



DOCSIS Set-Top Gateway and Advanced-mode DSG for the Cisco CMTS

This document describes the DOCSIS Set-Top Gateway (DSG) feature with its configuration and monitoring, from DSG Issue 0.9 through Advanced-mode DSG Issue 1.1 on the Cisco Cable Modem Termination System (CMTS). This document revision emphasizes DSG Issue 1.0 commencing with Cisco IOS Release 12.3(9a)BC, and A-DGS 1.1 commencing with Cisco IOS release 12.3(13)BC.

DSG is a CableLabs® specification that allows cable headend equipment such as the Cisco CMTS to provide a class of cable services known as out-of-band (OOB) messaging. OOB messaging is sent to set-top boxes (STBs) over existing Data-over-Cable Service Interface Specifications (DOCSIS) cable networks.

DSG 1.0 and A-DSG 1.1 allow cable Multiple System Operators (MSOs) and other service providers to combine both DOCSIS and Set-top Box (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, DSG 1.0 and earlier issues of DSG support the CableLabs® DOCSIS DSG-I01 and earlier specifications, as described in the “[DSG 1.0 Feature List](#)” section on [page 12](#). CableLabs® DOCSIS DSG-I01 is in the current status of “Issued” as characterized by stability, rigorous review in industry and cross-vendor interoperability.

Advanced-mode DSG 1.1 (A-DSG 1.1) supports the CableLabs® DOCSIS DSG-I02 specifications, with several new features as described in the “[A-DSG 1.1 Features and Enhancements for the Cisco CMTS](#)” section on [page 6](#). The CableLabs® DOCSIS DSG-I02 is in the current status of “Issued,” with the most recent status change being January, 2005.

For additional information about CableLabs® DSG specifications, refer to the following resources:

- *DOCSIS Set-top Gateway (DSG) Interface Specification Summary*
<http://www.cablemodem.com/specifications/gateway.html>

Feature Specifications for DOCSIS Set-Top Gateway

Feature History

Release	Modification
---------	--------------



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

© 2007 Cisco Systems, Inc. All rights reserved.

Release 12.3(13)BC	<p>Advanced-mode DSG 1.1 (A-DSG) introduced to support DOCSIS 1.1 on the Cisco CMTS:</p> <ul style="list-style-type: none"> • Cisco uBR10012 router with these field-replaceable units: <ul style="list-style-type: none"> – Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card – Cisco uBR10-LCP2-MC28C Cable Interface Line Card – Cisco uBR10-MC5X20S/U Broadband Processing Engine • Cisco uBR7200 Series with these field-replaceable units: <ul style="list-style-type: none"> – Cisco uBR-MC16U/X Cable Interface Line Card – Cisco uBR-MC28U/X Cable Interface Line Card
Release 12.3(9a)BC	<p>This feature was introduced for the Cisco uBR10012 universal broadband router.</p> <p>The following DSG 1.0 features are supported for each Cisco CMTS platform:</p> <ul style="list-style-type: none"> • 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	<p>This feature was introduced for the Cisco uBR7100 series and Cisco uBR7246VXR universal broadband routers.</p>

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 and A-DSG 1.1, page 3](#)
- [Restrictions for DOCSIS Set-Top Gateway Issues, page 4](#)
- [Information About DOCSIS Set-Top Gateway, page 6](#)
- [How to Configure DOCSIS Set-Top Gateway 1.0 on the Cisco CMTS, page 19](#)
- [How to Configure Advanced-mode DOCSIS Set-Top Gateway 1.1 on the Cisco CMTS, page 14](#)
- [How to Monitor the DOCSIS Set-Top Gateway Feature, page 31](#)
- [Configuration Examples for DOCSIS Set-Top Gateway, page 37](#)
- [Additional References, page 45](#)
- [System Messages, page 47](#)
- [Glossary, page 52](#)

Prerequisites for DOCSIS Set-Top Gateway and A-DSG 1.1

This section describes prerequisites for Advanced-mode DSG 1.1, and the prior issue of DSG 1.0, as supported in Cisco IOS release 12.3(9a)BC.

