Advanced-Mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers

The Advanced-Mode DOCSIS Set-Top Gateway (A-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*
- A-DSG 1.2 introduces support for the DOCS-DSG-IF MIB.

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

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the Feature Information Table at the end of this document.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://tools.cisco.com/ITDIT/CFN/. An account on http://www.cisco.com/ is not required.

Contents

Hardware Compatibility Matrix for Cisco cBR Series Routers

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

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

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

Prerequisites for Advanced-Mode DSG Issue 1.2

No special equipment or software is needed to use the Advanced-Mode DSG Issue 1.2 feature.

Restrictions for Advanced-Mode DSG Issue 1.2

This section contains restrictions that are specific to A-DSG 1.2 on a Cisco CMTS router.

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.

Multicast Configuration Restrictions

IP multicasting must be configured for correct operation of A-DSG 1.2. Specifically, IP multicast routing must be set in global configuration. Also, IP PIM must be configured on all bundle interfaces of cable interfaces that are to carry multicast traffic.

See the Configuring the Default Multicast Quality of Service, on page 6 and the Configuring IP Multicast Operations, on page 13 for additional Multicast information and global configurations supporting DSG.

NAT for DSG Unicast-only Mapping

A-DSG 1.2 supports multicast IP addressing. However, it also supports unicast IP destination addresses. On the Cisco cBR-8 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 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 router. The multicast IP address is the new destination IP address that is configured to map to one or a set of DSG tunnels.

PIM and SSM for Multicast

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

- **ip pim ssm**

Refer to the Configuring IP Multicast Operations, on page 13.

Subinterfaces

A-DSG 1.2 supports subinterfaces on the Cisco CMTS router.

Information About Advanced-Mode DSG Issue 1.2

A-DSG 1.2 offers these new or enhanced capabilities:

- A-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 and Agents

A-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.

FQDN Support

You can specify either a fully-qualified domain name (FQDN) or IP address for A-DSG classifier multicast group and source addresses using the **cable dsg cfr** command in global configuration mode. We recommend that you use an FQDN to avoid modification of multicast group and source addresses when network changes are implemented.

This feature allows you to use a hostname (FQDN) in place of the source IP address using the **cable dsg cfr** command. For example, you have two A-DSG tunnel servers, in two locations, sending multicast traffic to the same multicast address. In this scenario, you can specify a hostname for the source IP address and let the DNS server determine which source is sending the multicast traffic.

If you configure an A-DSG classifier with a hostname, the Cisco CMTS router immediately verifies if the hostname can be resolved against an IP address using the local host cache. If not, the router does not enable the classifier until the hostname is resolved. If the hostname cannot be resolved locally, the router performs a DNS query to verify the DSG classifiers.

The FQDN format does not support static Internet Group Management Protocol (IGMP) join requests initiated on the Cisco CMTS router. The IGMP static group IP address created automatically under a bundle interface at the time of A-DSG configuration is not displayed in the **show running-config interface** command output. To display the A-DSG static groups configured under a bundle interface, use the **show cable dsg static-group bundle** command in privileged EXEC mode.

DSG Name Process and DNS Query

Every DNS record contains a time to live (TTL) value set by the server administrator, and this may vary from seconds to weeks. The DSG name process supersedes the TTL value criterion to update A-DSG classifiers on the Cisco CMTS router.

The DSG name process enables the Cisco CMTS router to query the DNS server for faster classifier updates. To enable the Cisco CMTS router to perform a DNS query for an A-DSG classifier verification, you must configure one or more DNS servers using the **ip name-server** command in global configuration mode. You can also specify the DNS query interval using the **cable dsg name-update-interval** command in global configuration mode.

During a Cisco IOS software reload or a route processor switchover, the router may fail to query the DNS server if the interfaces are down, and the router may not wait for the interval specified using the **cable dsg name-update-interval** command to perform a DNS query. In this case, for an unresolved hostname, the router automatically performs a DNS query based on a system-defined (15 seconds) interval to facilitate faster DSG classifier updates. You cannot change the system-defined interval.

A-DSG Forwarding on the Primary Channel

You can disable A-DSG forwarding per primary capable interface using the **cable downstream dsg disable** command in interface configuration mode. Primary capable interfaces include modular, integrated cable interfaces, and Cisco cBR-8 CCAP cable interfaces.

For example, assume the cable interface 7/1/1 has A-DSG enabled and has four modular channels attached to it. However, you want A-DSG forwarding enabled only on two of these four modular channels. You can exclude the channels of your choice using the cable downstream dsg disable command. For details on how to disable modular channels, see the Disabling A-DSG Forwarding on the Primary Channel, on page 20.

