



# Advanced-mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS

---

**OL-11166-01**

**First Published: July 24, 2006**

**Last Published: January 15, 2009**

Cisco IOS Release 12.3(17a)BC2 introduces certified support for advanced-mode DOCSIS Set-Top Gateway (DSG) Issue 1.2. DSG Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™, to include the following enhancements:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*, CM-SP-DSG-I05-050812  
<http://www.cablelabs.com/specifications/archives/CM-SP-DSG-I05-050812.pdf>
- The set-top box dynamically learns the overall environment from the Cisco Cable Modem Termination System (CMTS), to include MAC address, traffic management rules, and classifiers.
- DSG 1.2 introduces support for the DOCS-DSG-IF MIB.

Cisco Advanced-mode DSG 1.2 is certified by CableLabs™, and is a powerful tool in support of latest industry innovations. Advanced-mode DSG 1.2 offers substantial support for enhanced DOCSIS implementation in the Broadband Cable environment. The set-top box dynamically learns the overall environment from the Cisco Cable Modem Termination System (CMTS), to include MAC address, traffic management rules, and classifiers.

This document describes the configuration, monitoring, troubleshooting, examples, and command-line interface enhancements supporting DSG Issue 1.2 on the Cisco CMTS. Refer to the “[Additional References](#)” section on page 34 for additional information about Management Information Base (MIB) support for DSG 1.2, and earlier versions of DSG.

## **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.



---

**Americas Headquarters:**

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

# Contents

- [Prerequisites for DSG Issue 1.2](#)
- [Restrictions for DSG Issue 1.2](#)
- [Information About DSG Issue 1.2](#)
- [How to Configure Advanced-mode DSG Issue 1.2](#)
- [Configuring Additional Features for Advanced-mode DOCSIS Set-Top Gateway 1.2 on the Cisco CMTS](#)
- [How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature](#)
- [Configuration Examples for DSG Issue 1.2](#)
- [Additional References](#)
- [Glossary](#)

## Prerequisites for DSG Issue 1.2

Cisco IOS Release 12.3(17a)BC2 introduces support for advanced-mode DSG 1.2 on the Cisco uBR7246VXR router and the Cisco uBR10012 router.

- The Cisco uBR7246VXR router requires 128 MB of RAM, and does not support the NPE-150 network processing engine in Cisco IOS Release 12.3(17a)BC2. The Cisco NPE-200 or a later network processing engine is required.
- The Cisco uBR10012 router supports Advanced-mode DSG 1.2 with the PRE2 performance routing engine module.

## Restrictions for DSG Issue 1.2

Cisco IOS release 12.3(17a)BC2, or a later 12.3BC release, must be installed on the Cisco universal broadband router. This section contains additional restrictions that are specific to Advanced-mode DSG 1.2 on the Cisco CMTS.

- [Command-line Interface Restrictions](#)
- [DSG Configuration File Transfer Operations](#)
- [Multicast Configuration Restrictions](#)
- [NAT for DSG Unicast-only Mapping](#)
- [PIM and SSM for Multicast](#)

## Command-line Interface Restrictions

The following DSG configuration commands, supported prior to Cisco IOS Releases 12.3(17a)BC2, are not supported for advanced-mode DSG 1.2. Refer to the [“Additional References” section on page 34](#) for information relating to DSG 1.1 and earlier supporting commands.

- **cable downstream dsg rule *rule-id* clients *clnt-list-id* tunnel *tunnel-id***
- **cable downstream dsg rule *rule-id* priority *priority***
- **cable downstream dsg rule vendor-param *vsif-grp-id***
- **cable downstream dsg rule *rule-id* uuid *ucid-num***
- **cable downstream dsg rule *rule-id* cfr *cfr-index***
- **cable downstream dsg rule *rule-id* disable**

## DSG Configuration File Transfer Operations

DSG 1.2 does not support the copying of a DSG configuration file from a TFTP server, file system, or bootflash to the running configuration.

Previously, with DSG 1.1, when copying the DSG configuration file from a file system or TFTP server to the running configuration, DSG rule error checking may disable a previously configured and valid DSG tunnel configuration. This issue has not been observed in DSG 1.1 when loading the DSG configuration file from the startup configuration, as during a reload.

## Multicast Configuration Restrictions

As with earlier versions of DSG Issues 0.9 and 1.0, IP multicasting must be configured for correct operation of Advanced-mode DSG 1.2. Specifically, IP multicast routing must be set in global configuration. Also, IP PIM must be configured on all WAN interfaces and cable interfaces that are to carry multicast traffic.

Advanced-mode DSG 1.2 creates changes to the running configuration, requiring the **ip igmp static-group** command for each multicast group that passes DSG traffic. For this reason, this configuration cannot be deleted in manual fashion once set, in order to sustain normal DSG 1.2 operations.

Refer to the [“Configuring Global Tunnel Group Settings for Advanced-mode DSG 1.2” section on page 5](#) and the [“Configuring IP Multicast Operations” section on page 14](#) for additional Multicast information and global configurations supporting DSG.

## NAT for DSG Unicast-only Mapping

Advanced-mode DSG 1.2 supports multicast IP addressing. However, DSG 1.2 also supports unicast IP destination addresses. On the Cisco uBR7246VXR router, DSG 1.2 support is provided with the configuration of Network Address Translation (NAT) on the router, to include these settings:

- WAN interface(s) are configured with the **ip nat outside** command.
- Cable interface(s) are configured with the **ip nat inside** command.
- For each mapping, additional configuration includes the IP NAT inside source static multicast IP address and the unicast IP address.

The unicast IP address is the unicast destination IP address of the DSG packets arriving at the Cisco CMTS. The multicast IP address is the new destination IP address that is configured to map to one or a set of DSG tunnel(s).

## PIM and SSM for Multicast

When using Source Specific Multicast (SSM) operation in conjunction with advanced-mode DSG 1.2, the following system-wide configuration command must be specified:

- **ip pim ssm**

Refer to the [“Configuring IP Multicast Operations” section on page 14](#).

## Subinterfaces

Advanced-mode DSG 1.2 does not support sub-interfaces on the Cisco CMTS in Cisco IOS release 12.3(17a)BC2.

## Information About DSG Issue 1.2

Advanced-mode DSG 1.2 offers substantial upgrades over advanced-mode DSG 1.1 and earlier Basic DSG on the Cisco CMTS. DSG 1.2 offers these new or enhanced capabilities:

- Advanced-mode DSG Client and Agent modes
- Advanced-mode MIBs supporting DSG 1.2, including the DOCS-DSG-IF-MIB
- Advanced-mode tunnels with increased security
- Cable Interface Bundling through Virtual Interface Bundling
- Downstream Channel Descriptor
- IP Multicast support
- Quality of Service (QoS)

### DSG 1.2 Clients

DSG 1.2 supports the DSG client and agent functions outlined by the CableLabs™ *DOCSIS Set-top Gateway (DSG) Interface Specification*, CM-SP-DSG-I05-050812.

### DSG 1.2 Agents

DSG 1.2 supports the DSG client and agent functions outlined by the CableLabs™ *DOCSIS Set-top Gateway (DSG) Interface Specification*, CM-SP-DSG-I05-050812.

## How to Configure Advanced-mode DSG Issue 1.2

Advanced-mode DSG Issue 1.2 entails support for DSG tunnel configuration, to include global, WAN-side, and interface-level settings in support of Multicast. This section contains the following procedures supporting A-DSG 1.2 in Cisco IOS Release 12.3(17a)BC2, and later Cisco IOS releases supporting Cisco Universal Broadband routers:

- [Configuring Global Tunnel Group Settings for Advanced-mode DSG 1.2](#)
- [Configuring the DSG Client Settings for Advanced-mode DSG 1.2](#)
- [Configuring Downstream DSG 1.2 Settings for Advanced-mode DSG 1.2](#)
- [Configuring IP Multicast Operations](#)
- [Configuring NAT to Support Unicast Messaging \(optional\)](#)
- [Configuring WAN Interfaces for MultiCast Operations](#)
- [Configuring a Standard IP Access List for Packet Filtering \(Optional\)](#)
- [Configuring a Standard IP Access List for Multicast Group Filtering \(Optional\)](#)
- [Displaying Global Configurations for Advanced-Mode DSG 1.2](#)

# Configuring Global Tunnel Group Settings for Advanced-mode DSG 1.2

This procedure configures global and interface-level commands on the Cisco CMTS to enable DSG 1.2 tunnel groups. Later DSG 1.2 configurations build on these settings.

## Global DSG 1.2 Tunnel Settings

This procedure sets and enables global configurations to support both DSG 1.2 clients and agents. Additional procedures provide additional settings for DSG 1.2 clients and agents.

## Prerequisites

Cisco IOS Release 12.3(17a)BC or a later DSG-supporting release must be installed previously on the Cisco CMTS.

## Restrictions

Cisco IOS Release 12.3(17a)BC or a later DSG-supporting release must be installed previously on the Cisco CMTS.

## SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **[no] cable dsg tg <group-id> channel <channel-id> [priority <priority>] [enable | disable]**
4. **[no] cable dsg tg <group-id> channel <channel-id> [ucid <u1>] | [ <u1> <u2> <un> ]**
5. **[no] cable dsg tg <group-id> channel <channel-id> [ vendor-param <vendor-group-id> ]**
6. **[no] cable dsg vendor-param <group-id> vendor <vendor-id> oui <oui> value <value-in-TLV>**
7. **[no] cable dsg chan-list <list-index> index <entry-index> freq <freq>**
8. **[no] cable dsg timer <index> [Tdsg1 <Tdsg1>] | [Tdsg2 <Tdsg2>] | [Tdsg3 <Tdsg3>] | [Tdsg4 <Tdsg4>]**
9. **Ctrl-Z**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> 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>  <b>Example:</b> Router# configure terminal Router(config)#	Enters global configuration mode.