General Prerequisites for A-DSG 1.1

- Cisco IOS release 12.3(13)BC or a later 12.3 BC release are required.
- Cisco A-DSG 1.1 is supported on the Cisco uBR10012 router with PRE2 performance routing engine modules.
- Cisco A-DSG 1.1 is supported on the Cisco uBR10012 router with the following cable interface line cards and broadband processing engines (BPEs):
 - Cisco uBR10-LCP2-MC16C/MC16E/MC16S Cable Interface Line Card
 - Cisco uBR10-LCP2-MC28C Cable Interface Line Card
 - Cisco uBR10-MC5X20S/U Broadband Processing Engine

General Prerequisites for DSG 1.0

- 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 for DSG 1.0

- 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 45](#).

Restrictions for DOCSIS Set-Top Gateway Issues

This section describes prerequisites and caveats for Advanced-mode DSG 1.1, and the prior issues of DSG 1.0 and 0.9, as supported in Cisco IOS release 12.3(9a)BC and earlier releases.

General Restrictions for A-DSG 1.1

Cisco DSG 1.1 has the following restrictions:

- Cisco DSG 1.1 does not support the PRE1 module on the Cisco uBR10012 router.
- Cisco DSG 1.1 does not support Service Flow Quality of Service (QoS), which is available at Layer 3.
- Cisco DSG 1.1 does not support tunnel security, but strictly access control lists (ACLs).
- Cisco DSG 1.1 does not support subinterfaces.
- Cisco DSG 1.1 does not support HCCP N+1 interoperability.
- Cisco DSG 1.1 does not support SNMP MIBS for A-DSG.

[Table 1](#) summarizes caveats from Cisco IOS Release 12.3(9a)BC that are resolved in Cisco IOS Release 12.3(13)BC with DSG 1.1:

Table 1 *Open Caveats for Cisco IOS Release 12.3(9a)BC*

DDTS ID Number	Description
CSCeh20144	Rule error checking into performed during reload.
CSCeh28108	DCD counter increments on the working after it becomes standby
CSCeh37862	DCD counters stop incrementing on the protect card

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.

General 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.

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 24](#). 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 contains the following topics, and describes the DOCSIS Set-Top Gateway feature for the Cisco CMTS, with emphasis on Advanced-mode DSG Issue 1.1 (A-DSG), and DSG 1.0:

- [A-DSG 1.1 Features and Enhancements for the Cisco CMTS, page 6](#)
- [General Feature Overview for DOCSIS Set-Top Gateway, page 9](#)
- [DSG 1.0 Feature List, page 12](#)
- [Primary Benefits of DOCSIS Set-Top Gateway, page 13](#)

A-DSG 1.1 Features and Enhancements for the Cisco CMTS

A-DSG 1.1 and Cisco IOS Release 12.3(13)BC introduce a significant and powerful set of features to MSOs and the Cisco CMTS. These features represent a significant change from DSG 1.0 and earlier DSG issues. Architectural and configuration changes unique to A-DSG emphasize the following:

- [A-DSG 1.1 Tunnels, page 6](#)
- [A-DSG 1.1 Classifiers, page 7](#)
- [A-DSG 1.1 Downstream Channel Descriptor \(DCD\), page 7](#)
- [A-DSG 1.1 Process, page 8](#)
- [A-DSG 1.1 Rule, page 8](#)

A-DSG 1.1 and CISCO-CABLE-DSG-IF-MIB

Cisco IOS Release 12.3(13)BC does not support the CISCO-CABLE-DSG-IF-MIB. Support for this MIB continues for basic-mode DSG 1.0.

A-DSG 1.1 Tunnels

The A-DSG Agent (the Cisco CMTS) allows the mapping of an IP multicast address to a DSG tunnel MAC address. Only one IP multicast address can be mapped to a one-tunnel MAC address. However, two tunnels can have the same MAC address.

