



# CHAPTER 5

## COPS Engine Operation on the Cisco CMTS

Revised: November 10, 2008, OL-1467-08

Cisco IOS Release 12.3(13a)BC introduces support for the Common Open Policy Service (COPS) engine feature on the Cisco universal broadband routers. The Cisco Cable Modem Termination System (CMTS) also supports Access control lists (ACLs) with the COPS engine.

This document describes the configuration, monitoring and examples of the COPS engine on the Cisco CMTS. Refer to the “[Additional References](#)” section on page 5-12 for further information about COPS in general, and in additional Cisco IOS releases.

### History for the COPS Engine Feature

#### Feature History

| Release     | Modification  |
|-------------|---|
| 12.3(13a)BC | Support for Common Open Policy Service (COPS) engine and Access Control Lists for COPS introduced for the Cisco uBR10012 router and Cisco uBR7246VXR router.  |
| 12.3(21)BC  | Support for PacketCable Client Accept Timeout feature added. Refer to the following document for additional information: <ul style="list-style-type: none"><li><i>PacketCable and PacketCable MultiMedia for the Cisco CMTS</i><br/><a href="http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html">http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_pkcb.html</a></li></ul> |

#### Supported Platforms

Cisco uBR7246VXR and Cisco uBR10012 universal broadband routers

### 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 the COPS Engine on the Cisco CMTS” section on page 5-2
- “Restrictions for the COPS Engine on the Cisco CMTS” section on page 5-2
- “Information About the COPS Engine on the Cisco CMTS” section on page 5-2
- “How to Configure the COPS Engine on the Cisco CMTS” section on page 5-3
- “Additional References” section on page 5-12

- [“Command Reference” section on page 5-14](#)

## Prerequisites for the COPS Engine on the Cisco CMTS

- Cisco IOS Release 12.3(13a)BC, or a later 12.3 BC release, is required for COPS engine support on the Cisco CMTS.
- 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.

## 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 [“Additional References” section on page 5-12](#) 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 tasks described in the following sections. Required tasks are described first; the tasks in the remaining sections are optional.

## Required COPS Configurations on the Cisco CMTS

- [Configuring COPS TCP and DSCP Marking, page 5-3](#)
- [Configuring COPS TCP Window Size, page 5-5](#)

## Optional COPS Configurations on the Cisco CMTS

- [Configuring Access Control List Support for COPS Engine, page 5-6](#)

## Verifying and Debugging COPS on the Cisco CMTS

- [Displaying and Verifying COPS Engine Configuration on the Cisco CMTS, page 5-7](#)
- [Show Commands for COPS Engine Information, page 5-8](#)
- [Debugging the COPS Engine on the Cisco CMTS, page 5-9](#)

## 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. Cisco IOS Release 12.3(13a)BC supports this function with the **cops ip dscp** command. 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.