Note If A-DSG downstream forwarding is disabled on a primary capable interface, the router does not create multicast service flows on the primary capable interface and stops sending Downstream Channel Descriptor (DCD) messages.

DOCSIS 3.0 DSG MDF Support

Support for DOCSIS 3.0 DSG Multicast DSID Forwarding (MDF) is introduced using DSG DA-to-DSID Association Entry type, length, value (TLV 13) in the MAC domain descriptor (MDD) message to communicate the association between a downstream service identifier (DSID) and a group MAC address used for DSG tunnel traffic. This is automatically supported on the Cisco CMTS router.

DOCSIS 2.0 hybrid CMs and DOCSIS 3.0 CMs use Dynamic Bonding Change (DBC) to get DSID information from the Cisco CMTS router, whereas DOCSIS 2.0 DSG hybrid embedded CMs and DOCSIS 3.0 DSG embedded CMs get DSID information from the Cisco CMTS router through MDD messages.

To disable MDF capability on all DSG embedded cable modems, including DOCSIS 3.0 DSG and DOCSIS 2.0 DSG hybrid modems, use the cable multicast mdf-disable command with the dsg keyword in global configuration mode.

Source Specific Multicast Mapping

Source Specific Multicast (SSM) is a datagram delivery model that best supports one-to-many applications, also known as broadcast applications. SSM is a core networking technology for the Cisco implementation of IP multicast solutions targeted for audio and video broadcast application environments.

The following two Cisco IOS components together support the implementation of SSM:

- Protocol Independent Multicast source-specific mode (PIM-SSM)
- Internet Group Management Protocol Version 3 (IGMPv3)

SSM mapping can be configured on Cisco CMTS routers.

For details on how to configure SSM mapping on a Cisco CMTS router, see the Source Specific Multicast (SSM) Mapping feature guide.

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.

Configuring the Default Multicast Quality of Service

According to DOCSIS 3.0, you must configure the default multicast quality of service (MQoS) when using the MQoS. This also applies to the DSG, which uses the MQoS by associating a service class name with the tunnel.

If the default MQoS is not configured, the DSG tunnel service class configuration is rejected. Similarly, if no DSG tunnel uses the MQoS, you are prompted to remove the default MQoS.

The CMTS selects the primary downstream channel to forward the multicast traffic when the default MQoS is configured and there is no matching MQoS group configuration. Otherwise, the wideband interface is used to forward the multicast traffic.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**configure terminal**
	
	Example:
	
	`Router# configure terminal`
	
	Example:
	
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable multicast group-qos default scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos default scn name1 aggregate`	Configures a service class name for the QoS profile.

	Command or Action	Purpose
Step 4	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Note If you configure or remove the default MQoS while the CMTS is sending multicast traffic, duplicate traffic is generated for approximately 3 minutes (or 3 times the query interval).

Configuring Global Tunnel Group Settings for Advanced-Mode DSG 1.2

This procedure configures global and interface-level commands on the Cisco CMTS router to enable DSG tunnel groups. A DSG tunnel group is used to bundle some DSG channels together and associate them to a MAC domain interface.

Global A-DSG 1.2 Tunnel Settings

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

Before You Begin

When DOCSIS Set-top Gateway (DSG) is configured to have quality of service (QoS) for tunnel, ensure that the default multicast QoS (MQoS) is also configured. For more information, see Configuring the Default Multicast Quality of Service, on page 6.

Note The DSG tunnel service class configuration is rejected, if default MQoS is not configured.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose

Step 2	**configure terminal**
	
	Example:
	
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**cable dsg tg***group-id* [**channel***channel-id* |**priority***DSG-rule-priority*] [**enable**|**disable**] **Example:** `Router(config)# cable dsg tg 1 channel 1 priority 1 enable`	Command allows the association of a group of tunnels to one or more downstream interfaces on the Cisco CMTS.
Step 4	**cabledsg tg***group-id* [**channel** *channel-id* [**ucid** *ID1*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 ucid 1`	Sets the upstream channel or channels to which the DSG 1.2 tunnel applies.
Step 5	**cable dsg tg** *group-id* [**channel** *channel-id* [**vendor-param** *vendor-group-id*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 vendor-param 1`	Sets the vendor-specific parameters for upstream DSG 1.2 channels.
Step 6	**cable dsg vendor-param** *group-id* **vendor** *vendor-index* **oui** *oui* **value** *value-in-TLV* **Example:** `Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB`	Configures vendor-specific parameters for A-DSG 1.2. To remove this configuration from the Cisco CMTS, use the no form of this command.
Step 7	**cable dsg chan-list** *list-index* **index** *entry-index* **freq** *freq* **Example:** `Router(config)# cable dsg chan-list 1 index 1 freq 47000000`	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, us the no form of this command.
Step 8	**cable dsg timer inde** [**Tdsg1** *Tdsg1*] | [**Tdsg2** *Tdsg2*] | [**Tdsg3** *Tdsg3*] | [**Tdsg4** *Tdsg4*] **Example:** `Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4`	Configures the A-DSG 1.2 timer entry to be associated to the downstream channel, and encoded into the Downstream Channel Descriptor (DCD) message. To remove the cable DSG timer from the Cisco CMTS, use the no form of this command.

