DOCSIS Set-Top Gateway for the Cisco CMTS

This document describes the DOCSIS Set-Top Gateway (DSG) feature with its configuration and monitoring from Issue 0.9 through Issue 1.0 on the Cisco Cable Modem Termination System (CMTS).

DSG is a CableLabs® specification that allows cable headends such as the Cisco CMTS to provide a class of cable services known as out-of-band (OOB) messaging to set-top boxes (STBs) over existing Data-over-Cable Service Interface Specifications (DOCSIS) cable networks. DSG 1.0 allows cable Multi-System Operators (MSOs) and other service providers to combine both DOCSIS and STB operations over a single, open and vendor-independent network without requiring any changes to the existing DOCSIS network infrastructure.

At the time of this Cisco publication, the CableLabs® DOCSIS DSG specification is in the current status of "Issued" as characterized by stability, rigorous review in industry and cross-vendor interoperability. The latest version of this developing specification is available at the following locations:

- http://www.cablemodem.com/specifications/gateway.html
- http://www.opencable.com/downloads/specs/SP-DSG-I01-020228.pdf

Feature Specifications for DOCSIS Set-Top Gateway

Feature History	
Release	**Modification**
Release 12.3(9a)BC	This feature was introduced for the Cisco uBR10012 universal broadband router. The following DSG 1.0 features are supported for each Cisco CMTS platform: • Vendor names are supported to 20 characters per SNMP requirements. • SNMP MIB support introduced for the DSG-IF-MIB. • Multicast MAC addresses are supported for DSG tunnels. DSG tunnel MAC addresses are no longer limited only to unicast addresses. • DSG 1.0 prevents the configuration of any reserved or otherwise inappropriate IP multicast addresses.
Release 12.2(15)BC2	This feature was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.

Finding Support Information for Platforms and Cisco IOS Software Images

Use Cisco Feature Navigator to find information about platform support and Cisco IOS software image support. Access Cisco Feature Navigator at http://www.cisco.com/go/fn. You must have an account on Cisco.com. If you do not have an account or have forgotten your username or password, click **Cancel** at the login dialog box and follow the instructions that appear.

Contents

Prerequisites for DOCSIS Set-Top Gateway

General Prerequisites

- With Cisco uBR7100 series and Cisco uBR7246VXR routers, the Cisco CMTS must be running Cisco IOS Release 12.2(15)BC2 or later Cisco IOS 12.2 BC release.
- With the Cisco uBR10012 router, the Cisco CMTS must be running Cisco IOS Release 12.3(9a)BC or later Cisco IOS 12.3 BC release.
- Set-top boxes must support the CableLabs DSG specifications through Version 1.0, available at the following locations:
  - *DOCSIS Set-top Gateway (DSG) Interface Specification*, SP-DSG-I01-020228

    http://www.cablemodem.com/specifications/gateway.html

    http://www.opencable.com/downloads/specs/SP-DSG-I01-020228.pdf

IP Multicast Prerequisites

- IP multicast routing must be enabled on the Cisco router for proper DSG operations. To enable IP multicast routing, use the **ip multicast-routing** command in global configuration mode.
- Protocol Independent Multicast (PIM) must be enabled on the cable interface and all outgoing WAN interfaces, using the **ip pim** interface command, before enabling and configuring the DOCSIS Set-Top Gateway feature. The DOCSIS Set-Top Gateway feature supports the following PIM modes:

  - **sparse-mode**—Sparse mode of operation.
  - **sparse-dense-mode**—The interface is treated in either sparse mode or dense mode of operation, depending on the mode in which the multicast group is operating.
  - **dense-mode**—Dense mode of operation.
- For best performance, Cisco recommends enabling fast switching of IP multicast on incoming and outgoing interfaces, using the **ip mroute-cache** command.
- (Optional) Multicast rate-limiting can be enabled on those cable interfaces that are configured for DSG operations, using the **ip multicast rate-limit out group-list** command.
- (Optional) To restrict which multicast groups can be seen by the hosts, use the **ip igmp access-group** command to selectively disable multicast groups from being seen by the set-top-boxes.

Tip For information on the IGMP multicast commands, see the documents listed in the "Additional References" section on page 34.

Restrictions for DOCSIS Set-Top Gateway

Restrictions for DSG Issue 0.9

Cisco IOS Release 12.2(15)BC2 has the following limitations for DSG Issue 0.9:

- You may have up to four separate conditional access (CA) vendors per router.
- Vendor names must be unique and are supported to a maximum of seven characters.
- Each CA vendor can have one or more DSG tunnels on each cable interface, up to the maximum of eight tunnels per vendor.
- You may have a maximum of eight DSG tunnels (as identified by the well-known MAC address) per CA vendor, for a maximum possible total of 32 DSG tunnels per router.
- DSG traffic should be less than 2.048 Mbps per vendor, so as to conform to the DSG specifications.
- If using bundled interfaces, configure the DSG configurations only on the master interface, not on the slave interfaces. However, when DSG has been properly configured on the master interface, DSG traffic can flow across both the master and slave interfaces.
- The DOCSIS Set-Top Gateway feature does not support one-to-many mappings (one IP multicast group for multiple DSG tunnels). This means that multiple CA vendors cannot use the same DSG tunnel — two vendors cannot be using a tunnel with the same IP multicast address.
- Cisco IOS Release 12.2(15)BC2 does not support the DOCSIS-SETTOP-GATEWAY-MIB in this initial implementation of the DOCSIS Set-Top Gateway feature.
- In Cisco IOS Release 12.2(15)BC2, N+1 HCCP high-availability redundancy does not preserve the DSG traffic and configuration after a switchover. If you configure a cable interface for both N+1 HCCP redundancy and for DSG operations, DSG traffic does not continue after a switchover.
- The Cisco uBR10012 router does not support DSG with this Cisco IOS release.

General Restrictions for DSG Issue 1.0

The following general restrictions apply to DSG Issue 1.0 on Cisco uBR7100 series, Cisco uBR7200 series and Cisco uBR10012 routers and the Cisco IOS 12.3(9a)BC release:

- You may have up to four separate conditional access (CA) vendors per router.
- Vendor names must be unique and are supported to a maximum of 20 characters.
- You may have a maximum of eight DSG tunnels (as identified by the well-known MAC address) per CA vendor, for a maximum possible total of 32 DSG tunnels per router.
- DSG traffic should be less than 2.048 Mbps per vendor, so as to conform to the DSG specifications.
- If using bundled interfaces, you must configure the DSG configurations only on the master interface, not on the slave interfaces. Error messages occur if you configure tunnels in the slave interface.
- If an interface that has DSG tunnels is configured as a slave, the DSG tunnels configured in that interface are removed.
- In DSG 1.0, you cannot configure DSG tunnels in subinterfaces or main interfaces that have subinterfaces.
- DSG does not support N+1 functionality.

Unicast Restrictions for DSG Issues 0.9 and 1.0

- DSG-related IP unicast traffic is supported only by configuring Network Address Translation (NAT) on the cable and WAN interfaces, as described in the "Configuring NAT to Support Unicast Messaging (optional)" section on page 14. If this is not done, the CMTS receives the unicast traffic from the DSG network controllers, but it does not forward that traffic to the set-top boxes.

Multicast Restrictions for DSG Issues 0.9 and 1.0

- You cannot create use the same IP multicast groups for both DSG traffic and for other IP multicast traffic. If an IP multicast group is being used for DSG traffic, do not use the **ip igmp static-group** command to manually configure that same IP multicast group for other, non-DSG traffic.
- Different CA vendors cannot share IP multicast addresses. Each vendor must use a unique set of IP multicast addresses, and after an IP multicast address is assigned to a DSG tunnel, that same address cannot be used for any other purpose. However, all other multicast addresses and groups can still be used on the interface for other multicast applications.
- DSG does not support BPI-encrypted IP multicast streams.
- DSG-related IP multicast rate shaping is not supported.

Information About DOCSIS Set-Top Gateway

This section describes the DOCSIS Set-Top Gateway feature:

Feature Overview

The DOCSIS Set-Top Gateway (DSG) feature allows the Cisco CMTS to provide a class of cable services known as out-of-band (OOB) messaging to set-top boxes (STBs) over existing DOCSIS networks. This allows MSOs and other service providers to combine both DOCSIS and STB operations over one, open, vendor-independent network, without any change to the existing network or cable modems.

Out-of-Band Messaging

Out-of-band (OOB) messages allow network control and management messages to be sent to customer premises equipment (CPE) devices, without interfering with the normal data traffic flow. OOB messages also have an advantage over in-band messages in that OOB messages are not dependent on the type of traffic or applications being sent over the network. This allows new OOB messages to be developed and implemented, without requiring any corresponding changes in the network application software.

Previously, OOB messages have been carried over dedicated channels that use proprietary video standards such as SCTE/DVS-167, SCTE/DVS-178, and DVB-RCCL/DAVIC-RCC. These existing systems have the following limitations:

- Multi-System Operators (MSOs) and other service providers are locked into legacy systems that require proprietary application servers and STBs, which might require additional licensing fees and service charges.
- Existing OOB messages (DVS167/178) are delivered over legacy transport mechanisms that are not adaptable for future service offerings.
- Upstream performance limitations (a maximum of 256 kbps) are unsuitable for large-scale deployment of a variety of interactive, real-time services.

To respond to these limitations, the CableLabs consortium developed the DSG specification to provide a multi-vendor solution that works with both legacy STB and DOCSIS transport paths. This allows MSOs and other service providers to use their legacy systems and STBs over their existing DOCSIS cable plants, while still preparing for DSG-capable STBs that support applications such as Video-on-Demand (VoD), online gaming and other interactive services.

DSG systems allow a wide variety of OOB messages, such as the following standard messages, in addition to generic and vendor-defined messages:

- Conditional Access (CA) messages, to identify which programs and services a user is entitled to receive.
- System Information (SI) messages for the management of the STB and its channels.
- Electronic program guide (EPG) to provide up-to-date program information for STB services and programs.

Basic Structure of a DSG Network

The DOCSIS Set-Top Gateway feature implements the DSG specification on the Cisco CMTS platform, allowing a Cisco CMTS to support both STBs and cable modems over the existing DOCSIS cable network. The CMTS creates a one-way IP datagram channel, called a DSG tunnel, to transport OOB messages to the STBs, allowing the consolidation of cable modem and STB traffic over the same DOCSIS downstream channel.

