
Router(config-pmap-c)# exit
Router(config-pmap)# exit
! Apply the new logging policy map to the aggregate control-plane interface.
Router(config)# control-plane
Router(config-cp)# service-policy type logging input cpplog-gig-policy
Router(config-cp)# end
Router#
Aug  8 12:53:08.618: %SYS-5-CONFIG_I: Configured from console by cisco on console
Router#

```

The following output displays the logging policy map that was just added to the aggregate control-plane interface:

```

Router# show policy-map type logging control-plane
Control Plane
Service-policy logging input: cpplog-gig-policy
  Class-map: cpplog-gig (match-all)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: input-interface GigabitEthernet0/3
    Match: dropped-packets
    log
  Class-map: class-default (match-any)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: any

```

Configuring Logging for a Specific Class: Example

The following example shows how to configure class-specific control plane logging for a specific class configured in a control plane policing service policy. This example also shows how to configure rate-limiting of logs to output only one log message every 5 seconds. For this example, you have a control plane policing service policy with classes defined for Interior Gateway Protocol (IGP), management, monitoring and, undesirable traffic. The undesirable class is configured to match packets that are destined to the router on UDP port 1434. The service policy is configured to drop all packets that

hit the undesirable class (in this case, packets that are destined for port 1434). For this example, you want to log all packets being dropped by the undesirable class, so that you will be aware that you are being attacked by 1434 packets.

In this example, you have the following control plane policing service policy configured:

```
Router# show policy-map cpp-policy
Policy Map cpp-policy
  Class cppclass-igp
  Class cppclass-management
    police rate 250 pps burst 61 packets
      conform-action transmit
      exceed-action drop
  Class cppclass-monitoring
    police rate 100 pps burst 24 packets
      conform-action transmit
      exceed-action drop
  Class cppclass-undesirable
    drop
  Class class-default
    police rate 50 pps burst 12 packets
      conform-action transmit
      exceed-action drop
```

To log all traffic for the undesirable class in the above service policy, perform the following steps:

! Enter control plane policing policy-map configuration mode.

```
Router# configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
Router(config)# policy-map cpp-policy
```

! Enter policy-map class configuration mode for the undesirable class.

```
Router(config-pmap)# class cppclass-undesirable
```

! Configure the log keyword with a rate limit of one log message every 5 seconds.

```
Router(config-pmap-c)# log interval 5000
```

```
Router(config-pmap-c)# end
```

Use the following command to verify that the log action has been added to the policy map under the undesirable class:

```
Router# show policy-map cpp-policy
Policy Map cpp-policy
  Class cppclass-igp
  Class cppclass-management
    police rate 250 pps burst 61 packets
      conform-action transmit
      exceed-action drop
  Class cppclass-monitoring
    police rate 100 pps burst 24 packets
      conform-action transmit
```

```

        exceed-action drop
    Class cppclass-undesirable
        drop
        log interval 5000
    Class class-default
        police rate 50 pps burst 12 packets
        conform-action transmit
        exceed-action drop

```

Configuring Logging for a Port-Filter Policy Map: Example

The following example shows how to configure class-specific control plane logging for a specific class configured in a Control Plane Protection port-filter policy map. This example also shows how to configure logging to display the packet-length field from the IP header for each packet that hits the port-filter class. For this example, you have a port-filter policy map configured to drop all traffic that is destined to closed TCP/UDP ports. For this example, you want to log all packets that are being dropped or allowed by the port-filter class.

In this example, you have the following port-filter service policy configured and applied to your control-plane host feature path. This policy blocks all traffic that is destined to closed or unlistened TCP/UDP ports:

```

Router# show policy-map type port-filter

Policy Map type port-filter pf-closed-port-policy
  Class pf-closed-ports
    Drop

```

The corresponding port-filter type class map that is used in the above port-filter policy map is configured as follows:

```

Router# show class-map type port-filter

Class Map type port-filter match-all pf-closed-ports (id 19)
  Match closed-ports

```

To log all traffic that is processed by the above pf-closed-ports class map in the above pf-closed-port-policy port-filter policy map, perform the following steps:

! Enter port-filter policy-map configuration mode.

```

Router# configure terminal

```

Enter configuration commands, one per line. End with CNTL/Z.

```

Router(config)# policy-map type port-filter pf-closed-port-policy

```

! Enter port-filter policy-map class configuration mode for the undesirable class.

```

Router(config-pmap)# class pf-closed-ports

```

! Configure the log keyword with the option to log the packet-length field in the IP header.

```

Router(config-pmap-c)# log total-length

```

```

Router(config-pmap-c)# end

```

Use the following command to verify that the log action has been added to the port-filter policy map under the appropriate class:

```

Router# show policy-map type port-filter

Policy Map type port-filter pf-closed-port-policy

```

```

Class pf-closed-ports
drop
  log interval 1000 total-length

```

Additional References

The following sections provide references related to the Control Plane Logging feature.

Related Documents

| Related Topic | Document Title |
|---|--|
| QoS commands: complete command syntax, command modes, command history, defaults, usage guidelines, and examples | Cisco IOS Quality of Service Solutions Command Reference |
| QoS feature overview | “Quality of Service Overview” module |
| Control plane protection | “Control Plane Protection” module |

Standards

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

MIBs

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

RFCs

| RFC | Title |
|------|-------|
| None | — |

Technical Assistance

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

Command Reference

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Quality of Service Solutions Command Reference* at http://www.cisco.com/en/US/docs/ios/qos/command/reference/qos_book.html. For information about all Cisco IOS commands, use the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or a Cisco IOS master commands list.

- **class-map**
- **debug control-plane**
- **policy-map**

Feature Information for Control Plane Logging

Table 1 lists the release history for this feature.

Not all commands may be available in your Cisco IOS software release. For release information about a specific command, see the command reference documentation.

Use Cisco Feature Navigator to find information about platform support and software image support. Cisco Feature Navigator enables you to determine which Cisco IOS and Catalyst OS software images support a specific software release, feature set, or platform. To access Cisco Feature Navigator, go to <http://www.cisco.com/go/cfn>. An account on Cisco.com is not required.



Note

Table 1 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release train. Unless noted otherwise, subsequent releases of that Cisco IOS software release train also support that feature.

Table 1 Feature Information for Control Plane Logging

| Feature Name | Releases | Feature Information |
|-----------------------|----------|--|
| Control Plane Logging | 12.4(6)T | Allows the control plane features to log all packets that match the class-map entries. |

CCDE, CCSI, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0903R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