### SUMMARY STEPS

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

3. `cops ip dscp [<0-63> | default | af11-af43 | cs1-cs7]`
4. `exit`

## DETAILED STEPS

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | <p><code>enable</code></p> <p><b>Example:</b><br/>Router&gt; enable</p>  | <p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>   |
| Step 2 | <p><code>configure terminal</code></p> <p><b>Example:</b><br/>Router# configure terminal</p>                               | <p>Enters global configuration mode.</p>  |
| Step 3 | <p><code>cops ip dscp [&lt;0-63&gt;   default   af11-af43   cs1-cs7]</code></p> <p><b>Example:</b><br/>Router(config)#</p> | <p>Specifies the marking for COPS messages that are transmitted by the Cisco router.</p> <p>The values for this command specify the markings with which COPS messages are transmitted. The following values are supported for the Cisco CMTS router:</p> <ul style="list-style-type: none"> <li>• <b>0-63</b>—DSCP value ranging from 0-63.</li> <li>• <b>af11</b>—Use AF11 dscp (001010)</li> <li>• <b>af12</b>—Use AF12 dscp (001100)</li> <li>• <b>af13</b>—Use AF13 dscp (001110)</li> <li>• <b>af21</b>—Use AF21 dscp (010010)</li> <li>• <b>af22</b>—Use AF22 dscp (010100)</li> <li>• <b>af23</b>—Use AF23 dscp (010110)</li> <li>• <b>af31</b>—Use AF31 dscp (011010)</li> <li>• <b>af32</b>—Use AF32 dscp (011100)</li> <li>• <b>af33</b>—Use AF33 dscp (011110)</li> <li>• <b>af41</b>—Use AF41 dscp (100010)</li> <li>• <b>af42</b>—Use AF42 dscp (100100)</li> <li>• <b>af43</b>—Use AF43 dscp (100110)</li> <li>• <b>cs1</b>—Use CS1 dscp (001000) [precedence 1]</li> <li>• <b>cs2</b>—Use CS2 dscp (010000) [precedence 2]</li> <li>• <b>cs3</b>—Use CS3 dscp (011000) [precedence 3]</li> <li>• <b>cs4</b>—Use CS4 dscp (100000) [precedence 4]</li> <li>• <b>cs5</b>—Use CS5 dscp (101000) [precedence 5]</li> <li>• <b>cs6</b>—Use CS6 dscp (110000) [precedence 6]</li> <li>• <b>cs7</b>—Use CS7 dscp (111000) [precedence 7]</li> <li>• <b>default</b>—Use default dscp (000000)</li> <li>• <b>ef</b>—Use EF dscp (101110)</li> </ul> |
| Step 4 | <p><code>exit</code></p> <p><b>Example:</b><br/>Router(config)# exit<br/>Router#</p>                                       | <p>Returns to privileged EXEC mode.</p>   |

## 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. Cisco IOS Release 12.3(13a)BC supports this function with the **cops tcp window-size bytes** command.

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

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cops tcp window-size bytes**
4. **exit**

### DETAILED STEPS

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                         | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal | Enters global configuration mode.   |
| Step 3 | <b>cops tcp window-size bytes</b><br><br><b>Example:</b><br>Router#            | <p>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 <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li>• <i>bytes</i>—This is the TCP window size setting in bytes. This value can range from 516 to 65535 bytes.</li> </ul> <p><b>Note</b> The default COPS TCP window size is 4000 bytes.</p> <p><b>Note</b> 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.</p> <p><b>Note</b> This command affects all TCP connections with all COPS servers.</p> |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>Router#          | Returns to privileged EXEC mode.  |

### Examples

The following example configures the TCP window size to be 64000 bytes.

```
Router(config)# cops tcp window-size 64000
```

## Configuring Access Control List Support for COPS Engine

Cisco IOS Release 12.3(13)BC introduces support for Access Control Lists (ACLs) for COPS. Perform the following steps to configure COPS ACLs on the Cisco CMTS.



### Note

When using ACLs with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cops listeners access-list** {*acl-num* | *acl-name*}
4. **exit**

### DETAILED STEPS

|        | Command or Action  | Purpose   |
|--------|--|---|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable   | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>  |
| Step 2 | <b>configure terminal</b><br><br><b>Example:</b><br>Router# configure terminal   | Enters global configuration mode.   |
| Step 3 | <b>cops listeners access-list</b> { <i>acl-num</i>   <i>acl-name</i> }<br><br><b>Example:</b><br>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, use the <b>no</b> form of this command. <ul style="list-style-type: none"> <li>• <i>acl-num</i>—Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.</li> <li>• <i>acl-name</i>—Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199.</li> </ul> |
| Step 4 | <b>exit</b><br><br><b>Example:</b><br>Router(config)# exit<br>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.

## 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.

### SUMMARY STEPS

1. **enable**
2. **show cops servers**
3. **show ip rsvp policy cops**
4. **show ip rsvp policy**

### DETAILED STEPS

|        | Command or Action  | Purpose  |
|--------|--|--|
| Step 1 | <b>enable</b><br><br><b>Example:</b><br>Router> enable                                     | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| Step 2 | <b>show cops servers</b><br><br><b>Example:</b><br>Router# show cops servers               | Displays server addresses, port, state, keepalives, and policy client information.                                 |
| Step 3 | <b>show ip rsvp policy cops</b><br><br><b>Example:</b><br>Router# show ip rsvp policy cops | Displays policy server addresses, ACL IDs, and client/server connection status.                                    |
| Step 4 | <b>show ip rsvp policy</b><br><br><b>Example:</b><br>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.

