



# Multicast VPN and DOCSIS 3.0 Multicast QoS Support

---

**Revised: July 29, 2008, Cisco IOS Release 12.2(33)SCA**

**First Published: February 14, 2008, Cisco IOS Release 12.2(33)SCA**

The CMTS enhanced multicast new features are consistent with DOCSIS 3.0 specifications and include:

- Enhanced multicast echo in which the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table.
- Enhanced multicast quality of service (MQoS) framework that specifies a group configuration (GC) to define a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN).
- Intelligent multicast admission control to include multicast service flows.
- Enhanced multicast VPN feature to configure and support multicast traffic in a multiprotocol label switching (MPLS)-VPN environment.

## Finding Feature Information in This Module

Your Cisco IOS software release may not support all of the features documented in this module. 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 Multicast VPN and DOCSIS 3.0 Multicast QoS Support](#)” section on page 931.

## 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 the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature, page 916](#)
- [Restrictions for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature, page 916](#)
- [Information About the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature, page 917](#)



---

**Americas Headquarters:**

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

© 2008 Cisco Systems, Inc. All rights reserved.

- [How to Configure the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature](#), page 919
- [Configuration Examples for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature](#), page 928
- [Where to Go Next](#), page 928
- [Additional References](#), page 929
- [Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support](#), page 931

## Prerequisites for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature

DOCSIS 1.1 or 2.0 modems are required for multicast encryption. [Table 1](#) shows the Cisco Cable Modem Termination System (CMTS) hardware compatibility prerequisites for this feature.

**Table 1** *Multicast VPN and DOCSIS 3.0 Multicast QoS Support Hardware Compatibility Matrix*

CMTS Platform	Processor Engine	Cable Interface Cards
Cisco uBR10012 Universal Broadband Router	<b>Cisco IOS Release 12.2(33)SCA</b> <ul style="list-style-type: none"> <li>• PRE-2</li> </ul>	<b>Cisco IOS Release 12.2(33)SCA</b> <ul style="list-style-type: none"> <li>• Cisco uBR10-MC5X20S/U/H</li> </ul>
Cisco uBR7246VXR Universal Broadband Router	<b>Cisco IOS Release 12.2(33)SCA</b> <ul style="list-style-type: none"> <li>• NPE-G1</li> <li>• NPE-G2</li> </ul>	<b>Cisco IOS Release 12.2(33)SCA</b> <ul style="list-style-type: none"> <li>• Cisco uBR-MC28U/X</li> <li>• Cisco uBR-MC16U/X</li> </ul>
Cisco uBR7225VXR Universal Broadband Router	<b>Cisco IOS Release 12.2(33)SCA</b> <ul style="list-style-type: none"> <li>• NPE-G1</li> </ul>	<b>Cisco IOS Release 12.2(33)SCA</b> <ul style="list-style-type: none"> <li>• Cisco uBR-E-28U</li> <li>• Cisco uBR-E-16U</li> <li>• Cisco uBR-MC28U/X</li> <li>• Cisco uBR-MC16U/X</li> </ul>

## Restrictions for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature

You can only configure type of service (ToS) for Cisco uBR7200 series universal broadband routers. This parameter is not recognized by the Cisco uBR10012 universal broadband router.

# Information About the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature

IP multicast—transmission of the same information to multiple cable network recipients—improves bandwidth efficiency and allows service providers to offer differentiated quality of service for different types of traffic. Enhanced multicast introduces multicast improvements as mandated by the introduction of DOCSIS 3.0 specifications.

**Note**

---

DOCSIS 3.0 standards retain backwards compatibility with the DOCSIS 2.0 multicast mode of operation.

---

The benefits of CMTS enhanced multicast are:

- Improved multicast echo
- Enhanced quality of service (QoS)
- Intelligent multicast admission control
- Multicast session limit support
- Multicast virtual private network (VPN)

## Improved Multicast Echo

In the enhanced multicast echo feature, the Layer 3 multicast switching path uses a parallel express forwarding (PXF) multicast routing table instead of the existing multicast echo path. Therefore, upstream packets are echoed using the Layer 3 switching path and all upstream data packets are treated similarly to the ingress packets from a WAN interface, in which they pass through existing classifiers and service flows.