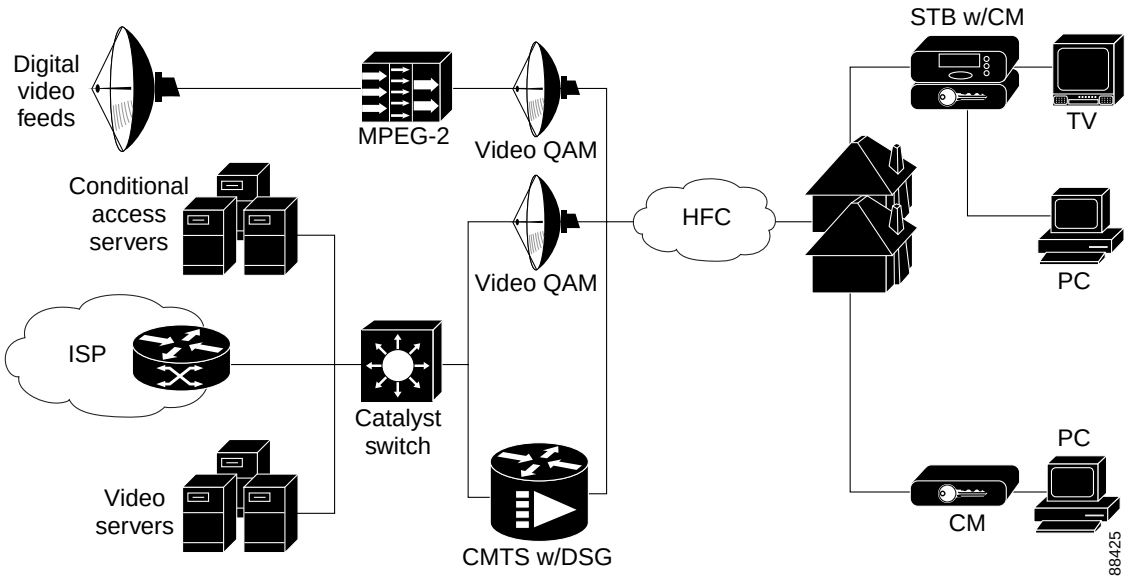
A typical DSG network contains the following components:

- Customer Premises Equipment (CPE)—Set-top box or computer that receives the cable signals coming from the cable modem termination system (CMTS).
- Set-Top Box (STB)—Customer premises equipment (CPE) that can access subscription and pay-per-view broadcast television services and interactive TV services. In a DSG network, each STB is a member of one or more multicast groups, which allows the STB to receive the OOB messages that are needed to receive the programs they are authorized to view.
- Point of Deployment (POD) module—Removable security card that is plugged into a STB to uniquely identify and authenticate the STB. This allows the CA servers to securely identify the STB and determine which programs and services it is authorized to receive.
- Network Controller—Network controllers originate out of band (OOB) DSG messages whose destinations are STBs.
- Conditional Access Server—Server systems that encrypt video programs using conditional access (CA) techniques so that only authorized subscribers are able to decrypt and view the programs. Typically, each vendor providers their own CA servers, which also maintain the other back office support systems that are necessary for billing and network management of the STBs.
- DSG Gateway—CMTS that forwards the DSG traffic from the network controllers to STBs.
- DSG Tunnel—This is an IP multicast datagram stream originating at the DOCSIS Set-Top Gateway and carrying out-of-band messages intended for set-top terminals. It is carried over the downstream DOCSIS channel and is identified by a well-known Ethernet MAC address. The well-known Ethernet unicast MAC address is reserved and published by the CA/POD provider. Multiple DSG tunnels may exist on a single downstream DOCSIS channel.

The CA servers transmit OOB messages on the network using multicast IP packets, which are received by STBs that are members of the appropriate multicast groups.

Figure 1 shows a typical DSG network.

Figure 1 DSG Network Diagram



Using Point of Deployment Modules and DSG Tunnels

CA vendors typically provide a Point of Deployment (POD) security module to each set-top box customer. Each POD contains a unique ID and a unique X.509 digital certificate that allows the CA/POD vendor's provisioning systems to securely identify and authenticate each set-top box.

Having securely identified and authenticated a set-top box, the CA/POD vendor transmits the OOB messages to the STB over a DSG tunnel, which is an IP multicast datagram stream carried over the DOCSIS downstream channel. Each DSG tunnel is identified by a well-known Ethernet unicast address that is reserved and published by the CA/POD vendor.

The CA/POD vendors can use the different DSG tunnels to provide different services. For example, one CA/POD vendor could define one tunnel for an Electronic Program Guide (EPG), another tunnel for conditional access (CA) programming, a third tunnel for emergency alerts, and a fourth tunnel for software upgrades. Other vendors can define their tunnels in different ways to provide other services.

DSG Addressing

The DOCSIS Set-Top Gateway feature uses the following types of addressing to ensure that the proper OOB messages are delivered to the appropriate STBs:

- Well-known MAC address—Defines the DSG tunnel being used. Each CA/POD vendor reserves and publishes one or more well-known MAC addresses that it uses for its particular services. The POD security modules from that vendor instruct the STB examine packets for one or more of the vendor's MAC addresses. If a packet has the correct well-known MAC address, the STB reads that particular packet.
- IP Multicast address—Each STB is a member of at least one multicast group. The STB itself does not use these IP addresses, but the Cisco CMTS uses these IP multicast addresses to perform the appropriate multicast joins for the appropriate STBs. This ensures that the STB receives the traffic that is appropriate for its multicast group.

The Cisco CMTS router supports an unlimited number of destination multicast addresses, which can be mapped to MAC addresses as follows:

- One-to-one mapping—One IP multicast group per one DSG tunnel (MAC address)
- Many-to-one mapping—Multiple IP multicast groups per one DSG tunnel (MAC address)

Note Cisco IOS Release 12.2(15)BC2 does not support one-to-many mappings (one IP multicast group per multiple MAC addresses/DSG tunnels). This means that multiple CA vendors cannot use the same DSG tunnel (that is, two vendors on the same interface cannot be using a tunnel with the same IP multicast address).

DSG Operation

DSG maps traffic based on the incoming multicast address or a well-known unicast address. The Cisco CMTS performs the following functions when the CMTS receives an OOB packet from the CA servers over the IP network:

1. The CMTS looks at the destination address (either the multicast group address or the well-known unicast address that the network controller and the CMTS agree on).
2. If the destination IP address matches the multicast group or the unicast address that will be translated via NAT, then MAC addresses for the packet are overwritten.
3. The CMTS then forwards the new packet on the downstream ports that are mapped to those well-known MAC addresses, using either a unicast or multicast broadcast, as appropriate.

4. The STBs on those downstreams receive the packet and examine the IP address. If the STB belongs to a multicast group that matches this multicast IP address, the STB examines the packet's MAC address.
5. If the MAC address is a well-known MAC address for the appropriate CA/POD vendor, the STB reads the packet and operates on the OOB messages that it contains.

Feature List

Cisco IOS Release 12.3(9a)BC introduces support for DOCSIS Set-Top Gateway (DSG) Issue 1.0 on the following Cisco CMTS platforms:

- Cisco uBR10012 universal broadband router
- Cisco uBR7246VXR universal broadband router
- Cisco uBR7100 series universal broadband router

DSG Issue 1.0 improves upon Issue 0.9 in the following ways:

- Performance enhancements through the Cisco uBR10012 PRE2 route processing engine
- Support for theCISCO-CABLE- DSG-IF-MIB for SNMP
- Support both unicast and multicast MAC addresses for DSG tunnels

In Cisco IOS Release 12.2(15)BC2, the DOCSIS Set-Top Gateway feature provides the following features:

- Provides one-way downstream transport of OOB messages.
- Supports multiple CA systems.
- Provides transparent transport of OOB messages to DOCSIS STBs over a maximum of eight DSG tunnels per vendor, using the existing DOCSIS 1.0/1.1 cable network.
- Supports four concurrent CA/POD vendors per router.
- Supports well-known MAC addresses for CA/POD vendor. These can include any or all of the following existing services:
  - Conditional Access Services (CAS)
  - Configuration/Maintenance
  - Electronic Program Guide (EPG)
  - Emergency Alert System (EAS)
  - Software Download
  - System Information (SI)
- Optionally supports mapping to Internet Group Management Protocol (IGMP) multicast tunnels (using RFC 1112 IP to MAC address translation), in addition to mapping to DSG multicast tunnels.
- One DSG tunnel can receive OOB messages from multiple IP addresses, over any type of IP network connection.
- Uses existing DOCSIS 1.0, DOCSIS 1.1, or DOCSIS 2.0 cable networks.
- Supports existing provisioning systems. STBs do not need to register with the CMTS using a DOCSIS ranging and registration sequence, nor do STBs need to obtain an IP address. The CMTS does not need to know the STB's native Ethernet MAC address.
- Supports the transmission of OOB messages to multiple STBs using IP multicast.

- DSG tunnels are transparent to the application data. You do not need to change existing applications or data streams to use the DOCSIS Set-Top Gateway feature.
- Supports using IP and IGMP access lists to provide a way of determining which IP packets are forwarded to the DSG tunnels and which are dropped. IP access lists can provide packet filtering and rate-limiting, while IGMP access lists can provide filtering on IP multicast groups.

Benefits

The DOCSIS Set-Top Gateway feature provides the following benefits to cable MSOs, service providers, and their partners and customers.

Part of CableLabs Specifications

The DOCSIS Set-Top Gateway feature is a CableLabs (http://www.cablelabs.com) specification allows cable MSOs and service providers to create and deploy new interactive services over existing cable networks. Providers can introduce new services, without impacting their existing customers.

Supports Existing DOCSIS Cable Networks

The DOCSIS Set-Top Gateway feature interoperates with existing DOCSIS-capable networks that can support new interactive services, such as VoD and online gaming, that are expected to become available on cable networks in the future. DOCSIS cable operators can deploy innovative interactive services using the best of the available advanced STB products and middleware and applications software, while still preserving their investment in existing headend systems.

Provides Additional Services

The DOCSIS Set-Top Gateway feature allows cable operators to offer Internet access, e-mail, chat services, and other high-bandwidth services, in addition to the existing STB services (such as EPG and CA). Providers can deliver high-speed data services to their cable TV subscribers using the DOCSIS network.

Provides the Capability to Use Multiple CA/POD Vendors

The DOCSIS Set-Top Gateway feature allows cable operators to offer services from many CA/POD vendors, as opposed to existing networks that typically limit the operator to only one vendor per network. This allows greater flexibility in combining or sharing operations between operators or providers.

Uses Standard DOCSIS Networks

The DOCSIS Set-Top Gateway feature uses existing DOCSIS 1.0, DOCSIS 1.1, and DOCSIS 2.0 networks. MSOs and other service providers can continue to create open-standard, vendor-independent DOCSIS networks, without having to maintain legacy STB systems that could disrupt DOCSIS operations.

Simplifies Network Operations and Cost

MSOs and other service providers can use one simplified return channel architecture to support both STBs and DOCSIS cable modems, instead of using two separate return channels. This lowers the complexity of managing CPE devices and requires less investment in headend equipment, which in turn lowers the overall operations and support costs.

Supports Higher Density of STBs

Depending on the CMTS platform, the higher bandwidth available in DOCSIS networks allows MSOs and other service providers to support a higher maximum number of STBs per headend system.

How to Configure the DOCSIS Set-Top Gateway Feature

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

Note All procedures begin and end at the privileged EXEC prompt (`Router#`).

Enabling and Configuring the DOCSIS Set-Top Gateway Feature

This section describes how to enable and configure the DOCSIS Set-Top Gateway on one or more cable interfaces.

SUMMARY STEPS

1. **configure terminal**
2. **interface cable** *interface*
3. **cable dsg** *tunnel-MAC-address group-ip-address CA-vendor-name*
4. **exit**
5. **cable dsg keepalive**
6. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**`configure terminal`**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**`interface cable`** *`interface`*
	
	Example:
	`Router(config)# interface cable 3/0`
	`Router(config-if)#`
		Enters interface configuration mode for the specified cable interface.
		