- **show cops servers**, see [Displaying COPS Servers on the Network, page 5-8](#)
- **show ip rsvp policy cops**, see [Displaying COPS Policy Information on the Network, page 5-8](#)
- **show ip rsvp policy**, see [Displaying Access Lists for COPS, page 5-8](#)

### 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.
```

## Debugging the COPS Engine on the Cisco CMTS

Cisco IOS Release 12.3(13a)BC and later releases support the following commands for debugging the COPS Engine on the Cisco CMTS:

- **debug packetcable cops**, see [Debugging COPS for PacketCable, page 5-9](#)
- **debug packetcable gate control**, see
- **deb packetcable subscriber**
- **show debug**

### Debugging COPS for PacketCable

To enable debugging processes for PacketCable with the COPS engine, use the **debug packetcable cops** command in privileged EXEC mode. To disable debugging, use the **no** form of this command.

**debug packetcable cops**

**no debug packetcable cops**

The following example illustrates the **debug packetcable cops** command.

```
Router# debug packetcable cops
Pktcbl COPS msgs debugging is on
```

### Debugging PacketCable Gate Control

To enable and display debugging processes for PacketCable gate control, use the **debug packetcable gate control** command in privileged EXEC mode. To disable this debugging, use the **no** form of this command:

**debug packetcable gate control**

**no debug packetcable gate control**

The following example illustrates gate control debugging:

```
Router# debug packetcable gate control
Pktcbl gate control msgs debugging is on
```

### Debugging PacketCable Subscribers

To enable and display debugging processes for PacketCable subscribers, use the **debug packetcable subscriber** command in privileged EXEC mode. To disable this debugging, use the **no** form of this command:

**debug packetcable subscriber *IP-addr***

**no debug packetcable subscriber *IP-addr***

The following example illustrates the activation of the **debug packetcable subscriber** command for the specified IP address:

```
Router# debug packetcable subscriber 68.1.2.5
Pktcbl on the subscriber debugging is on
```

## Displaying Enabled Debug Functions

To display current debugging information that includes PacketCable COPS messages on the Cisco CMTS, use the **show debug** command in privileged EXEC mode.

```
Router# show debug
PacketCable Client:
  Pktcbl COPS msgs debugging is on
PacketCable specific:
  Debugging is on for Subscriber 68.1.2.4, Mask 255.255.255.255
SLOT 6/0: Nov 19 04:57:09.219: %UBR10000-5-UNREGSIDTIMEOUT: CMTS deleted unregistered
Cable Modem 0002.8a8c.8c1a
SLOT 6/0: Nov 19 04:57:12.279: %UBR10000-5-UNREGSIDTIMEOUT: CMTS deleted unregistered
Cable Modem 0002.8a8c.92ae
*Nov 19 04:57:19.751: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.751: PktCbl(cops): Received a COPS DEC message, flags is 0x1
*Nov 19 04:57:19.755: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.755: PktCbl(cops): Received a COPS DEC message, flags is 0x1
*Nov 19 04:57:19.755: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.755: PktCbl(cops): Received a COPS DEC message, flags is 0x1
*Nov 19 04:57:19.755: PktCbl(cops): Received callback [code 2, handle: 0x63982B08] from
COPS engine
*Nov 19 04:57:19.755: PktCbl(ndle: 0x63982B08] from COPS engine
```

## COPS Engine Configuration Examples for Cable

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

- [COPS Server Specified Example](#)
- [COPS Server Display Examples](#)

For information about configuring COPS for RSVP, see the section “[How to Configure the COPS Engine on the Cisco CMTS](#)” section on page 5-3.

### COPS Server Specified Example

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
```

### COPS Server Display Examples

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

The following sections provide references related to COPS and other cable intercept features, whether in support of Cisco universal broadband routers, or more general IOS support for COPS.