The advantages of improved multicast echo are the following:

- Each outgoing interface has its own DSJIB/DSBlaze header to satisfy baseline privacy interface plus (BPI+) and downstream session identifier (DSID) requirements.
- The echoing decision is based on the PXF multicast routing table with packets forwarded only to interfaces that have existing clients.
- There is independent control of echoing multicast traffic for a single cable interface within a defined cable bundle.
- Bandwidth consumption is reduced because the upstream multicast data packets are not echoed to physical interfaces within the same cable bundle group that do not have an existing client.
- The Internet Group Management Protocol (IGMP) control packets echo functionality is retained allowing the ability to selectively enable or disable multicast echo for IGMP reports and data.
- Multicast QoS is supported because packets are following the same forwarding path as downstream multicast packets.

## Enhanced Quality of Service

In the new multicast QoS (MQoS) framework, you can specify a group configuration (GC) that defines a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN). For every GC, there is attached a group QoS configuration (GQC) and a group encryption rule.

Based on the session range, rule priority, and MVPN, a multicast service flow is admitted into a GC and the associated GQC and group encryption rule are applied to the flow. In MQoS implementation, the source address of the multicast session is not checked because the current implementation for cable-specific multicast supports IGMP Version 2 but not IGMP Version 3. The downstream service flow, service identifier (SID), and MAC-rewrite string are created at the time of a new IGMP join (or static multicast group CLI on the interface) and MQoS is applied to the new multicast group join.

The benefits of enhanced QoS are the following:

- Group classifiers can be applied at cable interface level and also at bundle interface level.
- Group service flow (GSF) definition is based on service class names. The GSF is similar to individual service flows and commonly includes the minimum rate and maximum rate parameters for the service class. GSF is shared by all cable modems on a particular downstream channel set (DCS) that is matched to the same group classifier rule (GCR). A default service flow is used for multicast flows that do not match to any GCR. A GSF is always in the active state.
- CMTS replicates multicast packets and then classifies them.
- Single-stage replication and two-stage replication are supported.
- Enhanced QoS is compatible and integrated with DOCSIS Set-Top Gateway (DSG).

## Intelligent Multicast Admission Control

Admission control allows you to categorize service flows into buckets. Examples of categories are the service class name used to create the service flow, service flow priority, or the service flow type such as unsolicited grant service (UGS). Bandwidth limits for each bucket can also be defined. For example, you can define bucket 1 for high priority packet cable service flows and specify that bucket 1 is allowed a minimum of 30 percent and a maximum of 50 percent of the link bandwidth.

Intelligent multicast admission control includes additional features such as the inclusion of multicast service flows using the GSF concept. GSFs are created based on the rules as defined in the GQC table. The rules link the multicast streams to a GSF through the session range. The service class name in the rule defines the QoS for that GSF. Additionally, another attribute is added to the rules and the group configuration table to specify the application type to which each GSF belongs. In this way, the QoS associated with each GSF is independent of the bucket category for the GSF.

The benefits of intelligent multicast admission control are the following:

- There is explicit acknowledgment of the establishment of each multicast session.
- Admission control does not consume additional bandwidth for multicast flows once the first flow is established.
- Service flows are cleaned up as the multicast session is torn down.

## Multicast Session Limit Support

In a multicast video environment, you can limit the number of multicast sessions admitted onto a particular service flow. The multicast session limit feature—which adds functionality on top of the multicast QoS infrastructure—enables you to specify the number of multicast sessions to be admitted on a particular service flow. If the current number of sessions has reached the defined limit, new sessions will be forwarded but they will make use of the default multicast service flow until a session ends to free up a slot for new sessions.

## Multicast Virtual Private Network

The new multicast VPN (MVPN) feature allows you to configure and support multicast traffic in a multiprotocol label switching (MPLS)-VPN environment. This feature supports routing and forwarding of multicast packets for each individual VPN virtual routing and forwarding (VRF) instance, and also provides a mechanism to transport VPN multicast packets across the service provider backbone.