Command or Action	Purpose
<p><b>Step 3</b></p> <pre>[no] cable dsg tg &lt;group-id&gt; channel &lt;channel-id&gt; [priority &lt;priority&gt;] [enable   disable]</pre> <p><b>Example:</b> Router(config)# cable dsg tg 1 channel 1 priority 1 enable</p>	<p>Command allows the association of a group of tunnels to one or more downstream interfaces on the Cisco CMTS.</p> <ul style="list-style-type: none"> <li>• <b>tg</b>—DSG tunnel-group id</li> <li>• <b>channel</b>—downstream channel index</li> <li>• <b>priority</b>—DSG Rule priority</li> <li>• <b>enable</b>—Enable tunnel-group</li> <li>• <b>disable</b>—Disable tunnel-group</li> </ul>
<p><b>Step 4</b></p> <pre>[no] cable dsg tg &lt;group-id&gt; channel &lt;channel-id&gt; [ ucid &lt;u1&gt; ]   [ &lt;u1&gt; &lt;u2&gt; &lt;un&gt; ]</pre> <p><b>Example:</b> Router(config)# cable dsg tg 1 channel 1 ucid 1</p>	<p>Sets the upstream channel or channels to which the DSG 1.2 tunnel applies.</p> <ul style="list-style-type: none"> <li>• <b>ucid</b>—List of Upstream channel ID for which the rule applies</li> </ul>
<p><b>Step 5</b></p> <pre>[no] cable dsg tg &lt;group-id&gt; channel &lt;channel-id&gt; [ vendor-param &lt;vendor-group-id&gt; ]</pre> <p><b>Example:</b> Router(config)# cable dsg tg 1 channel 1 vendor-param 1</p>	<p>Sets the vendor-specific parameters for upstream DSG 1.2 channels.</p> <ul style="list-style-type: none"> <li>• <b>vendor-param</b>—Vendor parameter index for the vendor specific parameters</li> </ul>
<p><b>Step 6</b></p> <pre>cable dsg vendor-param &lt;group-id&gt; vendor &lt;vendor-index&gt; oui &lt;oui&gt; value &lt;value-in-TLV&gt;</pre> <p><b>Example:</b> Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB</p>	<p>Configures vendor-specific parameters for A-DSG 1.2. To remove this configuration from the Cisco CMTS, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li>• <b>vendor-param</b>—Sets the DSG vendor parameter group identifier.</li> <li>• <b>vendor</b>—DSG vendor parameters vendor index setting.</li> <li>• <b>oui</b>—DSG vendor parameters vendor OUI setting. Includes the 0803&lt;oui&gt; tlv in the VSIF.</li> <li>• <b>value</b>—DSG vendor parameters vendor value setting.</li> </ul>
<p><b>Step 7</b></p> <pre>cable dsg chan-list &lt;list-index&gt; index &lt;entry-index&gt; freq &lt;freq&gt;</pre> <p><b>Example:</b> Router(config)# cable dsg chan-list 1 index 1 freq 47000000</p>	<p>Configures the A-DSG 1.2 downstream channel list. The channel list is a list of DSG channels (downstream frequencies) that set-top boxes can search to find the DSG tunnel appropriate for their operation. To remove the A-DSG 1.2 channel list from the Cisco CMTS, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li>• <b>list-index</b>—an index used to indicate a group of channels (downstream frequencies) to include in the DCD messages for an interface.</li> <li>• <b>entry-index</b>—DSG channel frequency entry index.</li> <li>• <b>freq</b>—Center frequency of the downstream channel in Hz. This value must be a multiple of 62500 Hz.</li> </ul>

	Command or Action	Purpose
Step 8	<p><b>Command:</b></p> <pre>cable dsg timer &lt;index&gt; [Tdsg1 &lt;Tdsg1&gt;]   [Tdsg2 &lt;Tdsg2&gt;]   [Tdsg3 &lt;Tdsg3&gt;]   [Tdsg4 &lt;Tdsg4&gt;]</pre> <p><b>Example:</b></p> <pre>Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4</pre>	<p>Configures the A-DSG 1.2 timer entry to be associated to the downstream channel, and encoded into the DCD message. To remove the cable DSG timer from the Cisco CMTS, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li><i>index</i>—Alphanumeric index identifier</li> <li><b>Tdsg1</b> &lt;Tdsg1&gt;—DSG Initialization Timeout (Tdsg1) setting</li> <li><b>Tdsg2</b> &lt;Tdsg2&gt;—DSG Operational Timeout (Tdsg2) setting</li> <li><b>Tdsg3</b> &lt;Tdsg3&gt;—DSG Two-Way Retry Timer (Tdsg3) setting</li> <li><b>Tdsg4</b> &lt;Tdsg4&gt;—DSG One-Way Retry Timer (Tdsg4) setting</li> </ul>
Step 9	<p><b>Command:</b></p> <pre>Ctrl-Z</pre> <p><b>Example:</b></p> <pre>Router(config)# Ctrl^Z Router#</pre>	<p>Returns to privileged EXEC mode.</p>

## Examples

The following example illustrates global upstream configurations implemented with the above commands:

```
Router> enable
Router# configure terminal
Router(config)# cable dsg tg 1 channel 1 priority 1 enable
Router(config)# cable dsg tg 1 channel 1 ucid 1
Router(config)# cable dsg tg 1 channel 1 vendor-param 1
Router(config)# Ctrl^Z
Router#
```

## Troubleshooting Tips

Refer to **debug** and **show** commands in the [“How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature”](#) section on page 24.

## What to Do Next

Refer to additional procedures in this section to complete the configuration of Advanced-mode DSG 1.2 on the Cisco CMTS:

- [Configuring the DSG Client Settings for Advanced-mode DSG 1.2](#)
- [Configuring Downstream DSG 1.2 Settings for Advanced-mode DSG 1.2](#)
- [Configuring Additional Features for Advanced-mode DOCSIS Set-Top Gateway 1.2 on the Cisco CMTS](#)

## Configuring the DSG Client Settings for Advanced-mode DSG 1.2

Once the global configurations and DSG client configurations are set for DSG 1.2 on the Cisco CMTS, use the following procedure to continue DSG 1.2 client configurations.

### Prerequisites

Cisco IOS Release 12.3(17a)BC or a later DSG-supporting release must be installed previously on the Cisco CMTS.

### Restrictions

Cisco IOS Release 12.3(17a)BC or a later DSG-supporting release must be installed previously on the Cisco CMTS.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **[no] cable dsg client-list <client-list-id> id-index <id> { application-id <app-id> | ca-system-id <sys-id> | mac-addr <mac-addr> | broadcast [broadcast-id] }**
4. **[no] cable dsg client-list <client-list-id> id-index <id> [ vendor-param <vendor-group-id>]**
5. **[no] cable dsg tunnel <tunnel id> mac\_addr <mac addr> tg <tunnel-group> clients <client-list-id> [enable | disable]**
6. **[no] cable dsg cfr <cfr index> dest\_ip <ipaddr> [tunnel <tunnel index>] | [dest-port <start> <end>] | [priority <priority>] | [src-ip <ipaddr> src-prefix-len <length>] | [enable | disable] [in-dcd <yes | no>]**
7. **Ctrl-Z**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>enable</b>  <b>Example:</b> 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>  <b>Example:</b> Router# configure terminal Router(config)#	Enters global configuration mode.



Command or Action	Purpose
<p><b>Step 3</b></p> <pre>[no] cable dsg client-list &lt;client-list-id&gt; id-index &lt;id&gt; { application-id &lt;app-id&gt;   ca-system-id &lt;sys-id&gt;   mac-addr &lt;mac-addr&gt;   broadcast [broadcast-id] }</pre> <p><b>Example:</b> Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd</p>	<p>Sets the DSG client parameters. Command is changed from earlier Cisco IOS Releases, and for DSG 1.2, this command specifies the optional broadcast ID to client ID broadcast type and vendor specific parameter index.</p> <ul style="list-style-type: none"> <li>• <b>client-list</b>—Sets the DSG Client list ID index, with argument <i>client-list-id</i></li> <li>• <b>id-index</b>—Sets the index to use for DSG Client ID settings, with index identifier value specified with <i>id</i>.</li> <li>• <b>application-id</b>—Sets the DSG Client type Application ID, specified by <i>app-id</i>.</li> <li>• <b>ca-system-id</b>—Sets the DSG Client type CA system ID, with value provided for <i>sys-id</i>.</li> <li>• <b>mac-addr</b>—Sets the DSG Client type MAC address with <i>mac-addr</i> value.</li> <li>• <b>broadcast</b>—Sets the DSG Client type broadcast identifier with the <i>broadcast-id</i> value.</li> </ul>
<p><b>Step 4</b></p> <pre>[no] cable dsg client-list &lt;client-list-id&gt; id-index &lt;id&gt; [ vendor-param &lt;vendor-group-id&gt; ]</pre> <p><b>Example:</b> Router(config-if)# cable dsg client-list 1 id-index 1 vendor-param 1</p>	<p>Sets vendor-specific parameters for the DSG client.</p> <ul style="list-style-type: none"> <li>• <b>client-list</b>—Sets the DSG Client list ID index, with argument <i>client-list-id</i>.</li> <li>• <b>id-index</b>—Sets the index to use for DSG Client ID settings, with index identifier value specified with <i>id</i>.</li> <li>• <b>vendor-param</b>—Sets the vendor parameter index for the vendor-specific parameters, and applied to the specified vendor group.</li> </ul>
<p><b>Step 5</b></p> <pre>[no] cable dsg tunnel &lt;tunnel id&gt; mac_addr &lt;mac addr&gt; tg &lt;tunnel-group&gt; clients &lt;client-list-id&gt; [enable   disable]</pre> <p><b>Example:</b> Router(config)# cable dsg tunnel mac-addr abcd.abcd.abcd tg 1 clients 1 enable</p>	<p>A DSG tunnel entry is configured using the following CLI. This CLI is changed to associate a tunnel-group and client-list ID to DSG tunnel. Also, an optional QoS service class name can be associated to the tunnel.</p> <ul style="list-style-type: none"> <li>• <b>tunnel</b>—Specifies the DSG tunnel to which this client setting applies, using the <i>tunnel id</i> identifier.</li> <li>• <b>mac-addr</b>—Sets the DSG Client type MAC address with <i>mac-addr</i> value.</li> <li>• <b>tg</b>—Sets the tunnel group associated with this DSG tunnel, identified with the <i>tunnel-group</i> value.</li> <li>• <b>clients</b>—Sets the client list to which this configuration applies, specified with the <i>client-list id</i> value.</li> <li>• <b>disable</b>—Disables the DSG tunnel.</li> <li>• <b>enable</b>—Enables the DSG tunnel.</li> </ul>