	Command or Action	Purpose
Step 9	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 21.

Adding DSG Tunnel Group to a Subinterface

This procedure adds a DSG tunnel group to a subinterface using the cable dsg tg group-id command. After adding the DSG tunnel-group to a subinterface, appropriate IP Internet Group Management Protocol (IGMP) static joins are created and forwarding of DSG traffic begins, if the downstream DSG is configured.

Before You Begin

The downstream DSG should exist to create IGMP static joins.

Restriction You can associate a DSG tunnel group to only one subinterface within the same bundle interface.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

Step 2	**configureterminal**
	
	Example:
	
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 3	**interface bundle***bundle-subif-number*
	
	Example:
	
	`Router(config)# interface bundle 11.2`
	`Router(config-subif)#`
		Specifies the interface bundle and enters the subinterface configuration mode.

	Command or Action	Purpose
Step 4	**cable dsg tg***group-id* **Example:** `Router(config-subif)# cable dsg tg 1`	Adds a DSG tunnel group to a subinterface.
Step 5	end **Example:** `Router(config-subif)# end`	Returns to privileged EXEC mode.

Configuring the DSG Client Settings for Advanced-Mode DSG 1.2

After 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.

Restriction The **in-dcd ignore** option is not supported by DSG-IF-MIBS specification.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**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*]} **Example:** `Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd`	Sets the DSG client parameters. This 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.

	Command or Action	Purpose
Step 4	**cable dsg client-list** *client-list-id* **id-index** *id* [**vendor-param** *vendor-group-id*] **Example:** `Router(config-if)# cable dsg client-list 1 id-index 1 vendor-param 1`	Sets vendor-specific parameters for the DSG client.
Step 5	**cable dsg tunnel** *tunnel id* **mac_addr** *mac addr* **tg** *tunnel-group* **clients** *client-list-id* [**enable** | **disable**] **Example:** `Router(config)# cable dsg tunnel mac-addr abcd.abcd.abcd tg 1 clients 1 enable`	This command is changed to associate a tunnel group and client-list ID to a DSG tunnel. Also, an optional QoS service class name can be associated to the tunnel. **Note** To associate a cable service class with an A-DSG tunnel on a Cisco CMTS router, use the cable dsg tunnel srv-class command in global configuration mode.
Step 6	**cable dsg cfr** *cfr index* [**dest-ip** {*ipaddr* |*hostname}]* [**tunnel** *tunnel-index*][**dest-port** *start end*]| [**priority** *priority*][**src-ip** {*ipaddr* |*hostname}* [**src-prefix-len** *length*]] [**enable** | **disable**] [**in-dcd** {**yes** | **no** | **ignore**}] **Example:** `Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority 2 src-ip ciscovideo.com src-prefix-len 24 enable`	Specifies the DSG classifier index, with optional support for the DCD parameter, indicating whether or not to include the classifier in the DCD message. **Note** When you use the **ignore** option, the DSG classifier is not included in the DCD message.

Step 7	**end**
	
	Example:
	
	`Router(config)# end`
	`Router#`
		Returns to privileged EXEC mode.

What to Do Next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 21.

Configuring Downstream DSG 1.2 Settings for Advanced-Mode DSG 1.2

When 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.