MVPN allows you to connect multiple remote sites or devices over either a Layer 3 or Layer 2 VPN. A Layer 3 VPN enables the routing of traffic inside the VPN. A Layer 2 VPN provides a bridging transport mechanism for traffic between remote sites belonging to a customer. To support multicast over Layer 3 VPNs, each VPN receives a separate multicast domain with an associated MVPN routing and forwarding (mVRF) table maintained by the provider edge (PE) router. In a cable environment, the PE router is a routing CMTS. The provider network builds a default multicast distribution tree (default-MDT) for each VPN between all the associated mVRF-enabled PE routers. This tree is used to distribute multicast traffic to all PE routers.

To enable maximum security and data privacy in a VPN environment, the CMTS distinguishes between multicast sessions on the same downstream interface that belong to different VPNs. To differentiate multicast traffic between different VPNs, the CMTS implements a per-VRF subinterface multicast security association identifier (MSAID) allocation feature that is BPI+ enabled. The MSAID is allocated for each cable bundle group for each subinterface. A multicast group has a specific MSAID for each VRF instance.

## How to Configure the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature

This section contains the following procedures:

- [Configuring a QoS Profile for a Multicast Group, page 920](#)
- [Configuring Encryption for a Multicast Group, page 921](#)
- [Configuring a Multicast QoS Group, page 922](#)
- [Configuring a Default Multicast QoS Group for VRF, page 925](#)
- [Verifying Configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature, page 927](#)

## Configuring a QoS Profile for a Multicast Group

To configure a QoS profile that can be applied to a QoS group configuration, use the **cable multicast group-qos** command. You must configure a QoS profile before you can add a QoS profile to a QoS multicast group.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable multicast group-qos** *number* *service-class-name* { | [ *max-sessions* ] }

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> 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><b>configure terminal</b></p> <p>Router# configure terminal</p> <pre><b>cable multicast group-qos</b> number service-class-name      {            [          max-sessions]}</pre> <p>Router(config)#: cable multicast group-qos 2 scn name1 control single</p>	<p>Enters global configuration mode.</p> <p>Configures a QoS profile that can be applied to a multicast QoS group.</p> <p><i>number</i>—Specifies the QoS profile number that can be applied to a multicast QoS group. The valid range is 1–255.</p> <p>If a number is not specified, a default QoS profile is applied. The default group qos configuration creates a default multicast service flow for each cable interface that is used when a multicast session does not match any classifiers of a GC on the interface.</p> <p><b>scn</b> <i>service-class-name</i>—Specifies the service class name for the QoS profile service class.</p> <p><b>control</b>—Specifies the type of control to the service flow.</p> <ul style="list-style-type: none"> <li><b>single</b>—Specifies that a separate service flow is created for each session:</li> <li><b>aggregate</b>—Specifies that service flows are grouped for sessions in the same MQoS group.</li> </ul> <p><b>limit</b> <i>max-sessions</i>—(Optional) Specifies the Internet Group Management Protocol (IGMP) session limit for aggregate service flows. The valid range is 1–255.</p>

## Configuring Encryption for a Multicast Group

To configure and enable an encryption profile that can be applied to a QoS group configuration (GC), use the **cable multicast group-encryption** command. You must configure an encryption profile before you can add an encryption profile to a QoS multicast group.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable multicast group-encryption** *number* **algorithm** **56bit-des**

	Command or Action	Purpose
Step 1	<p><b>Example:</b> 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><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>cable multicast group-encryption</b> <i>number</i> <b>algorithm</b> 56bit-des</p> <p><b>Example:</b> Router(config)#: cable multicast group-encryption 35 algorithm 56bit-des</p>	<p>Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile.</p> <ul style="list-style-type: none"> <li>• <i>number</i>—Enables encryption and specifies the encryption number that can be applied to a specific cable multicast QoS group. The valid range is 1–255.</li> <li>• —Specifies that the data encryption standard (DES) is 56 bits.</li> </ul>

You can specify a group configuration (GC) that defines a session range of multicast addresses and rule priorities and its associated multicast VPN (MVPN). For every GC, there is attached a group QoS configuration and a group encryption rule.