Command or Action	Purpose
<p><b>Step 6</b></p> <pre>[no] cable dsg cfr &lt;cfr index&gt; dest_ip &lt;ipaddr&gt; [tunnel &lt;tunnel index&gt;]   [dest-port &lt;start&gt; &lt;end&gt;]   [priority &lt;priority&gt;]   [src-ip &lt;ipaddr&gt; src-prefix-len &lt;length&gt;]   [enable   disable] [in-dcd &lt;yes   no&gt;]</pre> <p><b>Example:</b></p> <pre>Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority 2 src-ip 1.11.37.0 src-prefix-len 24 enable</pre>	<p>Specifies the DSG classifier index, with optional support for the DCD parameter, indicating whether or not to include the classifier in the DCD message. The <b>no</b> form of this command removes previously specified settings.</p> <ul style="list-style-type: none"> <li>• <b>cfr</b>—Sets the classifier index with the <i>cfr index</i> value.</li> <li>• <b>dest-ip</b>—Sets the destination IP address.</li> <li>• <b>dest-ports</b>—Sets the destination TCP/UDP ports range.</li> <li>• <b>disable</b>—Disables the classifier.</li> <li>• <b>enable</b>—Enables the classifier.</li> <li>• <b>priority</b>—Sets the classifier priority with the specified <i>priority</i> value.</li> <li>• <b>src-ip</b>—Sets the source IP address.</li> <li>• <b>tunnel</b>—Sets the tunnel index with the specified <i>tunnel index</i> value.</li> <li>• <b>in-dcd</b>—Keyword specifies whether or not the classifier is included in the DCD message.</li> </ul>
<p><b>Step 7</b></p> <p><b>Ctrl-Z</b></p> <p><b>Example:</b></p> <pre>Router(config)# Ctrl^Z Router#</pre>	<p>Returns to privileged EXEC mode.</p>

## Examples

The following example illustrates global configuration of DSG 1.2 on the Cisco CMTS, supporting the specified settings shown. Global configuration may vary, but this example is representative of a typical configuration:

```
Router(config)# cable dsg vendor-param 1 vendor 1 oui 000001 value 010101
Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd
Router(config)# cable dsg tg 1 channel 1
Router(config)# cable dsg tunnel 1 mac-addr 0abc.0abc.0abc tg 1 clients 1
Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority
2 src-ip 1.11.37.0 src-prefix-len 24
Router(config)# cable dsg timer 1 Tdsg1 4 Tdsg2 600 Tdsg3 300 Tdsg4 1800
Router(config)# cable dsg chan-list 1 index 1 freq 471000000
```

## Troubleshooting Tips

Refer to **debug** and **show** commands in the [“How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature”](#) section on page 24.

## What to Do Next

Refer to additional procedures in this section to complete the configuration of Advanced-mode DSG 1.2 on the Cisco CMTS:

- [Configuring Downstream DSG 1.2 Settings for Advanced-mode DSG 1.2](#)

## Configuring Downstream DSG 1.2 Settings for Advanced-mode DSG 1.2

Once the global and client configurations are set for DSG 1.2 on the Cisco CMTS, use the following procedure to continue with DSG 1.2 downstream configurations.

### Prerequisites

Cisco IOS Release 12.3(17a)BC or a later DSG-supporting release must be installed previously on the Cisco CMTS.

### Restrictions

Cisco IOS Release 12.3(17a)BC or a later DSG-supporting release must be installed previously on the Cisco CMTS.

### SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface cable** {slot/port | slot/subslot/port}
4. **[no] cable downstream dsg tg** <group-id> **channel** <channel-id>
5. **[no] cable downstream dsg chan-list** <list-index>

6. `[no] cable downstream dsg timer <timer-index>`
7. `[no] cable downstream dsg vendor-param <vsif-grp-id>`
8. `[no] cable downstream dsg [ dcd-enable | dcd-disable ]`
9. **Ctrl-Z**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><code>enable</code></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><code>configure terminal</code></p> <p><b>Example:</b> Router# configure terminal Router(config)#</p>	<p>Enters global configuration mode.</p>
Step 3	<p><code>interface cable {slot/port   slot/subslot/port}</code></p> <p><b>Example:</b> Router(config)# interface cable 8/1/1 Router(config-if)#</p>	<p>Enters interface configuration mode.</p> <ul style="list-style-type: none"> <li>• On the Cisco uBR7200 series router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.</li> <li>• On the Cisco uBR10012 router, the following are valid values: <ul style="list-style-type: none"> <li>– <i>slot</i> = 5 to 8</li> <li>– <i>subslot</i> = 0 or 1</li> <li>– <i>port</i> = 0 to 4 (depending on the cable interface)</li> </ul> </li> </ul>
Step 4	<p><code>[no] cable downstream dsg tg &lt;group-id&gt; channel &lt;channel-id&gt;</code></p> <p><b>Example:</b> Router(config-if)# cable downstream dsg tg 1 channel 1</p>	<p>Associates the DSG tunnel-group to the downstream interface. To remove this setting, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li>• <b>tg</b>—DSG tunnel-group id</li> <li>• <b>channel</b>—downstream channel index</li> </ul>
Step 5	<p><code>[no] cable downstream dsg chan-list &lt;list-index&gt;</code></p> <p><b>Example:</b> Router(config-if)# cable downstream dsg chan-list 2</p>	<p>Associates the A-DSG channel list entry to a downstream channel, to be included in the DCD message. To remove this setting, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li>• <b>chan-list</b>—Sets the downstream A-DSG 1.1 channel list.</li> <li>• <i>list-index</i>—This is an integer between 1 and 65535.</li> </ul>
Step 6	<p><code>[no] cable downstream dsg timer &lt;timer-index&gt;</code></p> <p><b>Example:</b> Router(config-if)# cable downstream dsg timer 3</p>	<p>Associates the DSG timers entry to a downstream channel, to be included in the DCD message. To remove this setting, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li>• <i>timer-index</i>—This is an integer between 1 and 65535.</li> </ul>

	Command or Action	Purpose
Step 7	<pre>[no] cable downstream dsg vendor-param &lt;vsif-grp-id&gt;</pre> <p><b>Example:</b> Router(config-if)# cable downstream dsg vendor-param 2</p>	<p>Associates A-DSG vendor parameters to a downstream, to be included in the DCD message. To remove this configuration from the Cisco CMTS, use the <b>no</b> form of this command.</p> <ul style="list-style-type: none"> <li><i>vsif-grp-id</i>—Value identifies vendor-specific parameters by the specified ID.</li> </ul>
Step 8	<pre>[no] cable downstream dsg [ dcd-enable   dcd-disable ]</pre> <p><b>Example:</b> Router(config-if)# cable downstream dsg dcd-enable</p>	<p>Enables DCD messages to be sent on a downstream channel. This command is used when there are no enabled rules or tunnels for A-DSG currently on the Cisco CMTS. To disable DCD messages, use the <b>disable</b> form of this command.</p>
Step 9	<pre>Ctrl^Z</pre> <p><b>Example:</b> Router(config-if)# Ctrl^Z Router#</p>	<p>Returns to privileged EXEC mode.</p>

## Examples

The following example illustrates downstream settings configured for DSG 1.2 on the Cisco CMTS:

```
cable downstream dsg chan-list 1
cable downstream dsg timer 1
cable downstream dsg tg 1 channel 1
```

The following example illustrates DSG rules associated with the same A-DSG tunnel and the same list of classifiers.

```
cable dsg cfr 1 dest-ip 224.2.1.1 tunnel 1
cable dsg cfr 2 dest-ip 224.2.1.2 tunnel 1
cable dsg cfr 3 dest-ip 224.2.1.3 tunnel 1
.
.
.
```

### Downstream 1

```
cable downstream dsg rule 2 clients 1 tunnel 1
cable downstream dsg rule 2 cfr 2 3
.
.
.
```

### Downstream 2

This setting below is the same tunnel as rule 2 of downstream 1.

```
cable downstream dsg rule 1 clients 1 tunnel 1
.
.
.
```

The setting below must be the same classifier list as rule 2 of downstream 1

```
cable downstream dsg rule 1 cfr 2 3
.
.
.
```

## Troubleshooting Tips

Refer to **debug** and **show** commands in the “[How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature](#)” section on page 24.

## What to Do Next

Refer to additional configuration options and monitoring procedures in this document.