		Note You can also specify a cable subinterface. If using subinterfaces, though, you should configure DSG operations only on the subinterfaces (and preferably only one subinterface), and not on the main interface.

	Command or Action	Purpose

Step 3	**cable dsg** *tunnel-MAC-address group-ip-address CA-vendor-name*
	
	Example:
	`Router(config-if)# cable dsg 0010.0025.0025 224.3.3.105 AAA`
	`Router(config-if)# cable dsg 0006.0006.0006 224.4.4.1 BBB`
	`Router(config-if)# cable dsg 0010.0001.0001 224.4.4.4 CCC`
	`Router(config-if)#`
		Configures the cable interface for DSG operations, using the following parameters to create the DSG tunnel:
		• *tunnel-MAC-address* = Well-known MAC address for the DSG tunnel. If the MAC address is 0.0.0, the DSG tunnel will create a one-way multicast tunnel, using the RFC 1112 algorithm for converting host group addresses to Ethernet MAC addresses.
		• *group-ip-address* = The multicast group IP address that is mapped to the specified tunnel for the DSG stream. You can specify only globally-scoped (224.0.1.0 through 238.255.255.255) and administratively-scoped (239.0.0.0 through 239.255.255.255) addresses. You cannot use local scope addresses (224.0.0.0 through 224.0.0.255).
		• *CA-vendor-name* = Unique name (up to 20 characters) for the Conditional Access (CA) vendor that owns the DSG tunnel. (You can support up to four vendors per router.)

	Note Repeat Step 2 and Step 3 for each cable interface and DSG tunnel to be configured.	

Step 4	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode.

Step 5	**cable dsg keepalive**
	
	Example:
	`Router(config)# cable dsg keepalive`
	`Router(config)#`
		(Optional) Enables keepalive messages over DSG tunnels on all cable interfaces. The default is **no cable dsg keepalive**, which disables the keepalive messages.
		Note Do not enable keepalive messages on the DSG tunnels unless you have found that your applications and set-top boxes require these messages.

Step 6	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode and 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.

SUMMARY STEPS

1. **configure terminal**
2. **ip multicast-routing**
3. **interface** *interface*
4. **ip pim** {**dense-mode** | **sparse-dense-mode** | **sparse-mode**}
5. **ip multicast rate-limit out group-list** *access-list rate*
6. **ip mroute-cache**
7. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**ip multicast-routing**
	
	Example:
	`Router(config)# ip multicast-routing`
	`Router(config)#`
		Enables multicast routing on the router.

Step 3	**interface** *interface*
	
	Example:
	`Router(config)# interface cable 3/0`
	`Router(config-if)#`
		Enters interface configuration mode for each cable interface or WAN interface being used for DSG traffic.

Step 4	**ip pim** {**dense-mode** | **sparse-dense-mode** | **sparse-mode**}
	
	Example:
	`Router(config-if)# ip pim dense-mode`
	`Router(config-if)#`
		Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature:
		• **sparse-mode**—Enables sparse mode of operation.
		• **sparse-dense-mode**—The interface is treated in either sparse mode or dense mode of operation, depending on which mode the multicast group operates in.
		• **dense-mode**—Enables dense mode of operation.
		Note You must configure this command on each interface that forwards multicast traffic.

	Command or Action	Purpose

Step 5	**ip multicast rate-limit out group-list** *access-list rate*
	
	Example:
	`Router(config-if)# ip multicast rate-limit out group-list 10 2048`
	`Router(config-if)#`
		(Optional) Enables multicast rate-limiting on the cable interface, using the following parameters:
		• **group-list** *access-list* = Access list number or name that controls which multicast groups are subject to the rate limit.
		• *rate* = Maximum transmission rate (in kbps). Any packets sent at greater than this value are silently discarded. The valid range is 0 to 4294967 kbps, but for DSG operations the maximum valid rate is 2048 kbps. The default is 0, which means no traffic is permitted.

Step 6	**ip mroute-cache**
	
	Example:
	`Router(config-if)# ip mroute-cache`
	`Router(config-if)#`
		(Optional) Enables IP multicast fast switching, also known as multicast distributed switching (MDS), on the interface.

	Note Repeat Step 3 through Step 6 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.	

Step 7	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router#`
		Exits interface configuration mode and returns to privileged EXEC mode.

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.

Tip This procedure should be performed after the cable interface has already been configured for DSG operations, as described in the "DSG Configuration Example" section on page 27.

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

Step 2	`interface` *`wan-interface`*
	
	Example:
	`Router(config)# interface FastEthernet0/0`
	`Router(config-if)#`
		Enters interface configuration mode for the specified WAN interface.

Step 3	`ip nat outside`
	
	Example:
	`Router(config-if)# ip nat outside`
	`Router(config-if)#`
		Configures the WAN interface as the "outside" (public) NAT interface.

	Command or Action	Purpose

Step 4	**interface cable** *interface*
	
	Example:
	`Router(config-if)# interface cable 3/0`
	`Router(config-if)#`
		Enters interface configuration mode for the specified cable interface.
		
		Note This cable interface should have previously been configured for DSG operations, as described in Enabling and Configuring the DOCSIS Set-Top Gateway Feature, page 10.

Step 5	**ip address** *ip-address mask* **secondary**
	
	Example:
	`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	**ip nat inside**
	
	Example:
	`Router(config-if)# ip nat inside`
	`Router(config-if)#`
		Configures the cable interface as the “inside” NAT (private) interface.

Step 7	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router(config)#`
		Exits interface configuration mode and returns to global configuration mode.

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`
	`Router(config)#`
		Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.
		
		• *ip-multicast-address* = This address should match the multicast address that was used when enabling DSG on the cable interface in Enabling and Configuring the DOCSIS Set-Top Gateway Feature, page 10.
		• *cable-ip-address* = This address should match the IP address of the incoming unicast packet.

	Note Repeat Step 2 and Step 8 for each cable interface to be configured for DSG unicast traffic.	

Step 9	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

Disabling the DOCSIS Set-Top Gateway Feature

This section describes how to disable the DOCSIS Set-Top Gateway feature on one or more cable interfaces.

SUMMARY STEPS

1. **configure terminal**
2. **interface cable** *interface*
3. **no cable dsg** *tunnel-MAC-address group-ip-address CA-vendor-name*
4. **exit**

DETAILED STEPS

	Command or Action	Purpose

Step 1	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		Enters global configuration mode.

Step 2	**interface cable** *interface*
	
	Example:
	`Router(config)# interface cable 3/0`
	`Router(config-if)#`
		Enters interface configuration mode for the specified cable interface.

Step 3	**no cable dsg** *tunnel-MAC-address group-ip-address CA-vendor-name*
	
	Example:
	`Router(config-if)# no cable dsg`
	`Router(config-if)#`
		Disables the DSG tunnel and removes its configuration from the cable interface.
		
		Note This command also automatically removes the IGMP static multicast group that is associated with this DSG tunnel. You do not need to manually remove the group using the **no ip igmp static-group** command.

	Note Repeat Step 2 and Step 3 for each cable interface to be configured.	

Step 4	**exit**
	
	Example:
	`Router(config)# exit`
	`Router#`
		Exits global configuration mode and returns to privileged EXEC mode.

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	`configure terminal`
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		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`
	`Router(config)#`
		Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask*.
		• *access-list* = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.
		• *group-ip-address* = 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.
		• *mask* = (Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.

	Command or Action	Purpose

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`
	`Router(config)#`
		Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask*.
		• *access-list* = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.
		• *group-ip-address* = 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.
		• *mask* = (Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.

Step 4	**access-list** *access-list* **deny any**
	
	Example:
	`Router(config)# access-list 90 deny any`
	`Router(config)#`
		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`
	`Router(config-if)#`
		Enters interface configuration mode for the specified cable interface.

Step 6	**ip access-group** *access-list*
	
	Example:
	`Router(config-if)# ip access-group 90`
	`Router(config-if)#`
		(Optional, but recommended) Configures the interface with the access list, so that packets are filtered by the list before being accepted on the interface.
		• *access-list* = 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 Step 3.

Step 7	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router#`
		Exits interface configuration mode and returns to Privileged EXEC mode.

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	**configure terminal**
	
	Example:
	`Router# configure terminal`
	`Router(config)#`
		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`
	`Router(config)#`
		Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask*.
		• *access-list* = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.
		• *group-ip-address* = 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.
		• *mask* = (Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.

	Command or Action	Purpose

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`
	`Router(config)#`
		Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask*.
		• *access-list* = Number or name of a standard IP access list. The number can range from 1 to 99 with no default.
		• *group-ip-address* = 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.
		• *mask* = (Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.

Step 4	**access-list** *access-list* **deny any**
	
	Example:
	`Router(config)# access-list 90 deny any`
	`Router(config)#`
		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`
	`Router(config-if)#`
		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`
	`Router(config-if)#`
		(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.
		• *access-list* = 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 Step 3.
		• *version* = (Optional) Specifies the IGMP version. The default is 2.

Step 7	**exit**
	
	Example:
	`Router(config-if)# exit`
	`Router#`
		Exits interface configuration mode and returns to privileged EXEC mode.

Monitoring the DOCSIS Set-Top Gateway Feature

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

Displaying a DOCSIS Set-Top Gateway Tunnel Configuration

To display the mapping table for a specific DSG tunnel, use the **show cable dsg** command in privileged EXEC mode. You can display information about DSG statistics and about DSG tunnels. The following examples are typical displays of each command:

The following example displays the mapping table for all DSG tunnel MAC addresses in Cisco IOS Release 12.3(9a)BC:

```
Router# show cable dsg tunnel

Group-ip        Src-ip          Tunnel-MAC      Interface   Packets   CA-vendor
239.0.0.112     *               0010.18ff.ff00  Cable6/0    0         nds
239.0.0.113     *               0010.18ff.ff00  Cable6/0    0         nds
224.1.1.1       *               0001.0001.0001  Cable6/0    0         abc
224.1.1.2       *               0001.0001.0002  Cable6/0    0         abc
224.1.1.3       *               0001.0001.0003  Cable6/0    0         abc
224.1.1.4       *               0001.0001.0004  Cable6/0    0         abc
224.1.1.5       *               0001.0001.0005  Cable6/0    0         abc
224.1.1.6       *               0001.0001.0006  Cable6/0    0         T5 t6
```

The following example displays the mapping table for the specified DSG tunnel MAC address:

```
Router# show cable dsg tunnel 0009.0009.0009

Group-ip        Src-ip          Tunnel-MAC      Interface   Packets   CA-vendor
224.13.13.1     *               0009.0009.0009  Cable5/0    0         AAA
224.12.12.1     *               0009.0009.0009  Cable5/0    0         AAA
```

The following example displays the statistics for all DSG vendor tunnels in Cisco IOS Release 12.3(9a)BC:

```
Router# show cable dsg stats
Vendor: bg, Tunnel count: 8
  0004.0004.0004
    229.4.4.4
      Cable8/1/0                Resolves: 27            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0002
    229.1.1.2
      Cable8/1/0                Resolves: 19            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0003
    229.1.1.3
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0004
    229.1.1.4
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0005
    229.1.1.5
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0006
    229.1.1.6
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0007
    229.1.1.7
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0001.0008
    229.1.1.8
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
```

```
Vendor: t, Tunnel count: 8
  0000.0000.0001
    230.0.0.1
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0002
    230.0.0.2
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0003
    230.0.0.3
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0004
    230.0.0.4
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0005
    230.0.0.5
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0006
    230.0.0.6
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0007
    230.0.0.7
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0000.0000.0008
    230.0.0.8
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0

Vendor: bg2, Tunnel count: 7
  0001.0002.0008
    229.1.2.8
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0002.0007
    229.1.2.7
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0002.0005
    229.1.2.5
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0002.0004
    229.1.2.4
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0002.0003
    229.1.2.3
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0002.0002
    229.1.2.2
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0
  0001.0002.0001
    229.1.2.1
      Cable8/1/0                Resolves: 11            Rcv/Fwd/Drp: 0/0/0


Vendor: nds, Tunnel count: 1
  dead.beaf.fefe
    239.0.0.113
      Cable8/1/0                Resolves: 39            Rcv/Fwd/Drp: 0/0/0

Router#
```

The following example displays the statistics for the specified DSG vendor tunnel in Cisco IOS Release 12.3(9a)BC:

```
Router# show cable dsg stats 0001.0001.0001

DSG statistics information

Vendor name is abc, tunnel MAC is 0001.0001.0001
Group address is 224.1.1.1, source address is *
  Interface is Cable6/0,   mapping entry is used 0
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets
```

Note The packet counters are automatically reset to zero for a tunnel when the tunnel does not receive any traffic for three minutes or more.