**enable**

**configure terminal**

**cable multicast group-encryption** *number* **algorithm** 56bit-des

**cable multicast group-qos** *number scn service-class-name control* {single | aggregate [limit *max-sessions*]}

5. **cable multicast qos group** *id priority value* [global]

6. **session-range** *ip-address ip-mask*

7. **tos** *low-byte high-byte mask*

8. **vrf** *name*

9. **application-id** *number*

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>enable</b></p> <p><b>Example:</b> 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><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p><b>cable multicast group-encryption</b> <i>number</i> <b>algorithm</b> <i>56bit-des</i></p> <p><b>Example:</b> Router(config-mqos)# cable multicast group-encryption 12 algorithm 56bit-des</p>	<p>(Optional) Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile.</p> <ul style="list-style-type: none"> <li>• —Enables encryption and specifies the encryption number that can be applied to a specific cable multicast QoS group. The valid range is 1–255.</li> <li>• —Specifies that the data encryption standard (DES) is 56 bits.</li> </ul>
Step 4	<p><b>cable multicast group-qos</b> <i>number scn</i> <i>service-class-name</i> <b>control</b> {<b>single</b>   <b>aggregate</b> [<b>limit</b> <i>max-sessions</i>]}</p> <p><b>Example:</b> Router(config-mqos)# cable multicast group-qos 5 scn name1 control single</p>	<p>(Optional) Configures a QoS profile that can be applied to a multicast QoS group.</p> <ul style="list-style-type: none"> <li>• —Specifies the QoS profile number that can be applied to a multicast QoS group. The valid range is 1–255.</li> </ul> <p><b>Note</b> If a number is not specified, a default QoS profile is applied. The default group qos configuration creates a default multicast service flow for each cable interface that is used when a multicast session does not match any classifiers of a GC on the interface.</p> <ul style="list-style-type: none"> <li>• —Specifies the service class name for the QoS profile service class.</li> <li>• —Specifies the type of control to the service flow: <ul style="list-style-type: none"> <li>– —Specifies that a separate service flow is created for each session.</li> <li>– —Specifies that service flows are grouped for sessions in the same MQoS group.</li> </ul> </li> <li>• —(Optional) Specifies the Internet Group Management Protocol (IGMP) session limit for aggregate service flows. The valid range is 1–255.</li> </ul>

	Command or Action	Purpose
Step 5	<p><b>cable multicast qos group</b> <i>id priority value</i> [<i>global</i>]</p> <p><b>Example:</b> Router(config)# cable multicast qos group 2 priority 6</p>	<p>Configures a multicast QoS group and enters multicast QoS configuration mode.</p> <ul style="list-style-type: none"> <li>—The number of the cable multicast QoS group. The valid range is 1–255.</li> <li>—The priority of the cable multicast QoS group. The valid range is 1–255.</li> <li>—(Optional) Specifies that the multicast QoS group configuration is applied to all cable interfaces.</li> </ul>
Step 6	<p><b>session-range</b> <i>ip-address ip-mask</i></p> <p><b>Example:</b> Router(config-mqos)# session-range 224.10.10.10 255.255.255.224</p>	<p>Specifies the session range IP address and IP mask of the multicast QoS group. You can configure multiple session ranges.</p>
Step 7	<p><b>tos</b> <i>low-byte high-byte mask</i></p> <p><b>Example:</b> Router(config-mqos)# tos 1 6 15</p>	<p>(Optional) Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for a multicast QoS group. The valid range for each is 0–255.</p>
Step 8	<p><b>vrf</b> <i>name</i></p> <p><b>Example:</b> Router(config-mqos)# vrf name1</p>	<p>(Optional) Specifies the name for the virtual routing and forwarding (VRF) instance.</p> <p><b>Note</b> If a multicast QoS (MQoS) group is not defined for this VRF, you will see an error message. You must either define a specific MQoS group for each VRF, or define a default MQoS group that can be assigned in those situations where no matching MQoS group is found. See the “<a href="#">Configuring a Default Multicast QoS Group for VRF</a>” section on page 925.</p>
Step 9	<p><b>application-id</b> <i>number</i></p> <p><b>Example:</b> Router(config-mqos)# application-id 25</p>	<p>(Optional) Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group. The valid range is 1–65535.</p>

## Configuring a Default Multicast QoS Group for VRF

Each virtual routing and forwarding (VRF) instance that is defined must match a defined MQoS group to avoid multicast stream crosstalk between VRFs. To avoid potential crosstalk, define a default MQoS group that is assigned to the VRF whenever the multicast traffic in the VRF does not match an existing MQoS group.