A-DSG tunnels are configured in global configuration mode. Then, each tunnel is associated to the classifier, also in global configuration mode. This association maps an IP multicast address to the tunnel MAC address. Interface configurations then construct the DCD messages that contain both global and interface information about the A-DSG 1.1 tunnel.

When removing the A-DSG tunnel configuration, all DSG classifiers, rules, and classifiers in the rule configuration associated to that tunnel must be unlinked.

For configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 14](#).

A-DSG 1.1 Classifiers

DSG classifier is used to provide additional layer 3 and layer 4 filtering for the DSG tunnel. DSG multicast software module applies the classifier parameters to incoming packets received from the DSG server in order to assign packets to the appropriate DSG tunnel.



Note

The A-DSG tunnel must be configured before a tunnel can be associated to the classifier. Therefore, the A-DSG classifier cannot be enabled until the tunnel is associated to the classifier.

When removing the classifier, classifier linked to the DSG rule must be removed. Also, before changing the classifier tunnel association to another DSG tunnel, if classifier is associated to a rule, then user must remove classifier associated with the rule. Figure 3 shows the flow of the configuration of classifier parameters.

For configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 14](#).

A-DSG 1.1 Downstream Channel Descriptor (DCD)

Unlike earlier issues of DSG, Advanced-mode DSG (A-DSG) uses a DOCSIS MAC Management Message called the Downstream Channel Descriptor (DCD) message, and this DCD message manages the DSG Tunnel traffic. The DCD message is sent once per second on each downstream and is used by the DCD Client to determine which tunnel and classifier to use.

The DCD is a DSG address table located in the DOCSIS MAC management message. The primary difference between DSG 1.0 (and earlier issues) and A-DSG 1.1 is that advanced mode uses DCD messages to manage the DSG Tunnel.

The DCD message contains a group of DSG Rules and DSG Classifiers, including the following:

- DSG Rules and Rule Priority
- DSG Classifiers
- Client Identifier (whether broadcast, CA System, application, or MAC-level)
- Vendor-specific information field
- Regionalization (per downstream within a cable interface bundle)
- SSM Interoperability

This collection of DSG Rules and DSG Classifiers in the DCD message is known as the DSG Address Table. The DCD message is sent by DSG Agent (CMTS) once per second on each downstream.

The DCD message provides several functions:

- Provides a consolidated keep-alive mechanism for all DSG Tunnels on a particular downstream.

- Provides an address substitution and classification mechanism to increase the flexibility and security of the DSG Tunnel.
- Allows the use of multicast addresses.
- Allows the MSO to assign any Set-top Device to any DSG Tunnel.
- Allows global changes to the DSG Client timers to allow operator driven changes in DSG eCM performance.

The maximum DCD message length is no more than minimum of 1522 bytes long or the MTU size. If DCD message length is greater, DCD message is fragmented and DCD message is sent in pieces. In that case, the DSG agent needs to space out the DCD fragment within one second.

A-DSG 1.1 supports the CableLabs® DOCSIS DSG-I02 specification, with these primary differences between DSG 1.0 and A-DSG 1.1:

- A-DSG 1.1 enables the learning of dynamic tunnel definitions. DSG 1.0 only had static tunnel definitions (set on the STB).
- A-DSG 1.1 supports several new command-line interface (CLI) configuration and **show** commands for advanced-mode configuration and network information.

For global configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 14.](#)

For interface configuration information, refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS” section on page 17.](#)

A-DSG 1.1 Process

The Advanced DCD process handles the construction and transmission of the DCD message on each downstream. A DCD timer is defined for each downstream and it is initialized during startup. The timer is started when the interface is up and DCD is enabled. The Advanced DCD process wakes up when timer expires and handles the DCD processing. The Figure 5 describes the flow of construction and transmission of the DCD message.

For global and timer configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 14.](#)

For interface configuration information, refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS” section on page 17.](#)

A-DSG 1.1 Rule

The parameters associated with the DSG rule are used by the DSG Client to determine which DSG Tunnel to receive and if there are any classifiers to apply. DSG rules are included in the DCD message. All the DSG parameters i.e. tunnels, classifiers, client ID list, vendor specific parameters, and UCID range must be configured before it can be associated to the DSG rule. When removing the rule configuration, the global configuration of the tunnel and classifiers associated to that rule should remain same. The flow of the DSG Rule configuration is shown in the Figure 4.