### Related Documents

| Related Topic                                | Document Title   |
|--|--|
| Broadband Cable Command Reference            | <ul style="list-style-type: none"> <li><i>Cisco Broadband Cable Command Reference Guide</i><br/><a href="http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html">http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html</a></li> </ul>   |
| Cable Monitor and Intercept                  | <ul style="list-style-type: none"> <li><i>Cable Monitor and Intercept Features for the Cisco CMTS</i><br/><a href="http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_mon.html">http://www.cisco.com/en/US/docs/cable/cmts/feature/guide/ufg_mon.html</a></li> </ul>   |
| COPS for RSVP in Mainline Cisco IOS releases | <ul style="list-style-type: none"> <li><i>Configuring COPS for RSVP</i><br/><a href="http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html">http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html</a></li> <li><i>COPS for RSVP</i><br/><a href="http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html">http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html</a></li> </ul> |

### Standards

| Standard                              | Title   |
|---------------------------------------|---|
| <a href="#">PKT-SP-ESP-I01-991229</a> | PacketCable™ Electronic Surveillance Specification (<br><a href="http://www.cablelabs.com/packetcable">http://www.cablelabs.com/packetcable</a> ) |

### MIBs

| MIB   | MIBs Link   |
|---|---|
| <ul style="list-style-type: none"> <li>No MIBs have been introduced or enhanced for support of this feature.</li> </ul> | <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><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></p> |

## RFCs

| RFC                   | Title   |
|-----------------------|---|
| General RFC Resources | <ul style="list-style-type: none"><li>• <i>RFC Index Search Engine</i><br/><a href="http://www.rfc-editor.org/rfcsearch.html">http://www.rfc-editor.org/rfcsearch.html</a></li><li>• <i>SNMP: Frequently Asked Questions About MIB RFCs</i><br/><a href="http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800c2612.shtml">http://www.cisco.com/en/US/tech/tk648/tk362/technologies_q_and_a_item09186a00800c2612.shtml</a></li></ul> |

## 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. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

# Command Reference

This section documents new commands that support the COPS engine on the Cisco CMTS in Cisco IOS Release 12.3(13a)BC and later releases.

- [cops ip dscp](#)
- [cops listeners access-list](#)
- [cops tcp window-size](#)

## cops ip dscp

To specify the marking for COPS messages that are transmitted by the Cisco router, use the **cops ip dscp** command in global configuration mode. To remove this configuration, use the **no** form of this command.

**cops ip dscp** *x*

**no cops ip dscp**

| Syntax Description |          |   |
|--------------------|----------|---|
|                    | <i>x</i> | <p>This value specifies the markings with which COPS messages are transmitted. The following values are supported:</p> <ul style="list-style-type: none"> <li>• <b>0-63</b>—DSCP value ranging from 0-63.</li> <li>• <b>af11</b>—Use AF11 dscp (001010)</li> <li>• <b>af12</b>—Use AF12 dscp (001100)</li> <li>• <b>af13</b>—Use AF13 dscp (001110)</li> <li>• <b>af21</b>—Use AF21 dscp (010010)</li> <li>• <b>af22</b>—Use AF22 dscp (010100)</li> <li>• <b>af23</b>—Use AF23 dscp (010110)</li> <li>• <b>af31</b>—Use AF31 dscp (011010)</li> <li>• <b>af32</b>—Use AF32 dscp (011100)</li> <li>• <b>af33</b>—Use AF33 dscp (011110)</li> <li>• <b>af41</b>—Use AF41 dscp (100010)</li> <li>• <b>af42</b>—Use AF42 dscp (100100)</li> <li>• <b>af43</b>—Use AF43 dscp (100110)</li> <li>• <b>cs1</b>—Use CS1 dscp (001000) [precedence 1]</li> <li>• <b>cs2</b>—Use CS2 dscp (010000) [precedence 2]</li> <li>• <b>cs3</b>—Use CS3 dscp (011000) [precedence 3]</li> <li>• <b>cs4</b>—Use CS4 dscp (100000) [precedence 4]</li> <li>• <b>cs5</b>—Use CS5 dscp (101000) [precedence 5]</li> <li>• <b>cs6</b>—Use CS6 dscp (110000) [precedence 6]</li> <li>• <b>cs7</b>—Use CS7 dscp (111000) [precedence 7]</li> <li>• <b>default</b>—Use default dscp (000000)</li> <li>• <b>ef</b>—Use EF dscp (101110)</li> </ul> |

### Defaults

- For messages transmitted by the Cisco router, the default DSCP value is 0.
- For incoming connections to the Cisco router, by default, the COPS engine takes the DSCP value used by the COPS server that initiates the TCP connection.