# Configuring Additional Features for Advanced-mode DOCSIS Set-Top Gateway 1.2 on the Cisco CMTS

See the following sections for how to enable, configure, disable, and monitor the Advanced-mode DOCSIS Set-Top Gateway feature:

- [Configuring IP Multicast Operations](#)
- [Configuring NAT to Support Unicast Messaging \(optional\)](#)
- [Configuring WAN Interfaces for MultiCast Operations](#)
- [Configuring a Standard IP Access List for Packet Filtering \(Optional\)](#)
- [Configuring a Standard IP Access List for Multicast Group Filtering \(Optional\)](#)

## Configuring IP Multicast Operations

This section describes how to configure the operation of IP multicast transmissions on the cable and WAN interfaces on the Cisco CMTS. You should perform this configuration on each cable interface being used for DSG traffic and for each WAN interface that is connected to a network controller or Conditional Access (CA) server that is forwarding IP multicast traffic.

### SUMMARY STEPS

1. **configure terminal**
2. **ip multicast-routing**
3. **ip pim ssm**
4. **ip cef**
5. **interface *interface***
6. **ip pim {dense-mode | sparsrse-mode | sparse-dense-mode}sparse-dense-mode | sparse-mode }**
7. **ip mroute-cache**
8. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>configure terminal</pre> <p><b>Example:</b> Router# configure terminal Router(config)# </p>	Enters global configuration mode.
Step 2	<pre>ip multicast-routing</pre> <p><b>Example:</b> Router(config)# ip multicast-routing Router(config)# </p>	Enables multicast routing on the router.
Step 3	<pre>ip pim ssm [vrf vrf-name] ssm {default   range access-list}</pre> <p><b>Example:</b> Router(config)# ip pim ssm range 4</p>	<p>Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command.</p> <ul style="list-style-type: none"> <li><b>vrf</b>— (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance.</li> <li><b>vrf-name</b>—(Optional) Name assigned to the VRF.</li> <li><b>default</b>—Defines the SSM range access list to 232/8.</li> <li><b>range access-list</b>—Specifies the standard IP access list number or name defining the SSM range.</li> </ul> <p><b>Note</b> When an SSM range of IP multicast addresses is defined by the <b>ip pim ssm</b> command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.</p> <p>For additional information about the <b>ip pim ssm</b> command, refer to the following document on Cisco.com:</p> <ul style="list-style-type: none"> <li><i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i>, Release 12.3 T <a href="http://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/123tip3r.html">http://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/123tip3r.html</a></li> </ul>
Step 4	<pre>ip cef [distributed] [accounting type   load-sharing algorithm algorithm   table type   traffic-statistics]</pre> <p><b>Example:</b> Router(config)# ip cef </p>	<p>Enables Cisco Express Forwarding (CEF) on the route processor card. To disable CEF, use the no form of this command.</p> <p>For additional information about the <b>ip cef</b> command, refer to the following document on Cisco.com:</p> <ul style="list-style-type: none"> <li><i>Cisco IOS Switching Services Command Reference</i>, Release 12.3 <a href="http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html">http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html</a></li> </ul>

	Command or Action	Purpose
Step 5	<pre>interface interface</pre> <p><b>Example:</b></p> <pre>Router(config)# interface cable 3/0 Router(config-if)#</pre>	Enters interface configuration mode for each cable interface or WAN interface being used for DSG traffic.
Step 6	<pre>ip pim {dense-mode   sparse-mode   sparse-dense-mode}</pre> <p><b>Example:</b></p> <pre>Router(config-if)# ip pim dense-mode Router(config-if)#</pre>	<p>Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature:</p> <ul style="list-style-type: none"> <li>• <b>dense-mode</b>—Enables dense mode of operation.</li> <li>• <b>sparse-mode</b>—Enables sparse mode of operation.</li> <li>• <b>sparse-dense-mode</b>—The interface is treated in either sparse mode, sparse-dense mode, or dense mode of operation, depending on the mode in which the multicast group operates.</li> </ul> <p><b>Note</b> You must configure this command on each interface that forwards multicast traffic.</p>
Step 7	<pre>ip mroute-cache</pre> <p><b>Example:</b></p> <pre>Router(config-if)# ip mroute-cache Router(config-if)#</pre>	(Optional) Enables IP multicast fast switching, also known as multicast distributed switching (MDS), on the interface.
	<p><b>Note</b> Repeat <a href="#">Step 5</a> through <a href="#">Step 7</a> for each cable interface that is being used for DSG traffic. Also repeat these steps on each WAN interface that is forwarding IP multicast traffic from the DSG network controllers and Conditional Access (CA) servers.</p>	
Step 8	<pre>exit</pre> <p><b>Example:</b></p> <pre>Router(config-if)# exit Router#</pre>	Exits interface configuration mode and returns to privileged EXEC mode.

## Examples

The following example illustrates globally configured advanced-mode DSG 1.2 settings in support of Multicast routing for SSM-type DSG configuration:

```
Router(config)# ip multicast-routing
Router(config)# ip pim ssm
Router(config)# ip cef
```

The following example illustrates WAN-side interface configurations for advanced-mode DSG 1.2 and access control lists for inbound packet filtering:

```
Router(config-if)# ip pim
Router(config-if)# ip mroute-cache
Router(config-if)# ip access-group 1 in
```

The following example illustrates interface-level configuration supporting Multicast IP routing traffic in advanced-mode DSG 1.2, with access control lists for inbound packet filtering:

```
Router(config-if)# ip pim sparse-mode
Router(config-if)# ip mroute-cache
Router(config-if)# ip igmp access-group 1
```



## Configuring NAT to Support Unicast Messaging (optional)

This section describes how to configure a Cisco CMTS router for Network Address Translation (NAT) so as to enable the use of IP unicast addresses for DSG messaging. This allows the Cisco CMTS router to translate incoming IP unicast addresses into the appropriate IP multicast address for the DSG traffic.

For the Cisco uBR10012 router, A-DSG 1.2 can also use an external router that is close to the Cisco CMTS to support unicast messaging. In this case, the nearby router must support NAT, and then send the address-translated multicast IP packets to the Cisco CMTS.



### Tip

This procedure should be performed after the cable interface has already been configured for DSG operations, as described in the [“Configuration Examples for DSG Issue 1.2”](#) section on page 31.



### Note

The Cisco CMTS router supports NAT only when it is running an “IP Plus” (-i-) Cisco IOS software image. Refer to the release notes for your Cisco IOS release for complete image availability and requirements.

## SUMMARY STEPS

1. **configure terminal**
2. **interface** *wan-interface*
3. **ip nat outside**
4. **interface cable** *interface*
5. **ip address** *ip-address mask secondary*
6. **ip nat inside**
7. **exit**
8. **ip nat inside source static** *ip-multicast-address cable-ip-address*
9. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal Router(config)#	Enters global configuration mode.
Step 2	<b>interface</b> <i>wan-interface</i>  <b>Example:</b> Router(config)# interface FastEthernet0/0 Router(config-if)#	Enters interface configuration mode for the specified WAN interface.

	Command or Action	Purpose
Step 3	<b>ip nat outside</b>  <b>Example:</b> Router(config-if)# ip nat outside Router(config-if)#	Configures the WAN interface as the “outside” (public) NAT interface.
Step 4	<b>interface cable interface</b>  <b>Example:</b> Router(config-if)# interface cable 3/0 Router(config-if)#	Enters interface configuration mode for the specified cable interface.  <b>Note</b> This cable interface should have previously been configured for DSG operations.
Step 5	<b>ip address ip-address mask secondary</b>  <b>Example:</b> Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary Router(config-if)#	Configures the cable interface with an IP address and subnet that should match the unicast address being used for DSG traffic. This IP address and its subnet must not be used by any other cable interfaces, cable modems, or any other types of traffic in the cable network.
Step 6	<b>ip nat inside</b>  <b>Example:</b> Router(config-if)# ip nat inside Router(config-if)#	Configures the cable interface as the inside (private) NAT interface.
Step 7	<b>exit</b>  <b>Example:</b> Router(config-if)# exit Router(config)#	Exits interface configuration mode and returns to global configuration mode.
Step 8	<b>ip nat inside source static ip-multicast-address cable-ip-address</b>  <b>Example:</b> Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2 Router(config)#	Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.  <ul style="list-style-type: none"> <li><i>ip-multicast-address</i> = This address should match the multicast address that was used when enabling DSG on the cable interface.</li> <li><i>cable-ip-address</i> = This address should match the IP address of the incoming unicast packet.</li> </ul>
	<b>Note</b> Repeat <a href="#">Step 2</a> and <a href="#">Step 8</a> for each cable interface to be configured for DSG unicast traffic.	
Step 9	<b>exit</b>  <b>Example:</b> Router(config)# exit Router#	Exits global configuration mode and returns to privileged EXEC mode.

## Configuring WAN Interfaces for MultiCast Operations

In addition to basic WAN interface configuration on the Cisco CMTS, described in other documents, the following WAN interface commands should be configured on the Cisco CMTS to support IP multicast operations with A-DSG 1.2, as required.

- **ip pim**
- **ip pim ssm**
- **ip cef**

These commands are described in the “[Configuring IP Multicast Operations](#)” section on page 14, and in the following documents on Cisco.com.

For additional information about the **ip pim** command, refer to the following document on Cisco.com:

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast*, Release 12.3  
[http://www.cisco.com/en/US/docs/ios/12\\_3/ipmulti/command/reference/iprnc\\_r.html](http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/iprnc_r.html)

For additional information about the **ip pim ssm** command, refer to the following document on Cisco.com:

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast*, Release 12.3 T  
[https://www.cisco.com/en/US/docs/ios/12\\_3t/ip\\_mcast/command/reference/ip3\\_i2gt.htm](https://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/ip3_i2gt.htm)

For additional information about the **ip cef** command, refer to the following document on Cisco.com:

- *Cisco IOS Switching Services Command Reference*, Release 12.3  
[http://www.cisco.com/en/US/docs/ios/12\\_3/switch/command/reference/swtch\\_r.html](http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html)

## Configuring a Standard IP Access List for Packet Filtering (Optional)

This section describes how to configure a standard IP access list so that only authorized traffic is allowed on the cable interface.