### SUMMARY STEPS

- 1.
- 2.
- 3.
4. `multicast qos` { `1` | `2` | `3` | `4` | `5` | `6` | `7` | `8` | `9` }
5. `session-range` `255 global`
6. `session-range` `224.0.0.0 224.0.0.0`
7. `tos`
8. `vrf`
9. `application-id`

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>enable</code>  <b>Example:</b> Router> <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"><li>• Enter your password if prompted.</li></ul>
Step 2	<code>configure terminal</code>  <b>Example:</b> Router# <code>configure terminal</code>	Enters global configuration mode.
Step 3	<code>cable multicast group-encryption</code> <code>number</code> <code>algorithm</code> <code>56bit-des</code>  <b>Example:</b> Router(config-mqos)# <code>cable multicast</code> <code>group-encryption 12 algorithm 56bit-des</code>	(Optional) Specifies an encryption number and encryption type of a specific cable multicast QoS group encryption profile. The valid range is 1–255.  The algorithm keyword and 56bit-des argument specify that the data encryption standard (DES) is 56 bits. <ul style="list-style-type: none"><li>• <code>enable</code>—Enables encryption and specifies the encryption number that can be applied to a specific cable multicast QoS group. The valid range is 1–255.</li><li>• <b>algorithm 56bit-des</b>—Specifies that the data encryption standard (DES) is 56 bits.</li></ul>

Command or Action	Purpose
<p><b>Step 4</b></p> <pre><b>cable multicast group-qos</b> <i>number scn</i> <i>service-class-name control {single   aggregate</i> <i>[limit max-sessions]}</i></pre> <p><b>Example:</b>  Router(config-mqos)# cable multicast group-qos 5 scn name1 control single</p>	<p>(Optional) Configures a QoS profile that can be applied to a multicast QoS group.</p> <ul style="list-style-type: none"> <li><b>number</b>—Specifies the QoS profile number that can be applied to a multicast QoS group. The valid range is 1–255.</li> <li><b>scn</b>—Specifies the service class name for the QoS profile service class.</li> <li><b>control</b>—Specifies the type of control to the service flow: <ul style="list-style-type: none"> <li><b>single</b>—Specifies that a separate service flow is created for each session.</li> <li><b>aggregate</b>—Specifies that service flows are grouped for sessions in the same MQoS group.</li> </ul> </li> <li><b>limit</b>—(Optional) Specifies the Internet Group Management Protocol (IGMP) session limit for aggregate service flows. The valid range is 1–255.</li> </ul>
<p><b>Step 5</b></p> <pre><b>cable multicast qos group</b> <i>id priority 255</i> <i>global</i></pre> <p><b>Example:</b>  Router(config)# cable multicast qos group 2 priority 255 global</p>	<p>Configures a default multicast QoS group and enters multicast QoS configuration mode.</p> <ul style="list-style-type: none"> <li><b>id</b>—The number of the cable multicast QoS group. The valid range is 1–255.</li> <li><b>priority 255</b>—The priority of the cable multicast QoS group is given the highest priority value of 255.</li> <li><b>global</b>—Specifies that the multicast QoS group configuration is applied to all cable interfaces.</li> </ul>
<p><b>Step 6</b></p> <pre><b>session-range</b> 224.0.0.0 224.0.0.0</pre> <p><b>Example:</b>  Router(config-mqos)# session-range 224.0.0.0 224.0.0.0</p>	<p>Specifies the session-range IP address and IP mask of the default multicast QoS group. By entering 224.0.0.0 for the IP address and the IP mask you cover all possible multicast sessions.</p>
<p><b>Step 7</b></p> <pre><b>tos</b> <i>low-byte high-byte mask</i></pre> <p><b>Example:</b>  Router(config-mqos)# tos 1 6 15</p>	<p>(Optional) Specifies the minimum type of service (ToS) data bytes, maximum ToS data bytes, and mask for the default multicast QoS group. The valid range for each is 0–255.</p>
<p><b>Step 8</b></p> <pre><b>vrf</b> <i>name</i></pre> <p><b>Example:</b>  Router(config-mqos)# vrf name1</p>	<p>Specifies the name of the virtual routing and forwarding (VRF) instance.</p>
<p><b>Step 9</b></p> <pre><b>application-id</b> <i>number</i></pre> <p><b>Example:</b>  Router(config-mqos)# application-id 5</p>	<p>(Optional) Specifies the application identification number of the multicast QoS group. This value is configured to enable admission control to the multicast QoS group. The valid range is 1–65535.</p>