Displaying All DOCSIS Set-Top Gateway Tunnel Configurations

To display the currently configured DSG tunnels on all interfaces, use the **show cable dsg** command in privileged EXEC mode. You can display information about DSG keepalive settings, statistics and DSG tunnels.

Examples from DSG 1.1 and Cisco IOS Release 12.3(X)BC

The following example illustrates the **show cable dsg tunnel** command for DSG Issue 1.1 on the Cisco uBR10012 router:

```
show cable dsg <tunnel mac addr | interface>
=============================================


Tunnel                                  Classifier
MAC Addr       Interface Srv-Class  Dst-IP      Pri   Src-IP     Packets
0004.0004.0004 C8/1/0    srvclassA  229.4.4.4   0     100.1.1.1  99
                                     229.4.4.5   1     100.1.1.2  99
```

The following example illustrates the **show cable dsg rule** command for DSG Issue 1.1 on the Cisco uBR10012 router:

```
Router# show cable dsg rule c8/1/0

Rule       UCID       Client  Tunnel  Vender      Classifier
ID     Pri Interface  Range   ID      ID   ID      Dst-IP Pri        Src-IP
1    1   C8/1/0  1-4  1       1       1    229.4.4.4  0   100.1.1.1  229.4.4.5 1 100.1.1.2

show cable dsg rule <interface>
===============================


Rule                 UCID    Client  Tunnel  Vender       Classifier
  ID     Pri Interface Range     ID      ID      ID     Dst-IP      Pri
Src-IP
1       1   C8/1/0    1-4      1       1       1       229.4.4.4   0
100.1.1.1
                                                         229.4.4.5   1
100.1.1.2
```

The following example illustrates the **show cable dsg rule** command for DSG Issue 1,1 on the Cisco uBR10012 router:

```
show cable dsg stats <tunnel mac addr | interface>
=================================================
0004.0004.0004 229.4.4.4 C8/1/0 DCD Sent: 99 DCD Change Count: 7
   Resolves: 10    Rcv/Fwd/Drp: 0/0/0
```

Examples from DSG 1.0 and Cisco IOS Release 12.3(9)

The following examples illustrate **show cable dsg** commands with Cisco IOS Release 12.3(9a)BC and DSG Issue 0.9:

```
Router# show cable dsg ?
  keepalive  Show DSG keepalive status
  stats      Show statistics information of DSG
  tunnel     Show DSG tunnel table
```

```
Router# show cable dsg keepalive
DSG keeplive is disabled, keepalives transmitted: 0

Router# show cable dsg stats
Vendor: bg, Tunnel count: 1
  0004.0004.0004
    229.4.4.4
      Cable8/1/0                Resolves: 0             Rcv/Fwd/Drp: 0/0/0

Router# show cable dsg tunnel
Dst-ip          Src-ip          Tunnel-MAC     Interface  Packets       Vendor
229.4.4.4       *               0004.0004.0004 Cable8/1/0 0             bg

Router# show cable dsg tunnel ?
  H.H.H   A DSG tunnel MAC address
  vendor  Show dsg tunnels for the specific vendor
  |       Output modifiers
  <cr>

Router# show cable dsg tunnel 0004.0004.0004
Dst-ip          Src-ip          Tunnel-MAC     Interface  Packets       Vendor
229.4.4.4       *               0004.0004.0004 Cable8/1/0 0             bg
```

The following examples illustrate **show cable dsg** commands with Cisco IOS Release 12.3(9a)BC and DSG Issue 1.0 with enhanced syntax on a Cisco uBR10012 router:

```
Router# show cable dsg stats 0050.4d00.0002
DSG statistics information

DSG keepalive is set

Vendor name is nds, tunnel MAC is 0050.4d00.0002
Group address is 224.1.2.3, source address is *
  Interface is Cable6/0,  interface Cable6/0 is bundle master
  mapping entry is used 85
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets
```

The following examples illustrate **show cable dsg** commands with Cisco IOS Release 12.3(9a)BC and DSG Issue 1.0 with enhanced syntax on a Cisco uBR7246VXR router:

```
stb-cmts# show cable dsg tunnel
Group-ip        Src-ip          Tunnel-MAC      Interface   Packets   CA-vendor
224.1.2.3       *               0050.4d00.0002  Cable6/0    0         nds


stb-cmts# show cable dsg tunnel 0050.4d00.0002
Group-ip        Src-ip          Tunnel-MAC      Interface   Packets   CA-vendor
224.1.2.3       *               0050.4d00.0002  Cable6/0    0         nds

Router# show cable dsg stats
DSG statistics information

DSG keepalive is set

Vendor: nds, Tunnel count: 1

Vendor name is nds, tunnel MAC is 0050.4d00.0002
Group address is 224.1.2.3, source address is *
  Interface is Cable6/0,  interface Cable6/0 is bundle master
  mapping entry is used 85
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets
```

Examples from DSG Issue 0.9

```
Router# show cable dsg tunnel

Dst-ip:         Src-ip:      Tunnel-MAC:        interface:  packets:  vendor:
229.2.0.99      *            1111.1111.1111     Cable4/0    123       bg
229.7.5.99      10.10.2.56   1111.2222.2222     Cable5/0    1         bg
229.7.5.98      *            1111.2222.2222     Cable3/0    4003      bg

Router# show cable dsg stat
Vendor: bg, Tunnel count: 2
1111.1111.1111
229.2.0.99
Cable4/0    Resolves: 4   Rcv/Fwd/Drp: 323/323/0
1111.2222.2222
229.7.5.99
Cable5/0    Resolves: 4   Rcv/Fwd/Drp: 1/1/0
229.7.5.98
Cable3/0    Resolves: 180 Rcv/Fwd/Drp: 6213/6213/0

Router# show cable dsg stats

DSG statistics information

Vendor: abc, Tunnel count: 3
Vendor: cisco, Tunnel count: 4

Vendor name is abc, tunnel MAC is 000d.000d.000d
Group address is 230.6.6.6, source address is *
  Interface is Cable3/0,   mapping entry is used 2
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is abc, tunnel MAC is 000e.000e.000e
Group address is 230.7.7.7, source address is *
  Interface is Cable3/0,   mapping entry is used 4
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is abc, tunnel MAC is 000c.000c.000c
Group address is 230.5.5.5, source address is *
  Interface is Cable3/0,   mapping entry is used 4
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is cisco, tunnel MAC is 000b.000b.000b
Group address is 230.4.4.4, source address is *
  Interface is Cable3/0,   mapping entry is used 4
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is cisco, tunnel MAC is 0009.0009.0009
Group address is 229.1.1.1, source address is *
  Interface is Cable3/0,   mapping entry is used 3
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is cisco, tunnel MAC is 0008.0008.0008
Group address is 228.1.1.1, source address is *
  Interface is Cable3/0,   mapping entry is used 4
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is cisco, tunnel MAC is 000a.000a.000a
Group address is 230.1.1.1, source address is *
  Interface is Cable3/0,   mapping entry is used 6
    Received 242217224 packets,  forwarded 180194756 packets
    Dropped 62022468 packets,  last second rate 501414 bits/sec

Vendor name is cisco, tunnel MAC is 000a.000a.000a
```

```
Group address is 230.1.1.1, source address is *
  Interface is Cable4/0,   mapping entry is used 18
    Received 242218258 packets,  forwarded 1482 packets
    Dropped 242216776 packets,  last second rate 501414 bits/sec

Vendor name is cisco, tunnel MAC is 000a.000a.000a
Group address is 230.1.1.1, source address is *
  Interface is Cable5/0.1,   mapping entry is used 6
    Received 242218258 packets,  forwarded 1534970 packets
    Dropped 240683288 packets,  last second rate 501414 bits/sec
Router#
```

Note The packet counters are automatically reset to zero for a tunnel when the tunnel does not receive any traffic for three minutes or more.

Configuration Examples for DOCSIS Set-Top Gateway

This section provides the following configuration examples for the DOCSIS Set-Top Gateway feature:

DSG Configuration Example

The following excerpt from a configuration for the cable interface on a Cisco uBR7246VXR router configures a cable interface for the DOCSIS Set-Top Gateway feature:

Tip In addition to the cable interface configuration commands, the **ip multicast-routing** command is also given in global configuration mode, and the **ip mroute-cache** command is also configured on the WAN interface that is providing the network connection for the CA and other DSG servers.

```
...
ip multicast-routing
...

interface GigabitEthernet 1/0
 ip mroute-cache
 description wan interface to CA and other DSG servers

...

interface c6/0
 ip address 10.10.10.11 255.255.255.0
 ip pim dense-mode
 ip igmp static-group 239.0.0.2
 ip multicast rate-limit out group-list
 ip mroute-cache
 cable dsg 1.2.3 239.0.0.2 CCC

...
```

Note The appropriate **ip igmp static-group** command is automatically added to the configuration when you enter the **cable dsg** command.