### Tip

---

This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the “[Additional References](#)” section on page 34.

---

### SUMMARY STEPS

1. **configure terminal**
2. **access-list** *access-list* **permit** *group-ip-address* [*mask*]
3. **access-list** *access-list* **deny** *group-ip-address* [*mask*]
4. **access-list** *access-list* **deny any**
5. **interface cable** *interface*
6. **ip access-group** *access-list*
7. **exit**

## DETAILED STEPS

	Command or Action	Purpose
Step 1	<p><b>configure terminal</b></p> <p><b>Example:</b> Router# configure terminal Router(config)#</p>	Enters global configuration mode.
Step 2	<p><b>access-list access-list permit group-ip-address [mask]</b></p> <p><b>Example:</b> Router(config)# access-list 90 permit 228.1.1.1 Router(config)#</p>	<p>Creates an access list specifying that permits access to the specific multicast address that matches the specified <i>group-ip-address</i> and <i>mask</i>.</p> <ul style="list-style-type: none"> <li><i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.</li> <li><i>group-ip-address</i> = IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels.</li> <li><i>mask</i> = (Optional) Bitmask that determines which addresses in the <i>group-ip-address</i> will be allowed access. The default is 255.255.255.255.</li> </ul>
Step 3	<p><b>access-list access-list deny group-ip-address [mask]</b></p> <p><b>Example:</b> Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255 Router(config)#</p>	<p>Configures the access list that denies access to any multicast address that matches the specified <i>group-ip-address</i> and <i>mask</i>.</p> <ul style="list-style-type: none"> <li><i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.</li> <li><i>group-ip-address</i> = IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels.</li> <li><i>mask</i> = (Optional) Bitmask that determines which addresses in the <i>group-ip-address</i> will be allowed access. The default is 255.255.255.255.</li> </ul>
Step 4	<p><b>access-list access-list deny any</b></p> <p><b>Example:</b> Router(config)# access-list 90 deny any Router(config)#</p>	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	<p><b>interface cable interface</b></p> <p><b>Example:</b> Router(config)# interface cable 3/0 Router(config-if)#</p>	Enters interface configuration mode for the specified cable interface.

Command or Action	Purpose
<p><b>Step 6</b></p> <pre>ip access-group access-list</pre> <p><b>Example:</b>  Router(config-if)# ip access-group 90  Router(config-if)# </p>	<p>(Optional, but recommended) Configures the interface with the access list, so that packets are filtered by the list before being accepted on the interface.</p> <ul style="list-style-type: none"> <li>• <i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 and should be the same list created in <a href="#">Step 3</a>.</li> </ul> <p><b>Note:</b> Standard Access lists only allow one address to be specified in the earlier step. If you apply an outbound access-list with only the multicast address of the tunnel denied, then the DSG traffic is not allowed to pass.</p> <p><b>Note</b> On the Cisco uBR10012 router, inbound access lists on the cable interface do not apply to multicast traffic, so they do not apply here. As a result, the Cisco uBR10012 requires that you use extended access lists that are blocked in the outbound direction for packets originating from the cable modem or CPE device on the network, and destined to the multicast group. The multicast group contains the classifiers associated with A-DSG 1.1 rules enabled on the interface.</p>
<p><b>Step 7</b></p> <pre>exit</pre> <p><b>Example:</b>  Router(config-if)# exit  Router# </p>	<p>Exits interface configuration mode and returns to Privileged EXEC mode.</p>

## Configuring a Standard IP Access List for Multicast Group Filtering (Optional)

This section describes how to configure a standard IP access list so that non-DOCSIS devices, such as DSG set-top boxes, can access only the authorized multicast group addresses and DSG tunnels.



### Tip

This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the [“Additional References” section on page 34](#).

### SUMMARY STEPS

1. **configure terminal**
2. **access-list** *access-list* **permit** *group-ip-address* [*mask*]
3. **access-list** *access-list* **deny** *group-ip-address* [*mask*]
4. **access-list** *access-list* **deny any**
5. **interface cable** *interface*
6. **ip igmp access-group** *access-list* [*version*]
7. **exit**

### DETAILED STEPS

	Command or Action	Purpose
Step 1	<b>configure terminal</b>  <b>Example:</b> Router# configure terminal Router(config)#	Enters global configuration mode.
Step 2	<b>access-list</b> <i>access-list</i> <b>permit</b> <i>group-ip-address</i> [ <i>mask</i> ]  <b>Example:</b> Router(config)# access-list 90 permit 228.1.1.1 Router(config)#	Creates an access list specifying that permits access to the specific multicast address that matches the specified <i>group-ip-address</i> and <i>mask</i> . <ul style="list-style-type: none"> <li>• <i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.</li> <li>• <i>group-ip-address</i> = IP address to be used as a base for this access list. It should be based on the group IP address used for the interface’s DSG tunnels.</li> <li>• <i>mask</i> = (Optional) Bitmask that determines which addresses in the <i>group-ip-address</i> will be allowed access. The default is 255.255.255.255.</li> </ul>

	Command or Action	Purpose
Step 3	<p><b>access-list</b> <i>access-list</i> <b>deny</b> <i>group-ip-address</i> [<i>mask</i>]</p> <p><b>Example:</b>  Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255  Router(config)#</p>	<p>Configures the access list that denies access to any multicast address that matches the specified <i>group-ip-address</i> and <i>mask</i>.</p> <ul style="list-style-type: none"> <li>• <i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.</li> <li>• <i>group-ip-address</i> = IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels.</li> <li>• <i>mask</i> = (Optional) Bitmask that determines which addresses in the <i>group-ip-address</i> will be allowed access. The default is 255.255.255.255.</li> </ul>
Step 4	<p><b>access-list</b> <i>access-list</i> <b>deny</b> <b>any</b></p> <p><b>Example:</b>  Router(config)# access-list 90 deny any  Router(config)#</p>	<p>Configures the access list so that it denies access to any IP addresses other than the ones previously configured.</p>
Step 5	<p><b>interface cable</b> <i>interface</i></p> <p><b>Example:</b>  Router(config)# interface cable 3/0  Router(config-if)#</p>	<p>Enters interface configuration mode for the specified cable interface.</p>
Step 6	<p><b>ip igmp access-group</b> <i>access-list</i> [<i>version</i>]</p> <p><b>Example:</b>  Router(config-if)# ip igmp access-group 90  Router(config-if)#</p>	<p>(Optional, but recommended) Configures the interface to accept traffic only from the associated access list, so that only authorized devices are allowed to access the DSG tunnels.</p> <ul style="list-style-type: none"> <li>• <i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 and should be the same list created in <a href="#">Step 3</a>.</li> <li>• <i>version</i> = (Optional) Specifies the IGMP version. The default is 2.</li> </ul>
Step 7	<p><b>exit</b></p> <p><b>Example:</b>  Router(config-if)# exit  Router#</p>	<p>Exits interface configuration mode and returns to privileged EXEC mode.</p>

# How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature

This section describes the following commands that you can use to monitor and display information about the Advanced-mode DOCSIS Set-Top Gateway feature:

- [Displaying Global Configurations for Advanced-Mode DSG 1.2, page 24](#)
- [Displaying Interface-level Configurations for Advanced-Mode DSG 1.2, page 27](#)
- [Debugging Advanced-Mode DSG 1.2](#)

## Displaying Global Configurations for Advanced-Mode DSG 1.2

The following **show** commands are enhanced in Cisco IOS Release 12.3(17a)BC2 to support advanced-mode DSG 1.2 on the Cisco CMTS. These commands display globally-configured or interface-level DSG settings, status, statistics, and multiple types of DSG 1.2 tunnel information.

- **show cable dsg tunnel**
- **show cable dsg tunnel ID**
- **show cable dsg tunnel ID cfr**
- **show cable dsg tunnel ID clients**
- **show cable dsg tunnel ID interfaces**
- **show cable dsg tunnel ID statistics**
- **show cable dsg tunnel ID verbose**
- **show cable dsg tg**
- **show cable dsg tg ID channel ID**
- **show cable dsg tg ID channel ID verbose**

### show cable dsg tunnel

To display tunnel MAC address, state, tunnel-group id, classifiers associated to tunnel and its state, use the **show cable dsg tunnel** command in privileged EXEC mode. This command also displays the number of interfaces to which a tunnel is associated, the clients associated, and the Qos service class name for all the configured tunnels.

The following example illustrates this command:

```
Router# show cable dsg tunnel
      tunnel          TG      cfr      tunnel  rule  client service
id  state mac-addr  id  id  state I/F  id  state listId class
1   en  0100.5e01.0001 1   1   en  C5/0  1   en  1   DSG-Rate1
      6   en
      7   en
      8   en
2   en  0100.5e01.0002 1   2   en  C5/0  2   en  2
3   en  0100.5e01.0003 1   3   en  C5/0  3   en  3
4   en  0002.0002.0001 2   4   en  C5/0  4   en  1
      C5/1  1   en  1
5   en  0002.0002.0002 2   5   en  C5/0  5   en  2   DSG-Rate2
      C5/1  2   en  2
6   en  0002.0002.0003 2   9   en  C5/0  6   en  21
      C5/1  3   en  21
```



## show cable dsg tunnel

To display information for a given DSG tunnel, use the **show cable dsg tunnel** command, specifying the tunnel for which to display information.