## Verifying Configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature

To verify the configuration of the Multicast VPN and DOCSIS 3.0 Multicast QoS Support feature, use the **show** commands described below.

- To show the configuration parameters for multicast sessions on a specific bundle, use the **show interface bundle multicast-sessions** command as shown in the following example:

```
Router# show interface bundle 1 multicast-sessions
```

```
Multicast Sessions on Bundle1
```

Group	Interface	GC	SAID	SFID	GQC	GEN	RefCount	GC-Interface	State
234.1.1.45	Bundle1.1	1	8193	---	1	5	1	Bundle1	ACTIVE
234.1.1.46	Bundle1.1	1	8193	---	1	5	1	Bundle1	ACTIVE
234.1.1.47	Bundle1.1	1	8193	---	1	5	1	Bundle1	ACTIVE

```
Aggregate Multicast Sessions on Bundle1
```

```
Aggregate Sessions for SAID 8193 GQC 1 CurrSess 3
```

Group	Interface	GC	SAID	SFID	AggGQC	GEN	RefCount	GC-Interface
234.1.1.45	Bundle1.1	1	8193	---	1	5	1	Bundle1
234.1.1.46	Bundle1.1	1	8193	---	1	5	1	Bundle1
234.1.1.47	Bundle1.1	1	8193	---	1	5	1	Bundle1

- To show the configuration parameters for multicast sessions on a specific cable, use the **show interface cable multicast-sessions** command as shown in the following example:

```
Router# show interface cable 7/0/0 multicast-sessions
```

```
Default Multicast Service Flow 3 on Cable7/0/0
```

```
Multicast Sessions on Cable7/0/0
```

Group	Interface	GC	SAID	SFID	GQC	GEN	RefCount	GC-Interface	State
234.1.1.45	Bundle1.1	1	8193	24	1	5	1	Bundle1	ACTIVE
234.1.1.46	Bundle1.1	1	8193	24	1	5	1	Bundle1	ACTIVE
234.1.1.47	Bundle1.1	1	8193	24	1	5	1	Bundle1	ACTIVE

```
Aggregate Multicast Sessions on Cable7/0/0
```

```
Aggregate Sessions for SAID 8193 SFID 24 GQC 1 CurrSess 3
```

Group	Interface	GC	SAID	SFID	AggGQC	GEN	RefCount	GC-Interface
234.1.1.45	Bundle1.1	1	8193	24	1	5	1	Bundle1
234.1.1.46	Bundle1.1	1	8193	24	1	5	1	Bundle1
234.1.1.47	Bundle1.1	1	8193	24	1	5	1	Bundle1

- To show the MSAID multicast group subinterface mapping, use the **show interface cable modem** command as shown in the following example:

```
Router# show interface cable 6/1/0 modem
```

SID	Priv	Type	State	IP address	method	MAC address	Dual IP
9	11	modem	online(pt)	101.1.0.6	dhcp	0006.28f9.8c79	N
9	11	host	unknown	111.1.1.45	dhcp	0018.1952.a859	N
10	10	modem	online(pt)	101.1.0.5	dhcp	0006.5305.ac19	N
10	10	host	unknown	111.1.0.3	dhcp	0018.1952.a85a	N
13	10	modem	online(pt)	101.1.0.3	dhcp	0014.f8c1.fdlc	N
8195	10	multicast	unknown	224.1.1.51	static	0000.0000.0000	N
8195	10	multicast	unknown	224.1.1.49	static	0000.0000.0000	N

```
8195 10 multicast unknown 224.1.1.50 static 0000.0000.0000 N
```