Subinterface Configuration Example

The following sample configuration shows a more complex configuration for the DOCSIS Set-Top Gateway feature on a Cisco uBR7114 router, showing the use of subinterfaces:

```
version 12.2
service timestamps debug uptime
service timestamps log uptime
service password-encryption
!
hostname dsg-ubr7114
!
logging queue-limit 100
!
no cable qos permission create
no cable qos permission update
cable qos permission modems
ip subnet-zero
!
!
ip cef
!
ip multicast-routing
mpls ldp logging neighbor-changes
!
!
!
interface FastEthernet0/0
 ip address 1.8.8.13 255.255.0.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface Cable1/0
 ip address 2.75.25.1 255.255.255.0
 ip pim dense-mode
 ip helper-address 1.8.35.200
 cable downstream annex B
 cable downstream modulation 256qam
 cable downstream interleave-depth 32
 cable downstream channel-id 0
 cable downstream rf-shutdown
 cable upstream 0 frequency 33008000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
!
interface Cable1/0.1
 ip igmp static-group 224.11.11.1
 ip igmp static-group 224.12.12.1
 ip igmp static-group 224.3.3.2
 ip igmp static-group 224.3.3.3
 ip igmp static-group 224.3.3.6
 ip igmp static-group 224.3.3.7
```

```
 ip igmp static-group 224.3.3.8
 ip igmp static-group 224.3.3.9
 ip igmp static-group 224.3.3.18
 ip igmp static-group 224.3.3.19
 ip igmp static-group 224.3.3.20
 ip igmp static-group 224.3.3.21
 ip igmp static-group 224.3.3.22
 ip igmp static-group 224.3.3.93
 ip igmp static-group 224.3.3.97
 ip igmp static-group 224.3.3.95
 ip igmp static-group 224.3.3.98
 ip igmp static-group 224.5.5.8
 ip igmp static-group 224.5.5.10
 ip igmp static-group 224.3.4.12
 ip igmp static-group 224.3.3.25
 ip igmp static-group 224.4.4.1
 ip igmp static-group 224.5.5.5
 ip igmp static-group 224.5.5.11
 ip igmp static-group 224.5.5.12
 ip igmp static-group 224.5.5.13
 ip igmp static-group 224.5.5.14
 ip igmp static-group 224.5.5.15
 ip igmp static-group 224.5.5.16
 ip igmp static-group 224.6.6.7
 ip igmp static-group 224.6.6.9
 ip igmp static-group 224.6.6.10
 ip igmp static-group 224.6.6.11
 ip igmp static-group 224.7.7.1
 ip igmp static-group 224.8.8.1
 ip igmp static-group 224.8.8.2
 ip igmp static-group 224.8.8.10
 ip igmp static-group 224.9.9.1
 cable dsg 0009.0009.0009 224.12.12.1 science
 cable dsg 0010.0010.0010 224.11.11.1 science
 cable dsg 0001.0001.0001 224.3.3.97 cisco
 cable dsg 0001.0001.0001 224.3.3.98 cisco
 cable dsg 0001.0001.0001 224.3.3.93 cisco
 cable dsg 0001.0001.0001 224.3.3.95 cisco
 cable dsg 0006.0006.0006 224.9.9.1 microso
 cable dsg 0005.0005.0005 224.8.8.1 ibm
 cable dsg 0001.0001.0001 224.7.7.1 cisco
 cable dsg 0001.0001.0002 224.4.4.1 cisco
 cable dsg 0005.0005.0005 224.8.8.2 ibm
 cable dsg 0001.0001.0001 224.3.3.2 cisco
 cable dsg 0001.0001.0001 224.3.3.3 cisco
 cable dsg 1234.1234.1234 224.5.5.5 cisco
 cable dsg 0001.0001.0001 224.3.3.6 cisco
 cable dsg 0001.0001.0001 224.3.3.7 cisco
 cable dsg 00dd.0001.0001 224.6.6.7 cisco
 cable dsg 0001.0001.0001 224.3.3.8 cisco
 cable dsg 0001.0001.0001 224.5.5.8 cisco
 cable dsg 0001.0001.0001 224.3.3.9 cisco
 cable dsg 10dd.0001.0001 224.6.6.9 ibm
 cable dsg 0000.0000.0000 224.8.8.10 science
 cable dsg 0001.0001.0001 224.5.5.10 cisco
 cable dsg 10dd.0002.0002 224.6.6.10 ibm
 cable dsg 0001.0001.0001 224.3.4.12 cisco
 cable dsg 0003.0001.0001 224.5.5.11 cisco
 cable dsg 0000.0000.0001 224.6.6.11 ibm
 cable dsg 0033.0001.0001 224.5.5.12 cisco
 cable dsg 00cc.0001.0001 224.5.5.13 cisco
 cable dsg 00cc.0001.0001 224.5.5.14 cisco
 cable dsg 00cd.0001.0001 224.5.5.15 cisco
 cable dsg 00dd.0001.0001 224.5.5.16 cisco
 cable dsg 0001.0001.0001 224.3.3.18 cisco
 cable dsg 0001.0001.0001 224.3.3.19 cisco
 cable dsg 0001.0001.0001 224.3.3.20 cisco
 cable dsg 0001.0001.0001 224.3.3.21 cisco
 cable dsg 0001.0001.0001 224.3.3.22 cisco
 cable dsg 0001.0001.0001 224.3.3.25 cisco
!
interface Cable1/0.2
 ip igmp static-group 224.11.11.2
 ip igmp static-group 224.13.13.1
 cable dsg 0009.0009.0009 224.13.13.1 science
```

```
 cable dsg 0011.0011.0011 224.11.11.2 science
!
interface Ethernet3/0
 ip address 10.0.0.2 255.0.0.0
 ip pim dense-mode
 duplex half
!
interface Ethernet3/1
 no ip address
 shutdown
 duplex half
!
interface Ethernet3/2
 no ip address
 shutdown
 duplex half
!
interface Ethernet3/3
 no ip address
 shutdown
 duplex half
!
router eigrp 1
 auto-summary
!
ip default-gateway 1.8.0.1
ip classless
ip route 0.0.0.0 0.0.0.0 1.8.0.1
ip route 1.0.0.0 255.0.0.0 1.8.0.1
ip route 223.255.254.254 255.255.255.255 1.8.0.1
no ip http server
no ip http secure-server
!
!
!
access-list 101 permit igmp host 10.0.0.1 host 224.3.3.1
cdp run
!
!
line con 0
line aux 0
line vty 0 4
 password lab
 login
line vty 5 15
 login
!
scheduler allocate 3996 400
```

Unicast Messaging Configuration Example

The following excerpt from a configuration file enables DSG operations on a cable interface, using unicast IP addresses for DSG messaging. This example is the same as the one given in DSG Configuration Example, page 27, except that the interfaces have been configured for NAT so as to enable the use of unicast DSG addresses.

```
...
ip multicast-routing
...

interface GigabitEthernet 1/0
 ip address 10.10.2.50 255.255.255.0
 ip nat outside
 ip mroute-cache
 description wan interface to CA and other DSG servers

...
```

```
interface c6/0
 ip address 10.10.10.11 255.255.255.0
 ip address 192.168.18.1 255.255.255.0 secondary
 ip pim dense-mode
 ip igmp static-group 239.0.0.2
 ip multicast rate-limit out group-list
 ip mroute-cache
 cable dsg 1.2.3 239.0.0.2 CCC
 ip nat inside

...

ip nat inside source static 239.0.0.2 192.168.18.1
...
```

Note The **ip nat inside source static** command uses the same IP multicast address that was used in the **cable dsg** command, and the same IP unicast address that was used in the **ip address secondary** command.

Packet Filtering Access List Configuration Example

The following excerpt from a configuration for a Cisco uBR7246VXR router shows an example of an extended IP access list being used to define the type of traffic that is allowed to be transmitted on a cable interface. Access list 101 permits traffic from two known hosts, denies all other TCP and UDP traffic, and denies IGMP traffic from a particular IP multicast address. All other IP traffic is allowed. The access list is then applied to the cable interface, using the **ip access-group** command.

```
interface Cable3/0
 ip address 10.48.1.1 255.255.255.0
 ip access-group 101 out
 ip pim sparse-mode
 ip helper-address 1.7.29.1
 ip igmp static-group 230.6.6.6
 ip igmp static-group 230.5.5.5
 ip igmp static-group 230.4.4.4
 ip igmp static-group 230.1.1.1
 ip igmp static-group 228.1.1.1
 ip igmp static-group 229.1.1.1
 ip igmp static-group 230.7.7.7
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 cable downstream channel-id 0
 cable upstream 0 frequency 17808000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 2
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable source-verify
 cable dhcp-giaddr primary
 cable dsg 000d.000d.000d 230.6.6.6 abc
```

```
 cable dsg 000e.000e.000e 230.7.7.7 abc
 cable dsg 000b.000b.000b 230.4.4.4 cisco
 cable dsg 000c.000c.000c 230.5.5.5 abc
 cable dsg 0009.0009.0009 229.1.1.1 cisco
 cable dsg 0008.0008.0008 228.1.1.1 cisco
 cable dsg 000a.000a.000a 230.1.1.1 cisco
 no keepalive
!
access-list 101 permit udp host 11.48.1.2 any
access-list 101 permit udp host 11.46.1.100 any
access-list 101 deny   udp any any
access-list 101 deny   tcp any any
access-list 102 deny   igmp any host 230.1.1.1
access-list 102 permit ip any any
```

IP Multicast Access List Configuration Example

The following excerpt from a configuration for a Cisco uBR7246VXR router shows a standard IP access list being configured to allow only traffic destined for a range of particular IP multicast addresses. The access list is applied to the cable interface using the **ip igmp access-group** command.

```
interface Cable 6/0
 ip address 10.44.61.1 255.255.255.0 secondary
 ip address 10.44.51.1 255.255.255.0
 ip pim sparse-dense-mode
 ip helper-address 10.8.35.200
 ip igmp static-group 239.0.0.100
 ip igmp static-group 239.192.16.11
 ip igmp static-group 239.192.16.12
 ip igmp static-group 239.192.16.13
 ip igmp static-group 239.192.16.14
 ip igmp static-group 239.192.16.17
 ip igmp static-group 239.192.16.18
 ip igmp static-group 239.192.16.32
 ip igmp static-group 239.192.16.16
 ip igmp query-interval 65535
 ip igmp access-group 96
 cable tftp-enforce
 cable max-hosts 6
 cable bundle 3 master
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream channel-id 1
 cable upstream 0 frequency 25000000
 cable upstream 0 power-level 0
 no cable upstream 0 shutdown
 cable upstream 1 frequency 25000000
 cable upstream 1 power-level 0
 no cable upstream 1 shutdown
 cable upstream 2 frequency 25000000
 cable upstream 2 power-level 0
 no cable upstream 2 shutdown
 cable upstream 3 frequency 25000000
 cable upstream 3 power-level 0
 no cable upstream 3 shutdown
 cable ip-broadcast-echo
 cable source-verify leasetimer 100
 cable dhcp-giaddr policy
. . .
access-list 96 permit 224.0.0.0 15.255.255.255
access-list 96 deny any
. . .
```

IP Multicast Rate-Limiting Access List Configuration Example

The following excerpt from a configuration for a Cisco uBR7246VXR router shows an example of IP multicast access lists being used to limit the maximum possible data rate for a number of different IP multicast addresses. This method ensures that a particular DSG tunnel does not use an excessive amount of bandwidth.