**show cable dsg tunnel** *tunnel-id* [**cfr** | **clients** | **interfaces** | **statistics** | **verbose**]

- **cfr**—Shows DSG tunnel classifiers.
- **clients**—Shows DSG tunnel clients.
- **interfaces**—Shows DSG tunnel interfaces.
- **statistics**—Shows DSG tunnel statistics.
- **verbose**—Shows DSG tunnel detail information.

The below example illustrates this command for DSG Tunnel 1:

```
Router# show cable dsg tunnel 1
      tunnel          TG      cfr      tunnel  rule  client service
id  state mac-addr    id  id  state I/F    id  state listId class
1   en  0100.5e01.0001  1   1   en  C5/0   1   en  1     DSG-Rate1
                        6   en
                        7   en
                        8   en
```

The below example illustrates detailed information about all the classifiers associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 cfr
tunnel cfr  cfr  cfr destination ip  source ip  srcPre d_port d_port
id     id   state pri address          address    length start end
1     1   en  0  230.1.0.1        0.0.0.0   32     0    65535
      6   en  0  231.1.1.6        0.0.0.0   32     0    65535
      7   en  0  231.1.1.7        0.0.0.0   32     0    65535
      8   en  0  231.1.1.8        0.0.0.0   32     0    65535
```

The below example illustrates detailed information about all the clients associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 clients
tunnel client client client      client      vendor
id     listId id    id type      address     group
1     1     1     MAC Addr   0100.5e00.0001
      2     Application ID 0x0951
      3     Broadcast    Unspecified
      4     Broadcast    4
```

The below example illustrates all DSG interfaces and rules associated to the specified tunnel.

```
Router# show cable dsg tunnel 1 interfaces
tunnel downstream  rule
id     interface  id
4     Cable5/0    4
      Cable5/1    1
```

## Router# show cable dsg tunnel 1 statistics

The below example illustrates packet statistics information about the specified tunnel.

```
Router# show cable dsg tunnel 1 statistics
tunnel cfr  cfr  destination ip  source ip  total      total
id     id   state address          address    forwarded  received
```

1	1	en	230.1.0.1	0.0.0.0	0	0
	6	en	231.1.1.6	0.0.0.0	0	0
	7	en	231.1.1.7	0.0.0.0	0	0
	8	en	231.1.1.8	0.0.0.0	0	0

The below example illustrates all detailed information about the specified tunnel.

```

Router#show cable dsr tunnel 1 verbose
Tunnel ID                               : 1
State                                    : enable
MAC Addr                                 : 0100.5e01.0001

TG Id                                     : 1

Cfr Id                                   : 1
State                                    : enable
Priority                                  : 0
Dest IP                                  : 230.1.0.1
Src IP                                    : 0.0.0.0
Src Prefix Length                        : 32
Dest Port Start                          : 0
Dest Port End                            : 65535
Forwarded                                 : 0
Received                                 : 0

Cfr Id                                   : 6
State                                    : enable
Priority                                  : 0
Dest IP                                  : 231.1.1.6
Src IP                                    : 0.0.0.0
Src Prefix Length                        : 32
Dest Port Start                          : 0
Dest Port End                            : 65535
Forwarded                                 : 0
Received                                 : 0

Cfr Id                                   : 7
State                                    : enable
Priority                                  : 0
Dest IP                                  : 231.1.1.7
Src IP                                    : 0.0.0.0
Src Prefix Length                        : 32
Dest Port Start                          : 0
Dest Port End                            : 65535
Forwarded                                 : 0
Received                                 : 0

Cfr Id                                   : 8
State                                    : enable
Priority                                  : 0
Dest IP                                  : 231.1.1.8
Src IP                                    : 0.0.0.0
Src Prefix Length                        : 32
Dest Port Start                          : 0
Dest Port End                            : 65535
Forwarded                                 : 0
Received                                 : 0

Client List Id                           : 1
Client Id                                 : 1
Client Id Type                            : MAC Addr           0100.5e00.0001
Client Id                                 : 2
Client Id Type                            : Application ID   0x0951
Client Id                                 : 3

```

```

Client Id Type                : Broadcast      Unspecified
Client Id                     : 4
Client Id Type                : Broadcast      4

Interface                     : Cable5/0
Rule Id                       : 1

```

The below example illustrates configured parameters for all DSG tunnel groups.

```

Router# show cable dsg tg
TG      Chan  TG      Rule Vendor UCID
id      id    state I/F    pri  Param list
1       1     en    C5/0   16   1      1 2 3 4
1       2     en                    0
2       1     en    C5/0   11   2
                C5/1
2       2     en                    0

```

The below example displays the same information as above for the specified tunnel group.

```

Router# show cable dsg tg 1 channel 1
TG      Chan  TG      Rule Vendor UCID
id      id    state I/F    pri  Param list
1       1     en    C5/0   16   1      1 2 3 4

```

The below example illustrates detailed information for the specified tunnel group.

```

Router# show cable dsg tg 1 channel 1 verbose
TG: 1      Chan: 1      state: en pri: 16 Vendor: 1      UCID: 1 2 3 4
          rule      tunnel      cfr
I/F      id state id state mac-addr      id state dest-ip      In-DCD listId
C5/0     1   en  1   en  0101.5e01.0001  1   en  230.1.0.1      yes   1
                                                6   en  231.1.1.6      no
                                                7   en  231.1.1.7      no
                                                8   en  231.1.1.8      no
          2   en  2   en  0101.5e01.0002  2   en  230.1.0.2      yes   2
          3   en  3   en  0101.5e01.0003  3   en  230.1.0.3      yes   3

```

## Displaying Interface-level Configurations for Advanced-Mode DSG 1.2

The following **show** commands are enhanced in Cisco IOS Release 12.3(17a)BC2 to support advanced-mode DSG 1.2 on the Cisco CMTS. These commands display interface-level configurations.

- **show cable dsg tunnel interfaces**
- **show interface cable dsg downstream**
- **show interface cable dsg downstream dcd**
- **show interface cable dsg downstream tg**
- **show interface cable downstream tg ID channel ID**
- **show interface cable dsg downstream tunnel ID**
- **show interface cable dsg downstream tunnel**

### show cable dsg tunnel interfaces

To display all interfaces and DSG rules for the associated tunnel, use the **show cable dsg tunnel interfaces** command in privileged EXEC mode.

**show cable dsg tunnel (*tunnel-id*) interfaces**

The following example illustrates this command:

```
Router#show cable dsg tunnel 1 interfaces
tunnel downstream rule
id interface id
4 Cable5/0 4
Cable5/1 1
```

**show interfaces cable dsg downstream**

To display information for downstream DSG 1.2 interfaces, use the **show interface cable dsg downstream** command in privileged EXEC mode. The following example illustrates syntax options for this command.

```
show interface cable {slot/port | slot/subslot/port} dsg downstream [tunnel | tg | dcd]
```

Keywords for this command include the following:

- **dcd**—Shows DSG downstream dcd message
- **tg**—Show DSG downstream tunnel-group
- **tunnel**—Show DSG downstream tunnel

**show interfaces cable dsg downstream**

To display DSG downstream interface configuration information, to include the number of DSG tunnels, classifiers, clients, and vendor-specific parameters, use the **show interfaces cable dsg downstream** command in privileged EXEC mode.

```
show interfaces cable {slot/port | slot/subslot/port} dsg downstream
```

The following example illustrates this command supporting DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream
chan chFreq chan timer init oper twoWay oneWay num num num num num
list index freq index timeout timeout timer timer rule tunnel cfr client vsp
1 1 471 1 4 600 300 1800 6 6 3 4 2
2 477
3 483
4 583
```

**show interfaces cable dsg downstream dcd**

To display DCD statistics for the given downstream, use the **show interfaces cable dsg downstream dcd** command in privileged EXEC mode. This command only displays DCD Type/Length/Value information if the **debug cable dsg** command is previously enabled.

```
show interfaces cable {slot/port | slot/subslot/port} dsg downstream dcd
```

The following example illustrates DCD statistics information supporting DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream dcd
dcd dcd num of dcd num of dcd num of dcd num of
state Tx sent fail change cnt fragment
en on 6502 0 28 1

Router# debug cable dsg
```

```

CMTS DSG debugging is on
Router#
Router# show interfaces c5/0 dsg downstream dcd
dcd dcd num of dcd num of dcd num of dcd num of
state Tx sent fail change cnt fragment
en on 6512 0 28 1

Router#
02:08:42: DCD TLV last sent:
32360101 01020110 03040102 03040412 02060100 5E000001 04020951 01000102
00040506 01005E01 00010602 00012B08 08030000 01010101 170F0202 00010501
00090605 04E60100 01322801 01020201 10030401 02030404 0403020A BC050601
005E0100 02060200 022B0808 03000001 01010117 0F020200 02050100 09060504
E6010002 32280101 03020110 03040102 03040404 04020123 05060100 5E010003
06020003 2B080803 00000101 0101170F 02020003 05010009 060504E6 01000332
38010104 02010B04 12020601 005E0000 01040209 51010001 02000405 06000200
0200012B 09080300 00010102 01022B09 08030000 02010201 02322A01 01050201
0B040403 020ABC05 06000200 0200022B 09080300 00010102 01022B09 08030000
02010201 02324601 01060201 0B042002 06002100 21000102 06002100 21000202
06002100 21000302 06002100 21000405 06000200 0200032B 09080300 00010102
01022B09 08030000 02010201 02332801 041C12E3 C001041C 6E714001 041CC9FE
C0010422 BFDFC002 02000403 02025804 02012C05 020708

```

## show interfaces cable dsg downstream tg

To display DSG tunnel group parameters, and rule information applying to the tunnel group, to include tunnels and tunnel states, classifiers, and client information, use the **show interfaces cable dsg downstream tg** command in privileged EXEC mode. You can display information for a specific tunnel, if specified.

