COPS Engine Operation

This document describes the Common Open Policy Service (COPS) engine feature on the Cisco CMTS routers. The Cisco CMTS routers also support Access control lists (ACLs) with the COPS engine.

Finding Feature Information

Finding Feature Information

Your software release may not support all the features that are documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. The Feature Information Table at the end of this document provides information about the documented features and lists the releases in which each feature is supported.

Hardware Compatibility Matrix for the Cisco cBR Series Routers

Note The hardware components that are introduced in a given Cisco IOS-XE Release are supported in all subsequent releases unless otherwise specified.

Table 1: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G • PID—CBR-SUP-8X10G-PIC	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R Cisco cBR-8 Downstream PHY Modules: • PID—CBR-D30-DS-MOD • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D30-US-MOD • PID—CBR-D31-US-MOD

Prerequisites for the COPS Engine on the Cisco CMTS Routers

- A compatible policy server must be connected to the network, such as the Cisco COPS QoS Policy Manager.
- Compliance with administrative policy, such as the Computer Assisted Law Enforcement Act (CALEA) or other lawful intercept (LI), is required for use of this feature on the Cisco CMTS routers.

Restrictions for the COPS Engine on the Cisco CMTS

- Resource Reservation Protocol (RSVP) is not configured on the Cisco CMTS. COPS engine configuration on the Cisco CMTS is limited to networks in which separate RSVP and COPS Servers are configured and operational.

Information About the COPS Engine on the Cisco CMTS

Common Open Policy Service (COPS) is a protocol for communicating network traffic policy information to network devices.

COPS works in correspondence with the Resource Reservation Protocol (RSVP), which is a means for reserving network resources—primarily bandwidth—to guarantee that applications sending end-to-end across the Internet will perform at the desired speed and quality. RSVP is not configured on the Cisco CMTS, but the Cisco CMTS presumes RSVP on the network for these configurations.

Refer to the for further information about COPS for RSVP.

How to Configure the COPS Engine on the Cisco CMTS

This section describes the tasks for configuring the COPS for RSVP feature on the Cisco CMTS.

To configure the COPS engine on the Cisco CMTS, perform the following tasks:

Configuring COPS TCP and DSCP Marking

This feature allows you to change the Differentiated Services Code Point (DSCP) marking for COPS messages that are transmitted or received by the Cisco router. The **cops ip dscp** command changes the default IP parameters for connections between the Cisco router and COPS servers in the cable network.

DSCP values are used in Quality of Service (QoS) configurations on a Cisco router to summarize the relationship between DSCP and IP precedence. This command allows COPS to remark the packets for either incoming or outbound connections.

The default setting is 0 for outbound connections. On default incoming connections, the COPS engine takes the DSCP value from the COPS server initiating the TCP connection.

Note   This feature affects all TCP connections with all COPS servers.

- For messages transmitted by the Cisco router, the default DSCP value is 0.
- For incoming connections to the Cisco router, the COPS engine takes the DSCP value used by the COPS server that initiates the TCP connection, by default.
- The **cops ip dscp** command allows the Cisco router to re-mark the COPS packets for either incoming or outbound connections.
- This command affects all TCP connections with all COPS servers.
- This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time.

Perform the following steps to enable optional DSCP marking for COPS messages on the Cisco CMTS.

Procedure

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

	Command or Action	Purpose
	Example: `Router> enable`	• Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cops ip dscp** [**<0-63>** | **default** | **af11-af43** | **cs1-cs7**] **Example:** `Router(config)# cops ip dscp default`	Specifies the marking for COPS messages that are transmitted by the Cisco router. The values for this command specify the markings with which COPS messages are transmitted. The following values are supported for the Cisco CMTS router: • **0-63**—DSCP value ranging from 0-63. • **af11**—Use AF11 dscp (001010) • **af12**—Use AF12 dscp (001100) • **af13**—Use AF13 dscp (001110) • **af21**—Use AF21 dscp (010010) • **af22**—Use AF22 dscp (010100) • **af23**—Use AF23 dscp (010110) • **af31**—Use AF31 dscp (011010) • **af32**—Use AF32 dscp (011100) • **af33**—Use AF33 dscp (011110) • **af41**—Use AF41 dscp (100010) • **af42**—Use AF42 dscp (100100) • **af43**—Use AF43 dscp (100110) • **cs1**—Use CS1 dscp (001000) [precedence 1] • **cs2**—Use CS2 dscp (010000) [precedence 2] • **cs3**—Use CS3 dscp (011000) [precedence 3] • **cs4**—Use CS4 dscp (100000) [precedence 4] • **cs5**—Use CS5 dscp (101000) [precedence 5] • **cs6**—Use CS6 dscp (110000) [precedence 6] • **cs7**—Use CS7 dscp (111000) [precedence 7] • **default**—Use default dscp (000000) • **ef**—Use EF dscp (101110)

	Command or Action	Purpose

Step 4	exit
	
	Example:
	
	`Router(config)# exit`
	`Router#`
		Returns to privileged EXEC mode.

Configuring COPS TCP Window Size

This feature allows you to override the default TCP receive window size that is used by COPS processes. This setting can be used to prevent the COPS server from sending too much data at one time.

Perform the following steps to change the TCP Window size on the Cisco CMTS.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cops tcp window-size** *bytes* **Example:** `Router(config)# cops tcp window-size 64000`	Overrides the default TCP receive window size on the Cisco CMTS. To return the TCP window size to a default setting of 4K, use the **no** form of this command. **Note** The default COPS TCP window size is 4000 bytes. **Note** This command does not affect existing connections to COPS servers. Once you issue this command, this function is supported only for new connections after that point in time. **Note** This command affects all TCP connections with all COPS servers.
Step 4	**exit** **Example:**	Returns to privileged EXEC mode.