In this example, a number of standard IP access lists are defined to permit traffic from a particular IP multicast address. These access lists are applied to the cable interface using the **ip multicast rate-limit** command.

```
!
interface Cable3/0
 ip address 10.48.1.1 255.255.255.0
 ip pim sparse-mode
 ip multicast rate-limit out group-list 10 128
 ip multicast rate-limit out group-list 20 256
 ip multicast rate-limit out group-list 30 512
 ip multicast rate-limit out group-list 40 1024
 ip multicast rate-limit out group-list 50 128
 ip multicast rate-limit out group-list 60 256
 ip multicast rate-limit out group-list 70 512
 ip multicast rate-limit out group-list 80 1024
 ip helper-address 1.7.29.1
 ip igmp static-group 230.6.6.6
 ip igmp static-group 230.5.5.5
 ip igmp static-group 230.4.4.4
 ip igmp static-group 230.1.1.1
 ip igmp static-group 228.1.1.1
 ip igmp static-group 229.1.1.1
 ip igmp static-group 230.7.7.7
 cable downstream annex B
 cable downstream modulation 64qam
 cable downstream interleave-depth 32
 cable downstream frequency 459000000
 cable downstream channel-id 0
 cable upstream 0 frequency 17808000
 cable upstream 0 power-level 0
 cable upstream 0 channel-width 1600000
 cable upstream 0 minislot-size 4
 cable upstream 0 modulation-profile 2
 no cable upstream 0 rate-limit
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislot-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislot-size 4
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislot-size 4
 cable upstream 3 modulation-profile 1
 cable upstream 3 shutdown
 cable source-verify
 cable dhcp-giaddr primary
 cable dsg 000d.000d.000d 230.6.6.6 abc
 cable dsg 000e.000e.000e 230.7.7.7 abc
 cable dsg 000b.000b.000b 230.4.4.4 cisco
 cable dsg 000c.000c.000c 230.5.5.5 abc
 cable dsg 0009.0009.0009 229.1.1.1 cisco
 cable dsg 0008.0008.0008 228.1.1.1 cisco
 cable dsg 000a.000a.000a 230.1.1.1 cisco
 no keepalive
!
...
access-list 10 permit 228.1.1.1
access-list 20 permit 229.1.1.1
access-list 30 permit 230.1.1.1
access-list 40 permit 230.4.4.4
access-list 50 permit 230.5.5.5
access-list 60 permit 230.6.6.6
access-list 70 permit 230.7.7.7
access-list 80 permit 230.8.8.8
...
```

Additional References

For additional information related to the DOCSIS Set-Top Gateway feature, refer to the following references:

Related Documents

Related Topic	Document Title
CMTS Command Reference	*Cisco Broadband Cable Command Reference Guide*, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 configuration guides and command references, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
IP Access Lists Configuration Guide	*Configuring IP Services, IP Addressing and Services, Cisco IOS IP Configuration Guide*, Release 12.2, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm
IP Access Lists Command Reference Guide	*IP Services Commands, Cisco IOS IP Command Reference, Volume 1, Addressing and Services*, Release 12.2, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm
IP Multicast Configuration Guide	*Cisco IOS IP Configuration Guide*, Release 12.3 on Cisco.com: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d581.html
IP Multicast Command Reference	*Cisco IOS IP Command Reference, Volume 3 of 3: Multicast*, Release 12.2, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprmc_r/index.htm
Configuring DOCSIS 1.1 on the Cisco CMTS	*Configuring DOCSIS 1.1 on the Cisco CMTS*, in the *CMTS Feature Guide*, at the following URL: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_docs.htm

Standards

Standards[1]	Title
SP-RFIv1.1-I09-020830	Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification, version 1.1
SP-DSG-I01-020228	DOCSIS Set-top Gateway (DSG) Interface Specification

1. Not all supported standards are listed.

MIBs

MIBs[1]	MIBs Link
Cisco IOS Release 12.3(9a)BC introduces SNMP support for the CISCO-CABLE-DSG-IF-MIB.	To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

1. Not all supported MIBs are listed.

RFCs

RFCs[1]	Title
RFC 1112	Host Extensions for IP Multicasting
RFC 2233	DOCSIS OSSI Objects Support
RFC 2365	Administratively Scoped IP Multicast
RFC 2665	DOCSIS Ethernet MIB Objects Support
RFC 2669	Cable Device MIB

1. Not all supported RFCs are listed.

Technical Assistance

Description	Link
Technical Assistance Center (TAC) home page, containing 30,000 pages of searchable technical content, including links to products, technologies, solutions, technical tips, and tools. Registered Cisco.com users can log in from this page to access even more content.	http://www.cisco.com/public/support/tac/home.shtml

System Messages

Cisco IOS Release 12.2(15)BC2 System Messages

Cisco IOS Release 12.2(15)BC2 adds the following system error message to provide information about the DSG feature:

```
%UBR7100-6-DSG_ALL_TUNNEL_REMOVED
%UBR7200-6-DSG_ALL_TUNNEL_REMOVED: All DSG tunnels are removed on interface
[chars] and its subinterfaces
```

Explanation An operator has disabled the DOCSIS Set-top Gateway (DSG) on the indicated cable interface and its subinterfaces, using the **no cable dsg** command.

Recommended Action No action is needed.

Cisco IOS Release 12.3(9a)BC2 System Messages

Cisco IOS Release 12.3(9a)BC2 adds the following system error message to provide information about the DSG feature:

```
%UBR7100-6-DDC_CFG_HASHFILTER_REMOVED
%UBR7200-6-DDC_CFG_HASHFILTER_REMOVED
%UBR10000-6-DDC_CFG_HASHFILTER_REMOVED: Hash-filter [dec] not present in global
config - Filter removed from [chars]
```

Explanation Thespecified hash filter was removed from the global configuration, and because the associated cable interface line card was not present in the chassis, the hash filter configuration was also removed from that cable interface line card configuration.

Recommended Action No action is needed.

```
%UBR7100-4-DDC_CFG_HASHID
%UBR7200-4-DDC_CFG_HASHID
%UBR10000-4-DDC_CFG_HASHID: Hash id [dec] does not exist in global configuration
```

Explanation The specified hash ID for the DOCSIS Dual-Channel (DDC) configuration is configured on a cable interface, but it is not configured globally, so that the router cannot map the appropriate OUI or MAC IDs appropriately.

Explanation Configure the hash ID globally, using the **cable redundancy hashfilter** command in global configuration mode.

```
%UBR7100-6-DDC_CFG_TARGET_REMOVED
%UBR7200-6-DDC_CFG_TARGET_REMOVED
%UBR10000-6-DDC_CFG_TARGET_REMOVED: Redundancy target invalid - removed from
[chars]
```

Explanation The router's MY ID configuration was removed from the configuration, but the associated cable interface line card was not present in the chassis, so the associated redundancy configuration is also removed from that card's interface configuration.

Recommended Action No action is needed.

```
%UBR7100-4-DDC_GENERAL_ERROR
%UBR7200-4-DDC_GENERAL_ERROR
%UBR10000-4-DDC_GENERAL_ERROR: Error: [chars]
```

Explanation The DOCSIS Dual-Channel (DDC) configuration generated the specified error.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-3-DDC_INVALID_HASHTYPE
%UBR7200-3-DDC_INVALID_HASHTYPE
%UBR10000-3-DDC_INVALID_HASHTYPE: The hash type [dec] for hash id [dec] is invalid
```

Explanation The specified hash ID in the DOCSIS Dual-Channel (DDC) configuration has an invalid configuration.

Recommended Action Verify the DDC configuration on the router. If the configuration appears correct, copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-3-DDC_INVALID_STATICMAP
%UBR7200-3-DDC_INVALID_STATICMAP
%UBR10000-3-DDC_INVALID_STATICMAP: The node [dec] for mac-address [enet] exceeds
maximum configured nodes.
```

Explanation The configuration for the DOCSIS Dual-Channel (DDC) contains an Organization Unique Identifier (OUI) or MAC address mapping that specifies a DCC node number outside ofthe valid range (from 1 to 3).

Recommended Action Check the configuration to verify that all of the appropriate downstreams have been configured for the DDC feature, and that the number of configured downstreams is not outside of the valid range. If the configuration appears correct, copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-4-DDC_LIST_ERROR
%UBR7200-4-DDC_LIST_ERROR
%UBR10000-4-DDC_LIST_ERROR: DDC list error
```

Explanation The DOCSIS Dual-Channel (DDC) software was unable to create a list or add an element to a list. This typically is due to a lack of resources, such as memory, or a failure of the interprocess communication (IPC) subsystem to send the required list control messages.

Recommended Action Display the current processor usage using the **show proc** command, and look for any processes that might be monopolizing the processor time. Display the running configuration with the **show running-config** command, and look for any commands that might be allocating large amounts of memory for specific buffers, such as the **logging buffered** command. Verify that you are using released software on the Cisco CMTS. If so, copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-4-DDC_MESSAGE_ERROR
%UBR7200-4-DDC_MESSAGE_ERROR
%UBR10000-4-DDC_MESSAGE_ERROR: DDC message error. type [dec]
```

Explanation The DOCSIS Dual-Channel (DDC) software was unable to send the specified interprocess communication (IPC) messages. This could be due to a lack of resources, such as memory, or due to the processor being at or near 100 percent utilization.

Recommended Action Display the current processor usage using the **show proc** command, and look for any processes that might be monopolizing the processor time. Display the running configuration with the **show running-config** command, and look for any commands that might be allocating large amounts of memory for specific buffers, such as the **logging buffered** command. Verify that you are using released software on the Cisco CMTS. If so, copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. If you cannot determine the nature of the error from the error message text or from the **show tech-support** command output, contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-4-DDC_NODE_ID_ERROR
%UBR7200-4-DDC_NODE_ID_ERROR
%UBR10000-4-DDC_NODE_ID_ERROR: Node id mismatch NPE: [dec]  linecard: [dec]
```

Explanation The node ID on the NPE subinterface is different than what is configured on the cable interface line card.

Recommended Action Verify that the configuration is correct. If so, copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-4-DDC_PROT_FREQ_ERROR
%UBR7200-4-DDC_PROT_FREQ_ERROR
%UBR10000-4-DDC_PROT_FREQ_ERROR: DS frequency not configured for the protect
target node [dec]
```

Explanation A downstream frequency is not configured on the specified target node.

Recommended Action Configure a downstream frequency on the appropriate downstream.

```
%UBR7100-4-DDC_SEMAPHORE_ERROR
%UBR7200-4-DDC_SEMAPHORE_ERROR
%UBR10000-4-DDC_SEMAPHORE_ERROR: DDC semaphore released when it was not taken
```

Explanation A DOCSIS Dual-Channel (DDC) semaphore flag was released, but the flag was not locked at the time. This indicates either that an unexpected situation or that a software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-4-DDC_UNEXPECTED_EVENT_ERROR
%UBR7200-4-DDC_UNEXPECTED_EVENT_ERROR
%UBR10000-4-DDC_UNEXPECTED_EVENT_ERROR: DDC unexpected event error [dec]
```

Explanation The DOCSIS Dual-Channel (DDC) software encountered an unexpected or unsupported event. This indicates either that an unexpected situation or that a software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-4-DDC_UNEXPECTED_MESSAGE_ERROR
%UBR7200-4-DDC_UNEXPECTED_MESSAGE_ERROR
%UBR10000-4-DDC_UNEXPECTED_MESSAGE_ERROR: DDC unexpected message error [dec]
```

Explanation The DOCSIS Dual-Channel (DDC) software received an unexpected or unsupported message. This indicates either that an unexpected situation or that a software error occurred.