## Configuration Examples for the Multicast VPN and DOCSIS 3.0 Multicast QoS Support Feature

This section provides the following configuration examples:

- [Configuring Group QoS and Group Encryption Profiles: Example, page 928](#)
- [Configuring a QoS Group: Example, page 928](#)

### Configuring Group QoS and Group Encryption Profiles: Example



#### Note

To add group QoS and group encryption profiles to a QoS group, you must configure each profile first before configuring the QoS group.

In the following example, QoS profile 3 and encryption profile 35 are configured.

```
configure terminal
cable multicast group-qos 3 scn name1 control single
cable multicast group-encryption 35 algorithm 56bit-des
```

### Configuring a QoS Group: Example

In the following example, QoS group 2 is configured with a priority of 6 and global application. To QoS group 2, QoS profile 3 and encryption profile 35 are applied. Other parameters are configured for QoS group 2 including application type, session range, ToS, and VRF.

```
cable multicast qos group 2 priority 6 global
group-encryption 35
group-qos 3
session-range 224.10.10.01 255.255.255.254
tos 1 6 15
vrf vrf-name1
application-id 44
```

## Where to Go Next

For further information on the commands required to configure, maintain, and troubleshoot Cisco uBR7200 series universal broadband routers, Cisco uBR10012 series universal broadband routers, and Cisco cable modems, see the *Cisco IOS CMTS Cable Command Reference* at:

[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)

## Additional References

The following sections provide references related to the Multicast VPN and DOCSIS 3.0 Multicast QoS Support feature.

### Related Documents

Related Topic	Document Title
CMTS cable commands	<i>Cisco IOS CMTS Cable Command Reference</i> <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>
DOCSIS 1.1 as it relates to Cisco CMTS	<i>Cisco IOS CMTS Cable Software Configuration Guide</i> <a href="http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/12_2sc/cbl_12_2sc_book.html">http://www.cisco.com/en/US/docs/ios/cable/configuration/guide/12_2sc/cbl_12_2sc_book.html</a>

### 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
No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by 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: <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a>

### RFCs

RFC	Title
RFC 2236	<i>Internet Group Management Protocol, Version 2</i>

## 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><a href="http://www.cisco.com/techsupport">http://www.cisco.com/techsupport</a></p>

# Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

Table 2 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 2 lists only the Cisco IOS software release that introduced support for a given feature in a given Cisco IOS software release. Unless noted otherwise, subsequent releases of that Cisco IOS software release also support that feature.

**Table 2** Feature Information for Multicast VPN and DOCSIS 3.0 Multicast QoS Support

Feature Name	Releases	Feature Information
Multicast VPN and DOCSIS 3.0 Multicast QoS Support	12.2(33)SCA	<p>Enhanced multicast new features include configuration of a QoS group to include QoS, encryption, VRF, ToS, application type, and session range parameters.</p> <p>The following commands were introduced or modified by this feature:</p> <ul style="list-style-type: none"> <li>• <b>application-id</b></li> <li>• <b>cable application-type include</b></li> <li>• <b>cable multicast group-encryption</b></li> <li>• <b>cable multicast group-qos</b></li> <li>• <b>cable multicast qos group</b></li> <li>• <b>session-range</b></li> <li>• <b>show interface bundle multicast-sessions</b></li> <li>• <b>show interface cable modem</b></li> <li>• <b>show interface cable multicast-sessions</b></li> <li>• <b>tos (multicast qos)</b></li> <li>• <b>vrf (multicast qos)</b></li> </ul>

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Pulse, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, AllTouch, 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, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Fast Step, Follow Me Browsing, FormShare, GainMaker, GigaDrive, HomeLink, iLYNX, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers,

Networking Academy, Network Registrar, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, 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. (0908R)

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.

© 2008 Cisco Systems, Inc. All rights reserved.