For global and timer configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 14.](#)

For interface configuration information, refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS” section on page 17.](#)

General Feature Overview for DOCSIS Set-Top Gateway

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:

- Multiple 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.

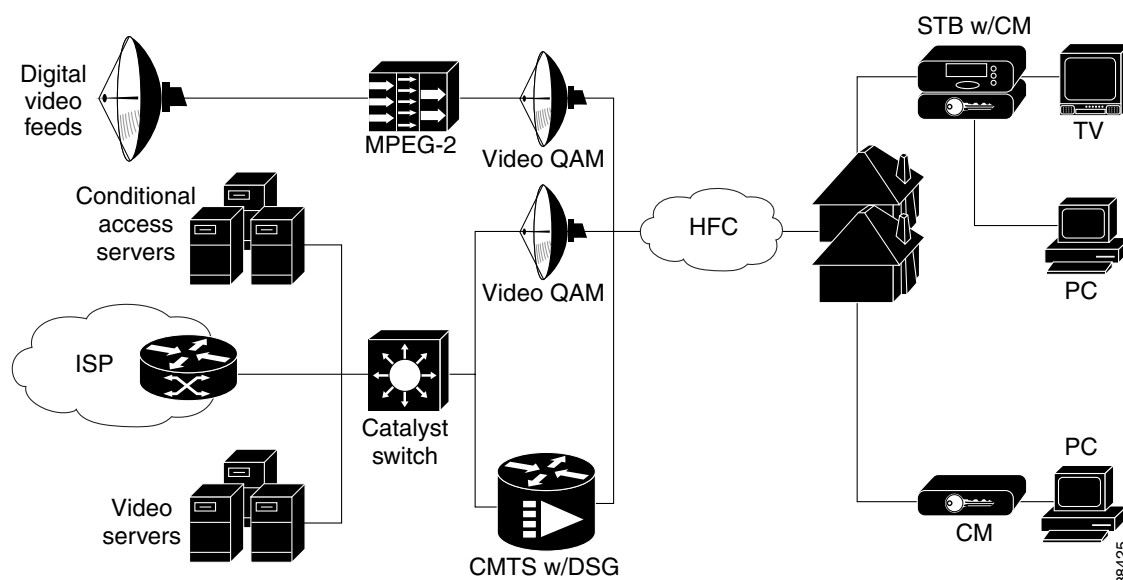
A typical DSG network contains the following components:

- 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 provides 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 to 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.

DSG 1.0 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 the CISCO-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.

Primary Benefits of DOCSIS Set-Top Gateway

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 Advanced-mode DOCSIS Set-Top Gateway 1.1 on the Cisco CMTS

This section contains two procedures, both of which are required to enable and configure A-DSG 1.1 on the Cisco CMTS:

- [Configuring Global A-DSG 1.1 Settings for the Cisco CMTS, page 14](#)
- [Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS, page 17](#)

Configuring Global A-DSG 1.1 Settings for the Cisco CMTS

Global configuration commands for A-DSG 1.1 configure the following settings on the Cisco CMTS:

- A-DSG 1.1 tunnels
- A-DSG clients
- Additional parameters such as classifiers, downstream channel lists, vendor specific parameters, and DSG timers