Recommended Action Copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

```
%UBR7100-3-DDC_UNEXPECTED_NODES
%UBR7200-3-DDC_UNEXPECTED_NODES
%UBR10000-3-DDC_UNEXPECTED_NODES: The number of nodes [dec] is invalid.
```

Explanation The configuration for the DOCSIS Dual-Channel (DDC) is outside of the valid range (from 1 to 3).

Recommended Action Check the configuration to verify that all of the appropriate downstreams have been configured for the DDC feature, and that the number of configured downstreams is not outside of the valid range. If the configuration appears correct, copy the error message exactly as it appears on the console or in the system log. Issue the **show tech-support** command to gather data that may help identify the nature of the error. Contact your Cisco technical support representative and provide the representative with the gathered information.

Command Reference

This section documents the following new or modified commands that are needed to configure and monitor the DOCSIS Set-Top Gateway (DSG) feature:

- **cable dsg**
- **cable dsg keepalive**
- **debug cable dsg**
- **show cable dsg**

Tip Other cable-specific commands are documented in the *Cisco Broadband Cable Command Reference Guide*, at the following URL:

http://www.cisco.com/univercd/cc/td/doc/product/cable/bbccmref/index.htm

All other commands used with this feature are documented in the Cisco IOS Release 12.2 command reference publications.

cable dsg

To enable the DOCSIS Set-Top Gateway (DSG) on a cable interface, and to configure its tunnel-mapping parameters, use the **cable dsg** command in cable interface configuration mode. To remove the DSG tunnel from the interface, use the **no** form of this command.

cable dsg *tunnel-MAC-address group-ip-address CA-vendor-name*

no cable dsg *tunnel-MAC-address group-ip-address CA-vendor-name*

Syntax Description

tunnel-MAC-address	Well-known MAC address for the DSG tunnel. The *tunnel-MAC-address* could also optionally be an Internet Group Management Protocol (IGMP) multicast address, using the algorithm for converting host group IP address to an Ethernet MAC address that is given in RFC 1112. If the MAC address is 0000.0000.0000, the DSG tunnel uses the algorithm given in RFC 1112 to derive the multicast address for the tunnel. **Note** You can specify only Global Scope (224.0.1.0 through 238.255.255.255) and Administratively Scoped (239.0.0.0 through 239.255.255.255) addresses. You cannot use Local Scope addresses (224.0.0.0 through 224.0.0.255).
group-ip-address	Multicast group IP address for the DSG stream.
CA-vendor-name	Name for the Conditional Access (CA) vendor that owns the DSG tunnel. This parameter is a string up to 7 characters in length and should match the vendor of the CA server. A maximum of four vendors per router are supported.

Defaults

No DSG tunnels are defined.

Command Modes

Interface and subinterface configuration (cable interface only)

Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
12.3(9a)BC	This command was introduced for the Cisco uBR10012 routers.

Usage Guidelines

This command enables DSG operations on the cable interface, creating a DSG tunnel that uses the specified IGMP multicast address and well-known MAC address. If you specify a tunnel MAC address of 0.0.0, the command converts it into an Ethernet multicast MAC address, using the following algorithm, which is given in RFC 1112:

An IP host group address is mapped to an Ethernet multicast address by placing the low-order 23-bits of the IP address into the low-order 23 bits of the Ethernet multicast address 01-00-5E-xx-xx-xx (hex). Because there are 28 significant bits in an IP host group address, more than one host group address may map to the same Ethernet multicast address.

For example, if you specify the command **cable dsg 0.0.0 228.9.9.9 AAA**, the command uses the IGMP IP address of 228.9.9.9 to generate the MAC address of 0100.5E09.0909 for the DSG tunnel. If the IGMP address were 228.129.9.9, the resulting MAC address would be 0100.5E01.0909.

Entering the **cable dsg** command also automatically configures the interface for the appropriate IGMP static group, using the **ip igmp static-group** command. Do not manually enter another **ip igmp static-group** command for this interface, because the system assumes that this IGMP configuration is for a separate configuration that cannot be used by the DSG subsystem.

Note If any previously configured static groups exist on this interface, you should remove those other **ip igmp static-group** commands on a cable interface before you can enter the **cable dsg** command. If you do not remove those other groups, the **cable dsg** command displays a warning notifying you that you should remove them.

The **no cable dsg** command similarly automatically removes the IGMP static group from the interface by issuing the **no ip igmp static-group** command. Do not manually remove this static group yourself.

In addition, you must have enabled Protocol Independent Multicast (PIM) on the cable interface, using the **ip pim** interface command, before enabling and configuring DSG operations. The DOCSIS Set-Top Gateway feature supports the following PIM modes:

- **sparse-mode**—Sparse mode of operation.
- **sparse-dense-mode**—The interface is treated in either sparse mode or dense mode of operation, depending on the mode in which the multicast group is operating.
- **dense-mode**—Dense mode of operation.

Limitations and Restrictions

The DOCSIS Set-Top Gateway feature also has the following limitations:

- If using bundled interfaces, configure the DSG configurations only on the master interface, not on the slave interfaces. However, when DSG has been properly configured on the master interface, DSG traffic can flow across both the master and slave interfaces.
- If using subinterfaces, you must configure the DSG tunnels only on subinterfaces. When DSG tunnels are configured on a subinterface, you cannot also configure the tunnels on the main interface. If you configure DSG tunnels on both the main interface and subinterfaces, the main interface can drop packets.

  We also recommend putting all DSG configurations on the same, single subinterface. Although you can configure DSG tunnels on multiple subinterfaces, this is not guaranteed to be supported in future software releases.
- You can configure up to four separate conditional access (CA) vendors per router.
- You can configure a maximum of eight DSG tunnels (as identified by the well-known MAC address) per CA vendor, for a maximum possible total of 32 DSG tunnels per router.
- Each CA vendor can have one or more DSG tunnels on each cable interface, but each DSG tunnel must be using a separate IP multicast address.
- IP multicast routing should be enabled on the router, using the **ip multicast-routing** command.

- Multicast rate-limiting can optionally be enabled on a cable interface that is configured for DSG operations, using the **ip multicast rate-limit out group-list** command.
- For best performance, fast switching of IP multicast should be enabled on incoming and outgoing interfaces, using the **ip mroute-cache** command.
- You cannot create use the same IP multicast groups for both DSG traffic and for other IP multicast traffic. If an IP multicast group is being used for DSG traffic, do not use the **ip igmp static-group** command to manually configure that same IP multicast group for other, non-DSG traffic.
- Different CA vendors cannot share IP multicast addresses. Each vendor must use a unique set of IP multicast addresses, and after an IP multicast address is assigned to a DSG tunnel, that same address cannot be used for any other purpose. However, all other multicast addresses and groups can still be used on the interface for other multicast applications.
- DSG-related IP unicast traffic is not supported. The CMTS receives the unicast traffic from the DSG network controllers, but it does not forward that traffic to the set-top boxes.
- DSG traffic should be less than 2.048 Mbps per vendor, so as to conform to the DSG specifications.
- DSG does not support BPI-encrypted IP multicast streams.

Note In Cisco IOS Release 12.2(15)BC2, N+1 HCCP high-availability redundancy does not preserve the DSG traffic and configuration after a switchover. If you configure a cable interface for both N+1 HCCP redundancy and for DSG operations, DSG traffic does not continue after a switchover.

Examples

The following example shows how to configure a cable interface on a Cisco uBR7246VXR router to enable the DSG feature on cable interface 3/0, using a well-known MAC address of 0001.0002.0003 and a destination IP address of 225.2.3.4:

```
Router# configure terminal
Router(config)# interface cable 3/0
Router(config-if)# ip pim dense-mode
Router(config-if)# ip multicast rate-limit out group-list 123 1024
Router(config-if)# cable dsg 1.2.3 225.2.3.4 CCC
Router(config-if)# exit
Router(config)# exit
Router#
```

Note The above configuration also automatically configures the interface with the appropriate IGMP static-group command (**ip igmp static-group 225.3.4.5**). This command will appear in the interface configuration and should not be removed manually.

The following example shows the error message that appears if you specify a broadcast IP address that has already been added to the router's IGMP database. This entry typically would have been created manually on the router or dynamically by a CPE device that is attached to a cable modem on the cable network.

```
Router# configure terminal
Router(config)# interface cable 3/0
Router(config-if)# cable dsg 1.1.1 224.3.3.10 cisco

Multicast group 224.3.3.10 is already in use on the interface Cable3/0, please retry.

Router#
```

The following example shows how to delete a DSG tunnel on a cable interface:

```
Router# configure terminal
Router(config)# interface cable 4/0
Router(config-if)# no cable dsg 0020.0020.0020 230.8.8.8 abc

4d17h: DSG: interface Cable5/0 left the igmp static group 230.8.8.8.
4d17h: DSG: tunnel 0020.0020.0020 is removed
4d17h: DSG: the specified DSG entry has been removed.

Router(config-if)# end
Router#
```

The following example shows the error message that appears when a unicast IP address is specified instead of a multicast IP address:

```
Router(config-if)# cable dsg 1.1.1 172.68.13.10 cisco

Only multicast is supported for current version.

Router(config-if)#
```

Related Commands

Command	Description
cable dsg keepalive	Enables keepalive messages over DOCSIS Set-Top Gateway (DSG) tunnels on a cable interface.
debug cable dsg	Enables the display of debugging messages for the operation of the DOCSIS Set-Top Gateway (DSG) feature.
show cable dsg	Displays the current DOCSIS Set-Top Gateway (DSG) tunneling parameters.

cable dsg keepalive

To enable keepalive messages over DOCSIS Set-Top Gateway (DSG) tunnels on all cable interfaces, use the **cable dsg keepalive** command in global configuration mode. To disable DSG keepalives (the default), use the **no** form of this command.

cable dsg keepalive

no cable dsg keepalive

Syntax Description

This command has no arguments or keywords.

Defaults

Keepalive messages are disabled (**no cable dsg keepalive**).

Command Modes

Global configuration

Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
12.3(9a)BC	This command was introduced for the Cisco uBR10012 routers.

Usage Guidelines

By default, the Cisco CMTS does not send keepalive messages on any DSG tunnels. When keepalives are enabled using the **cable dsg keepalive** command, the Cisco CMTS sends one keepalive message each second on each DSG tunnel on each downstream. In Cisco IOS Release 12.2(15)BC2, the keepalive packet is a null packet.

Note Do not enable DSG keepalive messages unless your application and DSG set-top boxes require them.

Tip Use the **show cable dsg** command to display whether keepalive messages are enabled.

Examples

The following example shows how to enable DSG keepalives on all cable interfaces on the router:

```
Router# configure terminal
Router(config)# cable dsg keepalive
Router(config)# exit
Router#
```

The following example shows how to disable DSG keepalives on all cable interfaces, which is the default configuration:

```
Router# configure terminal
Router(config)# no cable dsg keepalive
Router(config)# exit
Router#
```

Related Commands

Command	Description
cable dsg	Enables the DOCSIS Set-Top Gateway (DSG) on a cable interface, and configures its tunnel-mapping parameters.
debug cable dsg	Enables the display of debugging messages for the operation of the DOCSIS Set-Top Gateway (DSG) feature.
show cable dsg	Displays the current DOCSIS Set-Top Gateway (DSG) tunneling parameters.

debug cable dsg

To enable the display of debugging messages for the operation of the DOCSIS Set-Top Gateway (DSG) feature, use the **debug cable dsg** command in privileged EXEC mode. To stop the display of debugging messages, use the **no** form of this command.

debug cable dsg

no debug cable dsg

Syntax Description

This command has no arguments or keywords.