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**interface cable** {*slot* /*port* |*slot* /*subslot*/*port* } **Example:** `Router(config)# interface cable 8/1/1`	Enters interface configuration mode.
Step 4	**cable downstream dsg tg** *group-id* **[channel** *channel-id]* **Example:** `Router(config-if)# cable downstream dsg tg 1 channel 1`	Associates the DSG tunnel group to the downstream interface. To remove this setting, use the **no** form of this command.
Step 5	**cable downstream dsg chan-list** *list-index* **Example:** `Router(config-if)# cable downstream dsg chan-list 2`	Associates the A-DSG channel list entry to a downstream channel, to be included in the DCD message. To remove this setting, use the **no** form of this command.
Step 6	**cable downstream dsg timer** *timer-index* **Example:** `Router(config-if)# cable downstream dsg timer 3`	Associates the DSG timer entry to a downstream channel, to be included in the DCD message. To remove this setting, use the no form of this command.
Step 7	**cable downstream dsg vendor-param** *vsif-grp-id* **Example:** `Router(config-if)# cable downstream dsg vendor-param 2`	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 no form of this command.
Step 8	**cable downstream dsg** [**dcd-enable**	**dcd-disable**]	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

	Command or Action	Purpose
	Example: `Router(config-if)# cable downstream dsg dcd-enable`	Cisco CMTS. To disable DCD messages, use the **disable** form of this command.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip multicast-routing** **Example:** `Router(config)# ip multicast-routing`	Enables multicast routing on the router.
Step 3	**ip pim ssm** {**default** | **range**{*access-list* | *word* }} **Example:** `Router(config)# ip pim ssm range 4`	Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command. **Note** When an SSM range of IP multicast addresses is defined by the **ip pim ssm** command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.
Step 4	ip cef distributed **Example:** `Router(config)# ip cef distributed`	Enables Cisco Express Forwarding (CEF) on the route processor card. To disable CEF, use the no form of this command.

	Command or Action	Purpose
		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
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for each interface bundle being used for DSG traffic.
Step 6	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} **Example:** `Router(config-if)# ip pim dense-mode`	Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature: **Note** You must configure this command on each interface that forwards multicast traffic.
Step 7	Repeat Step 5, on page 14 and Step 6, on page 14 for each cable interface that is being used for DSG traffic. Also repeat these steps on each W AN interface that is forwarding IP multicast traffic from the DSG network controllers and Conditional Access (CA) servers.	
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DNS Query and DSG Name Process

The DSG name process enables the Cisco CMTS router to query the DNS server for faster classifier updates.

Before You Begin

Ensure that the IP DNS-based hostname-to-address translation is configured on the Cisco CMTS router using the **ip domain-lookup** command in global configuration mode. This is configured by default, and the status is not displayed in the running configuration.

Procedure

	Command or Action	Purpose
Step 1	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip domain-name** *name* **Example:** `Router(config)# ip domain-name cisco.com`	Sets the IP domain name that the Cisco IOS software uses to complete unqualified host names
Step 3	r **ip name-serve***server-address*[**multiple-server-addresses**] **Example:** `Router(config)# ip name-server 131.108.1.111`	Sets the server IP address.
Step 4	**cable dsg name-update-interval***minutes* **Example:** `Router(config)# cable dsg name-update-interval 10`	Sets the interval to check the DNS server for any FQDN classifier changes.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring NAT to Support Unicast Messaging

This section describes how to configure a Cisco CMTS router for Network Address Translation (NAT) 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 cBR-8 router, A-DSG 1.2 can 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 Advanced-Mode DSG, on page 24.

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.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface** *wan-interface* **Example:** `Router(config)# interface FastEthernet0/0`	Enters interface configuration mode for the specified WAN interface.
Step 3	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Configures the WAN interface as the "outside" (public) NAT interface.
Step 4	**interface bundle** *bundle-number* **Example:** `Router(config-if)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle. **Note** This interface bundle should have previously been configured for DSG operations.
Step 5	**ip address** *ip-address mask* **secondary** **Example:** `Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary`	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	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Configures the cable interface as the "inside" (private) NAT interface.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.

	Command or Action	Purpose
Step 8	**ip nat inside source static** *ip-multicast-address cable-ip-address* **Example:** `Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2`	Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.
Step 9	Repeat Step 2, on page 16 and Step 8, on page 17 for each cable interface to be configured for DSG unicast traffic.	
Step 10	**end** **Example:** `Router(config)# end`	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, on page 13, 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/iprmc_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

http://www.cisco.com/en/US/docs/ios/12_3t/ip_mcast/command/reference/ip3_i2gt.html

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

Configuring a Standard IP Access List for Packet Filtering

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, on page 27.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* .
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle.

	Command or Action	Purpose
Step 6	**ip access-group** *access-list* **Example:** `Router(config-if)# ip access-group 90`	(Optional, but recommended) Configures the interface with the access list, so that packets are filtered by the list before being accepted on the interface. **Note** 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. **Note** On the Cisco cBR-8 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 cBR-8 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.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to Privileged EXEC mode.