**Command Modes** Global configuration mode

| Command History | Release     | Modification                 |
|-----------------|-------------|------------------------------|
|                 | 12.3(13a)BC | This command was introduced. |

- Usage Guidelines**
- 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.

**Examples** The following example illustrates the **cops ip dscp** command with supported command variations:

```
Router(config)# cops ip dscp ?
<0-63>   DSCP value
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)
```

### Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the “Configuring Access Control List Support for COPS Engine” section on page 5-6.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Configuring COPS for RSVP*  
[http://www.cisco.com/en/US/docs/ios/12\\_2/qos/configuration/guide/qfcops\\_ps1835\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html)
- *COPS for RSVP*  
[http://www.cisco.com/en/US/docs/ios/12\\_1t/12\\_1t1/feature/guide/CopsRSVP.html](http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html)

## cops listeners access-list

To configure access control lists (ACLs) for inbound connections to all COPS listener applications on the Cisco CMTS, use the **cops listeners access-list** command in global configuration mode. To remove this setting from the Cisco CMTS, use the **no** form of this command.

```
cops listeners access-list {acl-num | acl-name}
```

```
no cops listeners access-list {acl-num | acl-name}
```

| Syntax Description |  |  |
|--------------------|--|--|
| <i>acl-num</i>     |  | Alphanumeric identifier of up to 30 characters, beginning with a letter that identifies the ACL to apply to the current interface.   |
| <i>acl-name</i>    |  | Numeric identifier that identifies the access list to apply to the current interface. For standard access lists, the valid range is 1 to 99; for extended access lists, the valid range is 100 to 199. |

**Command Default** Access lists are not configured by default on the Cisco router.

**Command Modes** Global configuration mode

| Command History | Release     | Modification                 |
|-----------------|-------------|------------------------------|
|                 | 12.3(13a)BC | This command was introduced. |

### Usage Guidelines



#### Note

When using Access Control Lists (ACLs) with cable monitor and the Cisco uBR10012 router, combine multiple ACLs into one ACL, and then configure cable monitor with the consolidated ACL. Further information about the Cable Monitor is available in the chapter titled “[Cable Monitor and Intercept Features for the Cisco CMTS](#).”

**Examples** The following example illustrates a short access list configuration for the COPS listener feature:

```
Router# cops listeners access-list 40
```

# cops tcp window-size

To override the default TCP receive window size on the Cisco CMTS, use the **cops tcp window-size** command in global configuration mode. This setting allows you to prevent the COPS server from sending too much data at one time. To return the TCP window size to a default setting of 4K, use the **no** form of this command.

**cops tcp window-size** *bytes*

**no cops tcp window-size**

## Syntax Description

|              |   |
|--------------|---|
| <i>bytes</i> | This is the TCP window size setting in bytes. This value can range from 516 to 65535 bytes. |
|--------------|---|

## Defaults

The default COPS TCP window size is 4000 bytes.

## Usage Guidelines

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.

## Examples

The following example configures the TCP window size to be 64000 bytes.

```
Router(config)# cops tcp window-size 64000
```

The following example illustrates online help for this command:

```
Router(config)# cops tcp window-size ?
<516-65535> Size in bytes
```

## Command Modes

Global configuration mode

## Command History

| Release     | Modification                 |
|-------------|------------------------------|
| 12.3(13a)BC | This command was introduced. |

## Additional COPS Information

Cisco 12.3(13a)BC also supports Access Control Lists (ACLs) for use with COPS. Refer to the “Configuring Access Control List Support for COPS Engine” section on page 5-6.

For additional information about configuring COPS on the Cisco CMTS, refer to the following documents on Cisco.com:

- *Configuring COPS for RSVP*  
[http://www.cisco.com/en/US/docs/ios/12\\_2/qos/configuration/guide/qcfcops\\_ps1835\\_TSD\\_Products\\_Configuration\\_Guide\\_Chapter.html](http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfcops_ps1835_TSD_Products_Configuration_Guide_Chapter.html)
- *COPS for RSVP*  
[http://www.cisco.com/en/US/docs/ios/12\\_1t/12\\_1t1/feature/guide/CopsRSVP.html](http://www.cisco.com/en/US/docs/ios/12_1t/12_1t1/feature/guide/CopsRSVP.html)

■ cops tcp window-size