**show interfaces cable {slot/port | slot/subslot/port} dsg downstream tg [channel channel-id]**

The following example illustrates typical information displayed with this command in DSG 1.2:

```

Router#show interfaces c5/0 dsg downstream tg
TG: 1 Chan: 1 state: en pri: 16 Vendor: 1 UCID: 1 2 3 4

rule tunnel cfr client
I/F id state id state mac-addr id state dest-ip In-DCD listId
C5/0 1 en 1 en 0101.5e01.0001 1 en 230.1.0.1 yes 1
6 en 231.1.1.6 no
7 en 231.1.1.7 no
8 en 231.1.1.8 no
2 en 2 0101.5e01.0002 2 en 230.1.0.2 yes 2
3 en 3 en 0101.5e01.0003 3 en 230.1.0.3 yes 3

TG: 2 Chan: 1 state: en pri: 11 Vendor: 2 UCID:

rule tunnel cfr client
I/F id state id state mac-addr id state dest-ip In-DCD listId
C5/0 4 en 4 en 0002.0002.0001 4 en 230.2.2.1 no 1
5 en 5 en 0002.0002.0002 5 en 230.2.2.2 no 2
6 en 6 en 0002.0002.0003 9 en 231.1.1.9 no 21

```

The following examples displays the same type of information as above for the given tunnel group.

```

Router# show interfaces c5/0 dsg downstream tg 1 channel 1
TG: 1 Chan: 1 state: en pri: 16 Vendor: 1 UCID: 1 2 3 4

rule tunnel cfr client
I/F id state id state mac-addr id state dest-ip In-DCD listId
C5/0 1 en 1 en 0101.5e01.0001 1 en 230.1.0.1 yes 1

```

				6	en 231.1.1.6	no	
				7	en 231.1.1.7	no	
				8	en 231.1.1.8	no	
2	en 2	en 0101.5e01.0002	2	en 230.1.0.2	yes	2	
3	en 3	en 0101.5e01.0003	3	en 230.1.0.3	yes	3	

## show interfaces cable dsg downstream tunnel

To display tunnel information associated with the downstream, use the **show interfaces cable dsg downstream tunnel** command in privileged EXEC mode.

**show interfaces cable {slot/port | slot/subslot/port} dsg downstream tunnel**

The following example illustrates interface information for the DSG downstream tunnel in DSG 1.2:

```
Router# show interfaces c5/0 dsg downstream tunnel
      tunnel      TG      cfr      rule      client service
id  state mac-addr  id  id  state id  state listId class
1   en  0100.5e01.0001  1   1   en  1   en  1   DSG-Rate1
      6   en
      7   en
      8   en
2   en  0100.5e01.0002  1   2   en  2   en  2
3   en  0100.5e01.0003  1   3   en  3   en  3
4   en  0002.0002.0001  2   4   en  4   en  1
5   en  0002.0002.0002  2   5   en  5   en  2   DSG-Rate2
6   en  0002.0002.0003  2   9   en  6   en  21
```

## show interfaces c5/0 dsg downstream tunnel

To display DSG tunnel information associated with the downstream, use the **show interfaces cable dsg downstream tunnel** command in privileged EXEC mode:

**show interfaces cable {slot/port | slot/subslot/port} dsg downstream tunnel tunnel-id**

The following example illustrates information for the specified interface and tunnel:

```
Router# show interfaces c5/0 dsg downstream tunnel 1
Router# show interfaces c5/0 dsg downstream tunnel
      tunnel      TG      cfr      rule      client service
id  state mac-addr  id  id  state id  state listId class
1   en  0100.5e01.0001  1   1   en  1   en  1   DSG-Rate1
      6   en
      7   en
      8   en
```

## Debugging Advanced-Mode DSG 1.2

The following commands enable debugging and troubleshooting DSG-specific issues for Advanced-Mode DSG 1.2. To enable debugging for DSG 1.2 on the Cisco CMTS, use the **debug cable dsg** command in privileged EXEC mode:

**debug cable dsg [ dcd | pkt ]**

This command has the following three forms and purposes:

- **debug cable dsg**—Provides general DSG 1.2 debugging.
- **debug cable dsg dcd**—Provides DCD-related debugging for DSG 1.2.
- **debug cable dsg pkt**—Provides packet-related debugging for DSG 1.2.

# Configuration Examples for DSG Issue 1.2

This configuration example, supporting advanced-mode DSG 1.2 in Cisco IOS Release 12.3(17a)BC2, illustrates a sample DSG network featuring these components:

- Two Cisco universal broadband routers
- IP Multicast for each DSG implementation
- Two DSG Clients for each Cisco CMTS
- Two DSG Servers (one for each Cisco CMTS)

Each Cisco CMTS is configured as follows, and the remainder of this topic describes example configurations that apply to this architecture.

## CMTS Headend #1

- DSG Server #1—Connected to Cisco CMTS via IP Multicast, with DSG Server having IP Address 12.8.8.1
- Destination IP Address for the Cisco CMTS—228.9.9.1
- DSG Tunnel Address—0105.0005.0005
- Downstream #1 Supporting two DSG Clients:
  - DSG Client #1—ID 101.1.1
  - DSG Client #2—ID 102.2.2

## CMTS Headend #2

- DSG Server #2—Connected to Cisco CMTS via IP Multicast, with DSG Server having IP Address 12.8.8.2
- Destination IP Address for the Cisco CMTS—228.9.9.2
- DSG Tunnel Address—0106.0006.0006
- Downstream #2 Supporting two DSG Clients:
  - DSG Client #1—ID 101.1.1
  - DSG Client #2—ID 102.2.2

## Example of Two DSG Tunnels with MAC DA Substitution

In this configuration, and given the two Cisco CMTS Headends cited above, below are the two sets of DSG rules, with each set applying to each Cisco CMTS, in respective fashion.

These settings apply to DSG #1 and two downstreams:

- DSG Rule ID 1
- DSG Client ID 101.1.1
- DSG Tunnel Address 105.5.5

These settings apply to DSG Rule #2 and two downstreams:

- DSG Rule ID 1
- DSG Client ID 102.2.2
- DSG Tunnel Address 106.6.6

**DSG Example with Regionalization Per Downstream**

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below are two downstream rules that can be configured in this architecture, for example:

- Downstream Rule #1
  - DSG Rule ID #1
  - DSG Client ID—101.1.1
  - DSG Tunnel Address—105.5.5
- Downstream Rule #2
  - DSG Rule ID #2
  - DSG Client ID—102.2.2
  - DSG Tunnel Address—106.6.6

**DSG Example with Regionalization Per Upstream**

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below are two upstream rules that can be configured in this architecture, for example:

- Upstream Rule #1
  - DSG Rule ID #1
  - DSG Client ID—101.1.1
  - DSG UCID Range—0 to 2
  - DSG Tunnel Address—105.5.5
- Upstream Rule #2
  - DSG Rule ID #2
  - DSG Client ID—102.2.2
  - DSG UCID Range—3 to 5
  - DSG Tunnel Address—106.6.6

**Example of Two DSG Tunnels with Full Classifiers and MAC DA Substitution**

In this configuration, and given the two Cisco CMTS Headends cited above, below are the two sets of DSG rules, with each set applying to each Cisco CMTS, in respective fashion.

These settings apply to DSG #1:

- DSG Rule ID 1
- Downstreams 1 and 2
- DSG Client ID 101.1.1
- DSG Tunnel Address 105.5.5
- DSG Classifier ID—10
- IP SA—12.8.8.1
- IP DA—228.9.9.1
- UDP DP—8000

These settings apply to DSG Rule #2:

- DSG Rule ID 2



- Downstreams 1 and 2
- DSG Client ID 102.2.2
- DSG Tunnel Address 106.6.6
- DSG Classifier ID—20
- IP SA—12.8.8.2
- IP DA—228.9.9.2
- UDP DP—8000

#### **Example of One DSG Tunnel Supporting IP Multicast from Multiple DSG Servers**

In this configuration, and given the two Cisco CMTS Headends cited earlier in this topic, below is an example of one DSG Tunnel with multiple DSG servers supporting IP Multicast:

- DSG Rule ID 1
- Downstreams 1 and 2
- DSG Client ID 101.1.1 and 102.2.2
- DSG Tunnel Address 105.5.5
- DSG Classifier ID—10
  - IP SA—12.8.8.1
  - IP DA—228.9.9.1
  - UDP DP—8000
- DSG Classifier ID—20
  - IP SA—12.8.8.2
  - IP DA—228.9.9.2
  - UDP DP—8000

## Additional References

The following sections provide references related to <<Feature>>.