Configuring a Standard IP Access List for Multicast Group Filtering

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, on page 27.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* .
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface cable** *interface* **Example:** `Router(config)# interface cable 3/0`	Enters interface configuration mode for the specified cable interface.
Step 6	**ip igmp access-group** *access-list* [*version*] **Example:** `Router(config-if)# ip igmp access-group 90`	(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.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Disabling A-DSG Forwarding on the Primary Channel

You can disable A-DSG forwarding per primary capable interface.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface modular-cable** *slot* /*subslot*/*port* :*interface-number* **Example:** `Router(config)# interface modular-cable 1/0/0:0`	Specifies the modular cable interface and enters cable interface configuration mode. Variables for this command may vary depending on the Cisco CMTS router and the Cisco IOS-XE software release.
Step 3	**cable downstream dsg disable** **Example:** `Router(config-if)# cable downstream dsg disable`	Disables A-DSG forwarding and DCD messages on the primary capable interface.
Step 4	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

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

The following commands display globally-configured or interface-level DSG settings, status, statistics, and multiple types of DSG 1.2 tunnel information.

show cable dsg cfr

To verify all DSG classifier details, such as the classifier state, source, and destination IP addresses, use the **show cable dsg cfr** command.

To verify details of a particular DSG classifier, use the **show cable dsg cfr** *cfr-id* command.

To verify the detailed output for all DSG classifiers, use the **show cable dsg cfr verbose** command.

To verify the detailed output for a single DSG classifier, use the **show cable dsg cfr** *cfr-id* **verbose** command.

show cable dsg host

To verify the mapping of the DSG hostnames and IP addresses on a Cisco CMTS router, use the **show cable dsg host** command.

To verify the verbose output of the mapping of the DSG hostnames and IP addresses on a Cisco CMTS router, use the **show cable dsg host verbose** command.

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.

To display information for a given DSG tunnel, use the **show cable dsg tunnel** *tunnel-id* 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.

show cable dsg tg

To display the configured parameters for all DSG tunnel groups, use **show cable dsg tg** command.

Note The **Chan state** column in the **show cable dsg tg** command output indicates that a channel belonging to a tunnel group is either enabled or diabled. It is possible that a tunnel group is enabled but a particular channel in that tunnel group is disabled.

To display the configured parameters for the specified tunnel group, use **show cable dsg tg** *tg-id* **channel** *channel-id* command.

To display detailed information for the specified tunnel group, use **show cable dsg tg** *tg-id* **channel** *channel-id* **verbose** command.

show running-config interface

To display a tunnel group attached to a subinterface, use the **show running-config interface** command in privileged EXEC mode, as shown in the example below:

```
Router# show running-config interface bundle 11.2
!
interface Bundle11.2
 ip address 4.4.2.1 255.255.255.0
 no ip unreachables
 ip pim sparse-mode
 ip igmp static-group 230.1.1.30
 no cable ip-multicast-echo
 cable dsg tg 61
end
```

Note The IGMP static group IP address created automatically at the time of DSG configuration is not displayed in the **show running-config interface** command output.

show cable dsg static-group bundle

To verify all DSG static groups configured under a bundle interface, use the **show cable dsg static-group bundle** command in privileged EXEC mode.

Displaying Interface-level Configurations for Advanced-Mode DSG 1.2

The following **show** commands display interface-level configurations for A-DSG 1.2.

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**

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 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 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 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.

Debugging Advanced-Mode DSG

To enable debugging for A-DSG on a Cisco CMTS router, use the debug cable dsg command in privileged EXEC mode.

Configuration Examples for Advanced-Mode DSG

This configuration example 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

Example: Enabling DNS Query

The following example shows how to enable a DNS query on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# ip domain-lookup
Router(config)# ip domain-name cisco.com
Router(config)# ip name-server 131.108.1.111
Router(config)# cable dsg name-update-interval 10
Router(config)# end
```

Example: Disabling A-DSG Forwarding on the Primary Channel

The following example shows how to disable A-DSG forwarding on a primary capable modular interface on the Cisco CMTS router:

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
Router(config-if)# cable downstream dsg disable
Router(config-if)# end
```

Additional References

The following sections provide references related to A-DSG 1.2.

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Advanced-Mode DSG 1.2 for the Cisco CMTS Routers

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

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

Table 2: Feature Information for DOCSIS Set-Top Gateway and A-DSG for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS Set-Top Gateway for the Cisco CMTS Routers	Cisco IOS-XE Release 16.5.1	This feature was integrated into Cisco IOS-XE Release 16.5.1 on the Cisco cBR Series Converged Broadband Routers.