Defaults

Debugging is disabled.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
12.3(9a)BC	This command was introduced for the Cisco uBR10012 routers.

Usage Guidelines

Because this command can produce a large volume of debug information, use this command only when you have also enabled debugging for a particular interface or MAC address, using the **debug cable interface** and **debug cable mac-address** commands, respectively.

Examples

The following example shows how to enable debugging output using the **debug cable dsg** command:

```
Router# debug cable dsg

CMTS debug DSG debugging is on

Router#
```

The following sample messages show that a DSG tunnel has been created, along with its mappings:

```
Router(config-if)# cable dsg 6.6.6 237.2.2.2 exn
Router(config-if)#
DSG: a mapping entry created for 0006.0006.0006 237.2.2.2 on Cable3/0
DSG: got mac 0006.0006.0006 for group 237.2.2.2 on Cable3/0
DSG: mac 0006.0006.0006 is resolved for 237.2.2.2 on Cable3/0
DSG: interface Cable3/0 joined the igmp static group 237.2.2.2.
```

The following sample messages show that a particular DSG tunnel and its mappings have been deleted and removed:

```
DSG: tunnel 0001.0002.0003 is removed
DSG: Vendor entry CCC is freed
```

```
DSG: mapping entry freed for 235.5.5.5 0001.0002.0003 Cable 3/0
DSG: The specified DSG entry has been removed.
DSG: interface Cable 3/0 left the igmp static group 235.5.5.5
DSG: all tunnels have been removed on interface Cable 3/0 and its subinterfaces
```

The following messages show that the Cisco CMTS is using its internal DSG tables to resolve a particular MAC address:

```
DSG: mac 0001.0002.0003 is resolved for 225.2.2.2 on Cable5/0
```

The following sample messages show that the Cisco CMTS is using its internal DSG tables to find the appropriate MAC address for an IP multicast group:

```
DSG: got mac 0001.0002.0003 for group 225.2.2.2 on Cable5/0
```

The following sample messages show that the Cisco CMTS is using its internal DSG tables to find the appropriate IP multicast group for a particular MAC address:

```
DSG: got group 225.2.2.2 from mac 0001.0002.0003
```

The following sample messages show the debug message that shows an unexpected event occurred while the DSG subsystem was waiting to send the next keepalive message:

```
DSG: Unexpected event for CMTS DSG process
```

Related Commands

Command	Description
cable dsg	Enables the DOCSIS Set-Top Gateway (DSG) on a cable interface, and configures its tunnel-mapping parameters.
cable dsg keepalive	Enables keepalive messages over DOCSIS Set-Top Gateway (DSG) tunnels on a cable interface.
show cable dsg	Displays the current DOCSIS Set-Top Gateway (DSG) tunneling parameters.

show cable dsg

To display the current DOCSIS Set-Top Gateway (DSG) tunneling parameters, use the **show cable dsg** command in privileged EXEC mode.

show cable dsg {**stats** | **tunnel**} [**vendor** *CA-vendor-name* | *tunnel-mac-address*]

Syntax Description

stats	Displays configuration and run-time statistics about the currently-defined DSG tunnels.
tunnel	Displays the mapping of DSG tunnels to vendors or well-known MAC addresses.
vendor *CA-vendor-name*	(Optional) Displays information about a specific Conditional Access (CA) vendor. This parameter can be any arbitrary string up to 8 characters in length.
tunnel-MAC-address	(Optional) Displays information for the specified well-known MAC address for the DSG tunnel. If you specify a MAC address of 0000.0000.0000, the command displays information for all DSG tunnels, which is the default display.

Defaults

Displays information for all DSG tunnels.

Command Modes

Privileged EXEC

Command History

Release	Modification
12.2(15)BC2	This command was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR routers.
12.3(9a)BC	This command was introduced for the Cisco uBR10012 routers.

Examples

The following example shows a typical display for the **show cable dsg tunnel** command for DSG Issue 1.0:

```
Router# show cable dsg tunnel
Group-ip        Src-ip          Tunnel-MAC      Interface   Packets   CA-vendor
224.1.2.3       *               0050.4d00.0002  Cable6/0    0         nds
```

The following example shows a typical display for the **show cable dsg tunnel** command for DSG Issue 0.9:

```
Router# show cable dsg tunnel

Group-ip        Src-ip          Tunnel-MAC      Interface   Packets   CA-vendor
225.2.2.2       *               0001.0002.0003  Cable3/0    1589      BBB
230.6.6.6       *               000d.000d.000d  Cable3/0    12868464  abc
230.7.7.7       *               000e.000e.000e  Cable3/0    24330138  abc
230.4.4.4       *               000b.000b.000b  Cable3/0    22008648  cisco
230.5.5.5       *               000c.000c.000c  Cable3/0    6424012   abc
229.1.1.1       *               0009.0009.0009  Cable3/0    12868440  cisco
228.1.1.1       *               0008.0008.0008  Cable3/0    6424012   cisco
230.1.1.1       *               000a.000a.000a  Cable3/0    24370812  cisco
230.8.8.8       *               000f.000f.000f  Cable3/0    23035116  abc
```

The following example shows a typical display for the **show cable dsg stats** command for DSG Issue 0.9:

```
Router# show cable dsg stats

DSG statistics information

DSG keepalive is set

Vendor: DDD, Tunnel count: 1
Vendor: BBB, Tunnel count: 2

Vendor name is DDD, tunnel MAC is 0001.0002.0003
Group address is 226.2.2.2, source address is *
  Interface is Cable5/1,   mapping entry is used 1
    Received 5968 packets,  forwarded 5289 packets
    Dropped 679 packets,  last second rate 16878 bits/sec

Vendor name is BBB, tunnel MAC is 0009.0010.0011
Group address is 227.2.2.2, source address is *
  Interface is Cable3/0,  interface Cable3/0 is bundle master
  mapping entry is used 2
    Received 0 packets,  forwarded 0 packets
    Dropped 0 packets,  last second rate 0 bits/sec

Vendor name is CCC, tunnel MAC is 0005.0006.0007
Group address is 228.3.3.3, source address is *
  Interface is Cable5/1,   mapping entry is used 2
    Received 5970056 packets,  forwarded 400333 packets
    Dropped 5569723 packets,  last second rate 96768 bits/sec
```

The following example shows a typical display for the **show cable dsg stats** command for an individual vendor for DSG Issue 0.9:

```
Router# show cable dsg stats vendor CCC

DSG statistics information

DSG keepalive is set

Vendor: CCC, Tunnel count: 1

Vendor name is CCC, tunnel MAC is 0005.0006.0007
Group address is 228.3.3.3, source address is *
  Interface is Cable5/1,   mapping entry is used 2
    Received 5970056 packets,  forwarded 400333 packets
    Dropped 5569723 packets,  last second rate 96768 bits/sec
```

Note The packet counters for both the **stats** and **tunnel** options for a particular DSG tunnel continue to increase as long as traffic is received over that tunnel. If the tunnel does not receive any traffic for three minutes or more, the counters are automatically reset to 0.

The following example shows a typical display for the **show cable dsg stats** command for an individual vendor when the associated cable interface is shut down. The Received, Forwarded, and Dropped counters are not displayed when an interface is shut down.

```
Router(config)# interface c5/1
Router(config-if)# shutdown
Router(config-if)# exit
Router(config)# exit
Router# show cable dsg stats vendor CCC
```

```
DSG statistics information

DSG keepalive is set

Vendor: CCC, Tunnel count: 1

Vendor name is CCC, tunnel MAC is 0005.0006.0007
Group address is 228.3.3.3, source address is *
  Interface is Cable5/1,   mapping entry is used 2

Router#
```

Table 1 describes the major fields shown in the **show cable dsg** command:

Table 1 show cable dsg Field Descriptions

Field	Description
DSG keepalive is set	If keepalive messages have been enabled for an IP multicast group, using the **cable dsg keepalive** command, this message is displayed.
Dest-ip, Group address	Multicast group IP address for the DSG stream.
Src-ip, Source address	Source IP address for the DSG stream. If an asterisk (*) appears as the source IP address, it indicates that the source IP address is 0.0.0.0, which allows any IP address as the source IP address.
Mapped-MAC, Tunnel-MAC	Well-known MAC address used for the DSG tunnel. If you configured the DSG tunnel with a MAC address of 0000.0000.0000 using the **cable dsg** command, this field shows the MAC address that the CMTS derived using the MAC to IP multicast addressing mapping that is specified in RFC 1112.
Interface	Cable interface on which this DSG tunnel is configured.
mapping entry is used	Number of times that this particular DSG tunnel mapping has been used to resolve the well-known MAC address from the tunnel's group address. This can be used as a very rough approximation of the number set-top boxes (STBs) that have been mapped to this DSG tunnel since the last time the counter was cleared.
Packets	Number of packets transmitted over the DSG tunnel.
CA-vendor	Name for the Conditional Access (CA) vendor that owns this tunnel.
Received	Number of packets received by the multicast group. This counter includes all interfaces that are receiving traffic for the multicast group. The field is not shown when an interface is shut down, but the counter continues to increase as long as the multicast group is receiving traffic. When the interface is reenabled, the counter shows the latest number of packets received.

Table 1 show cable dsg Field Descriptions (continued)

Field	Description
Forwarded	Number of packets forwarded on the cable interface for the multicast group. This counter is reset to 0 whenever an interface is shut down and reenabled. The field is not shown when an interface is shut down.
Dropped	Number of packets that were dropped that were for the multicast group. This counter includes all interfaces that are receiving traffic for the multicast group. The field is not shown when an interface is shut down, but the counter continues to increase as long as the multicast group is receiving traffic and dropping packets. When the interface is reenabled, the counter shows the latest number of packets dropped.

Note The Received and Dropped counters reflect activity for the multicast group and are not affected when a cable interface is shut down and reenabled, as long as the multicast group continues to receive traffic. The Forwarded counter reflects activity for the particular cable interface and is reset to zero whenever the interface is shut down and reenabled. All packet counters are also automatically reset to zero if the DSG tunnel does not receive traffic for three minutes or more.

Related Commands

Command	Description
cable dsg	Enables the DOCSIS Set-Top Gateway (DSG) on a cable interface, and configures its tunnel-mapping parameters.
cable dsg keepalive	Enables keepalive messages over DOCSIS Set-Top Gateway (DSG) tunnels on a cable interface.
debug cable dsg	Enables the display of debugging messages for the operation of the DOCSIS Set-Top Gateway (DSG) feature.

Glossary

This section describes terms and acronyms that are used in this manual and not otherwise defined. See the *Internetworking Terms and Acronyms* for terms not included in this glossary.

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.

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

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

DOCSIS Set-Top Gateway (**DSG**)—A specification from Cable Labs 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 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.

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.

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.

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.

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 terminal—See set-top box (STB).