Command or Action	Purpose
Router(config)# **exit** Router#	

Configuring Access Control List Support for COPS Engine

Perform the following steps to configure COPS ACLs on the Cisco CMTS.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**cops listeners access-list**{ *acl-num* |*acl-name* } **Example:** Router# **cops listeners access-list 40**	Configures access control lists (ACLs) for inbound connections to all COPS listener applications on the Cisco CMTS. To remove this setting from the Cisco CMTS, us the **no** form of this command.
Step 4	**exit** **Example:** Router(config)# **exit** Router#	Returns to privileged EXEC mode.

What to do next

Access lists can be displayed by using the **show access-list** command in privileged EXEC mode.

Restricting RSVP Policy to Specific Access Control Lists

Perform the following steps to restrict the RSVP policy to specific ACLs, as already configured on the Cisco CMTS.

For ACL configuration, refer to the Configuring Access Control List Support for COPS Engine, on page 6.

Procedure

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** Router# **configure terminal**	Enters global configuration mode.
Step 3	**interface cable** (*slot* /*subslot* /*port* } **Example:** Router(config)#**interface cable 8/0/1** Router(config-if)#	Enters interface configuration mode.
Step 4	**ip rsvp policy cops** *ACL-1 ACL-2* **servers** *iP-addr1 IP-addr2* **Example:** Router(config-if)# **ip rsvp policy cops 40 160 servers 161.44.130.164 161.44.129.2**	Tells the router to apply RSVP policy to messages that match the specified ACLs, and specifies the COPS server or servers for those sessions.
Step 5	exit **Example:** Router(config)# **exit** Router#	Returns to privileged EXEC mode.

Displaying and Verifying COPS Engine Configuration on the Cisco CMTS

Once COPS is enabled and configured on the Cisco CMTS, you can verify and track configuration by using one or all of the **show** commands in the following steps.

Procedure

	Command or Action	**Purpose**
Step 1	**enable** **Example:** Router> **enable**	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**show cops servers** **Example:** Router# **show cops servers**	Displays server addresses, port, state, keepalives, and policy client information.

	Command or Action	Purpose
Step 3	show ip rsvp policy cops **Example:** Router# **show ip rsvp policy cops**	Displays policy server addresses, ACL IDs, and client/server connection status.
Step 4	show ip rsvp policy **Example:** Router# **show ip rsvp policy**	Displays ACL IDs and their connection status.

Show Commands for COPS Engine Information

The following examples display three views of the COPS engine configuration on the Cisco router. These respective show commands verify the COPS engine configuration.

Displaying COPS Servers on the Network

This example displays the policy server address, state, keepalives, and policy client information:

```
Router# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
    COPS CLIENT: Client type: 1.  State: 0.
```

Displaying COPS Policy Information on the Network

This example displays the policy server address, the ACL ID, and the client/server connection status:

```
Router# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

Displaying Access Lists for COPS

This example displays the ACL ID numbers and the status for each ACL ID:

```
Router# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

COPS Engine Configuration Examples for Cable

The following sections provide COPS for RSVP configuration examples on the Cisco CMTS:

Example: COPS Server Specified

The following example specifies the COPS server and enables COPS for RSVP on the server. Both of these functions are accomplished by using the **ip rsvp policy cops** command. By implication, the default settings for all remaining COPS for RSVP commands are accepted.

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# ip rsvp policy cops servers 161.44.130.168 161.44.129.6
Router(config)# exit
```

Example: COPS Server Display

The following examples display three views of the COPS for RSVP configuration on the router, which can be used to verify the COPS for RSVP configuration.

This example displays the policy server address, state, keepalives, and policy client information:

```
Router# show cops servers
COPS SERVER: Address: 161.44.135.172. Port: 3288. State: 0. Keepalive: 120 sec
Number of clients: 1. Number of sessions: 1.
    COPS CLIENT: Client type: 1.  State: 0.
```

This example displays the policy server address, the ACL ID, and the client/server connection status:

```
Router# show ip rsvp policy cops
COPS/RSVP entry. ACLs: 40 60
PDPs: 161.44.135.172
Current state: Connected
Currently connected to PDP 161.44.135.172, port 0
```

This example displays the ACL ID numbers and the status for each ACL ID:

```
Router# show ip rsvp policy
Local policy: Currently unsupported
COPS:
ACLs: 40 60 . State: CONNECTED.
ACLs: 40 160 . State: CONNECTING.
```

Additional References

Related Documents

Related Topic	Document Title
Cisco CMTS Commands	Cisco CMTS Cable Command Reference
COPS for RSVP	• *Configuring COPS for RSVP* http://www.cisco.com/en/US/docs/ios-xml/ios/qos_rsvp/configuration/12-4t/cops_rsvp.htm • *COPS for RSVP* http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html

Standards

Standard	Title
PKT-SP-ESP-I01-991229	PacketCable™ Electronic Surveillance Specification (http://www.packetcable.com)

MIBs

MIB	MIBs Link
• No MIBs have been introduced or enhanced for support of this feature.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
General RFC Resources	• *RFC Index Search Engine* http://www.rfc-editor.org/rfcsearch.html • *SNMP: Frequently Asked Questions About MIB RFCs* http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800c2612.

Technical Assistance

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

Feature Information for COPS Engine Operation

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

Note The following table lists the software release in which a given feature is introduced. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Table 2: Feature Information for COPS Engine Operation

Feature Name	Releases	Feature Information
COPS Engine Operation	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.