### Related Documents

Related Topic	Document Title
Cisco IOS Release Notes supporting Cisco IOS Release 12.3 BC	<ul style="list-style-type: none"> <li>• <i>Cisco uBR7200 Series - Cisco IOS Release 12.3 BC</i> <a href="http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html">http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html</a></li> <li>• <i>Cisco uBR10012 - Cisco IOS Release 12.3 BC</i> <a href="http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html">http://www.cisco.com/en/US/docs/cable/cmts/ubr10012/release/notes/12_3bc/ubr10k_123bc_rn.html</a></li> </ul>
General Cisco IOS Commands supporting Cisco Universal Broadband Routers	<ul style="list-style-type: none"> <li>• <i>Cisco Broadband Cable Command Reference Guide</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></li> </ul>
Internetworking Terms and Acronyms	<ul style="list-style-type: none"> <li>• <i>Internetworking Terms and Acronyms</i> <a href="http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html">http://www.cisco.com/en/US/docs/internetworking/terms_acronyms/ita.html</a></li> </ul>

### Standards

Standard	Title
CableLabs™ <i>DOCSIS Set-top Gateway (DSG) Interface Specification</i> , CM-SP-DSG-I05-050812	<a href="http://www.cablelabs.com/specifications/archives/CM-SP-DSG-I05-050812.pdf">http://www.cablelabs.com/specifications/archives/CM-SP-DSG-I05-050812.pdf</a>

### MIBs

MIB	MIBs Link
MIBs additions and enhancements supporting advanced-mode DSG 1.2, to include DOCS-DSG-IF-MIB	<ul style="list-style-type: none"> <li>• <i>Cisco CMTS Universal Broadband Router MIB Specifications Guide</i> <a href="http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html">http://www.cisco.com/en/US/docs/cable/cmts/mib/12_2sc/reference/guide/ubrmibv5.html</a></li> </ul>
To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:	<ul style="list-style-type: none"> <li>• <i>Cisco MIB Locator</i> <a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a></li> </ul>

### RFCs

No Requests for Comment (RFCs) have been added in support of advanced-mode DSG 1.2

## Technical Assistance

Description	Link
<p>The Cisco Technical Support &amp; 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.</p>	<p><a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a></p>

# Glossary

This section describes terms and acronyms that are used in this manual and not otherwise defined.

**Application ID**—This is a 16 bit field indicating a numeric ID for an application running on the Set-top Device. The Application ID is typically assigned through a Source Name Sub-table (SNS) from [SCTE 65] carried in the Broadcast DSG Tunnel.

**CA\_system\_ID**—This is a 16 bit field indicating the type of CA system applicable for either the associated ECM and/or EMM streams. The CA\_system\_ID may be used as a DSG Client ID in DSG Advanced Mode.

**CableCARD™**—A detachable device defined in OpenCable™ and distributed by cable providers that connects to the cable receiver and manages Conditional Access.

**CA vendor**—A programming provider that has encrypted its programs using conditional access (CA) techniques, so that only authorized subscribers are able to decrypt and view the programs. When referring to the network topology, the term “CA vendor” typically refers to the servers that are providing the digitally encrypted program streams.

**Cable Card**—Another term for POD. See POD.

**conditional access (CA)**—Methods for encrypting video programs so that only authorized subscribers are able to decrypt and view the programs.

**customer premises equipment (CPE)**—Set-top box, host, or other device at the subscriber’s site that receives the cable signals coming from the cable modem termination system (CMTS), CA servers, and other DSG servers.

**Data-over-Cable Service Interface Specifications (DOCSIS)**—A suite of specifications maintained by CableLabs that describe the operation of a data network over a hybrid fiber-coaxial (HFC) cable network.

**DOCSIS Set-Top Gateway (DSG)**—A specification from CableLabs that allows operators of a DOCSIS cable network to provide out-of-band (OOB) messaging to set-top boxes (STBs) over existing cable networks. This allows MSOs and other service providers to combine both DOCSIS and STB operations over a single, open, vendor-independent network. Vendors can provide advanced STB video and electronic programming services, without interfering with the existing DOCSIS cable network.

**DSG Address Table**—The collection of DSG Rules and DSG Classifiers contained within the DCD message. The DSG Client uses its DSG Client ID as an index into the DSG Address Table to determine what DSG Tunnel Address to receive.

**DSG Advanced Mode**—Operation with the DCD message. Address assignment is dynamic. The DSG Tunnel Address is determined by the DSG Agent and learned by the DSG Client through the DSG Address Table in the DCD message.

**DSG Agent**—The DSG Agent is the implementation of the DSG protocol within the CMTS. The DSG Agent creates the DSG Tunnel, places content from the DSG Server into the DSG Tunnel, and sends the DSG Tunnel to the DSG Client.

**DSG Basic Mode**—Operation without the DCD message. Address assignment is static. The DSG Tunnel Address is determined by the DSG Client and learned by the DSG Agent through configuration. This mode provides backwards compatibility with earlier versions of the DSG specification.

**DSG Channel**—Any DOCSIS downstream channel that contains one or more DSG Tunnels.

**DSG Client**—The DSG Client is the implementation of the DSG protocol within the Set-top Device. The DSG Client terminates the DSG Tunnel and receives content from the DSG Server. There may be more than one DSG Client within a Set-top Device.

**DSG Client ID**—This is an identifier that uniquely identifies a DSG Client. The DSG Client ID is unique per DSG Client, but is not unique per Set-top Device as the same DSG Client which provides the same function may exist in multiple Set-top Devices. In DSG Basic Mode, the DSG Client ID is a 6 byte MAC address. In DSG Advanced Mode, the DSG Client ID may additionally be a 2 byte Application ID, a 2 byte CA\_system\_ID, or a broadcast ID.

**DSG Rule**—A row entry within the DSG Address Table that assigns a DSG Client ID to a DSG Tunnel Address.

**DSG Server**—The DSG Server refers to any server such as an Application Server or other network attached device that provides content that is transported through the DSG Tunnel to the DSG Client.

**DSG Tunnel**—An IP multicast datagram stream originating at the DOCSIS Set-Top Gateway and carrying out-of-band messages intended for set-top boxes. It is carried over the downstream DOCSIS channel and is identified by a well-known Ethernet MAC address that is reserved and published by the CA/POD provider. Multiple DSG tunnels may exist on a single downstream DOCSIS channel.

**embedded cable modem**—A DOCSIS cable modem that is integrated into the customer premises equipment (for example, a set-top box that contains tuners for both DOCSIS signals and DSG signals).

**multicast address**—A broadcast address that is targeted to and received by multiple hosts, as opposed to a unicast address that is intended for only one particular host. Both the Ethernet MAC Layer 2 and the IP Layer 3 protocols support multicast addressing. IP multicast addresses are divided into three separate subgroups:

- Local Scope Addresses—IP addresses 224.0.0.0 through 224.0.0.255. These addresses are reserved for the exclusive use of the network protocol layer and are never forwarded beyond the local network. These addresses cannot be used for DSG traffic.
- Global Scope Addresses—IP addresses 224.0.1.0 through 238.255.255.255. These addresses are allocated dynamically throughout the Internet. These addresses can be used for DSG traffic.
- Administratively Scoped Addresses—IP addresses 239.0.0.0 through 239.255.255.255. These addresses are reserved for use within private networks. These addresses can be used for DSG traffic, assuming that the video servers and set-top boxes are within the same private network.

**network controller**—Computers system that manages the set-top boxes or other CPE devices within a cable system. In a DSG network, the network controller transmits its control and other messages using a dedicated out-of-band channel.

**One-Way**—This expression infers that the downstream path (from the network to the subscriber) is operational, and that the upstream path (from the subscriber to the network) is not operational. This may occur because the upstream path is not available, the Set-top Device is not registered, or the Set-top Device does not support a two-way mode of operation. Compare with Two-Way.

**out-of-band (OOB) messaging**—Describes a form of network management in which the network controller sends control and information messages to one or more hosts or set-top boxes using a dedicated channel that is separate from the channel used to send programs and other user data. In a DSG network, OOB messages are transmitted using IP multicast packets and are received by those set-top boxes that are members of the appropriate multicast groups. The OOB messages can include the following types of messages:

- Conditional Access (CA) messages including entitlements
- System Information (SI) messages
- Electronic Program Guide (EPG) messages
- Emergency Alert System (EAS) messages
- Other generic messages

**Point of Deployment (POD) module**—Removable PCMCIA-form factor security card that is plugged into a set-top box (STB) to uniquely identify and authenticate the STB. Each POD contains a unique ID that identifies the STB, as well as an X.509 certificate that the POD uses to establish secure authentication with the CA servers. This allows the CA provisioning servers to securely identify the STB and determine which programs and services it is authorized to receive. A POD module is more frequently referred to as a Cable Card.

**QoS Parameter Set**—The set of Service Flow Encodings that describe the Quality of Service attributes of a Service Flow or a Service Class.

**Service Class**—A set of queuing and scheduling attributes that is named and that is configured at the CMTS. A Service Class is identified by a Service Class Name. A Service Class has an associated QoS Parameter Set.

**set-top box (STB)**—Customer premises equipment (CPE) providing subscription and pay-per-view broadcast television services and interactive TV services. In a DSG network, the each STB is a member of one or more multicast groups, allowing the STB to receive the OOB messages that allow its subscribers to receive the programs they are authorized to view.

**Set-top Controller**—This is the computer system responsible for managing the Set-top Devices within a cable system. It manages Set-top Devices through control and information messages sent via the Out-Of-Band channel.

**Set-top Device**—A cable receiver that contains an embedded Cable Modem for DOCSIS connectivity, an embedded processor for an application environment, and either an embedded or removable module for Conditional Access. In OpenCable™, this definition refers to the combination of an Advanced Host Device and a CableCARD™.

**set-top terminal**—See set-top box (STB).

**Two-Way**—This expression infers that the downstream path and the upstream path are operational. Compare with One-Way.

**Unicast Address**—Address specified for a message sent to a single network destination. Compare with broadcast and multicast.

**Well-Known MAC Address**—Refers to the MAC address of the DSG Client within the Set-top Device. This MAC address has been assigned by the manufacturer of the CableCARD and/or Conditional Access system within the Set-top Device, and has been made known to the MSO for use in configuring the DSG Agent.

**Note**

---

See [Internetworking Terms and Acronyms](#) for terms not included in this glossary.

---

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned 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. (1110R)

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.

© 2009 Cisco Systems, Inc. All rights reserved.