These global A-DSG parameters are uniquely identified by A-DSG indexes. The indexes are then used with interface commands to define DCD messages. The interface commands define the DSG rules, tunnel traffic, and parameters to include in the DCD message. The following procedure describes global configuration for A-DSG 1.1, to precede interface configuration.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **cable dsg tunnel <tunnel-id> mac_addr <mac addr> [srv-class <service-class-name>] | [enable | disable]**
4. **cable dsg cfr <cfr index> dest_ip <ipaddr> [tunnel <tunnel index>] | [dest-ports <start> <end>] | [priority <priority>] | [src-ip <ipaddr>] | src-ip <ipaddr> [enable | disable]**
5. **cable dsg chan-list <list-index> index <entry-index> freq <freq>**
6. **cable dsg client-list <client-list-id> id-index <id> {application-id | ca-system-id | mac-addr | broadcast} <value>**
7. **cable dsg timer <index> [Tdsg1 <Tdsg1>] | [Tdsg2 <Tdsg2>] | [Tdsg3 <Tdsg3>] | [Tdsg4 <Tdsg4>]**
8. **cable dsg vendor-param <group-id> vendor <vendor-index> oui <oui> value <value-in-TLV>**
9. **Ctrl^Z**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	cable dsg tunnel <tunnel-id> mac_addr <mac addr> [srv-class <service-class-name>] [enable disable] Example: Router(config)# cable dsg 1.1.1 224.3.3.10 cisco	Creates A-DSG 1.1 tunnels. The destination MAC address and Quality of Service (QoS) class must be set when using this command. To remove this configuration from the Cisco CMTS, use the no form of this command. To disable A-DSG 1.1 tunnels on the Cisco CMTS, use the disable form of this command. <ul style="list-style-type: none"> tunnel-id—Alphanumeric string to identify the A-DSG tunnel in related show and configuration commands. mac_addr mac-addr—(Required) Destination MAC address. srv-class service-class-name—(Required) <ul style="list-style-type: none"> srv-class—Keyword sets service class name associated with the A-DSG tunnel. service-class-name—Alphanumeric string of the associated service class name enable—Enables the specified A-DSG tunnel. disable—Disables the specified A-DSG tunnel.
Step 4	cable dsg cfr <cfr index> dest_ip <ipaddr> [tunnel <tunnel index>] [dest-ports <start> <end>] [priority <priority>] [src-ip <ipaddr>] src-ip <ipaddr> [enable disable] Example: Router(config)# cable dsg cfr 1 dest-ip 224.10.10.101 tunnel 1 dest-port 0 65535 priority 1	Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS. This command creates an index to which one or several A-DSG 1.1 classifiers apply. To remove one or more specified A-DSG 1.1 classifiers from the Cisco CMTS, use the no form of this command. To disable one or more specified A-DSG 1.1 classifiers, but retain their configuration, use the disable form of this command. <ul style="list-style-type: none"> cfr index— dest_ip <ipaddr>—destination IP address tunnel <tunnel index>—tunnel index dest-ports <start> <end>—destination TCP/UDP ports range priority <priority>—Classifier priority src-ip <ipaddr>] src-ip <ipaddr>—source IP address enable—enable classifier disable—disable classifier

Command or Action	Purpose
Step 5 cable dsg chan-list <list-index> index <entry-index> freq <freq> Example: Router(config)#	Configures the A-DSG 1.1 downstream channel list. To remove the A-DSG 1.1 channel list from the Cisco CMTS, use the no form of this command. <ul style="list-style-type: none"> <i>list-index</i>— <i>entry-index</i>—DSG channel frequency entry index. <i>freq</i>—Center frequency of the downstream channel in Hz.
Step 6 cable dsg client-list <client-list-id> id-index <id> { application-id ca-system-id mac-addr broadcast } <value> Example: Router(config)# cable dsg chan-list 1 index 1 freq 47000000	Configures client parameters and associated DSG rule for A-DSG 1.1. To remove this configuration, use the no form of the command. <ul style="list-style-type: none"> client-list <client-list-id>—Alphanumeric string that names the DSG client list. <i>id-index</i> <id>—DSG Client ID settings application-id <value>—DSG Client type Application ID broadcast <value>—DSG Client type broadcast ca-system-id —DSG Client type CA system ID mac-addr <value>—DSG Client type Mac address
Step 7 cable dsg timer <index> [Tdsg1 <Tdsg1>] [Tdsg2 <Tdsg2>] [Tdsg3 <Tdsg3>] [Tdsg4 <Tdsg4>] Example: Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4	Configures the A-DSG 1.1 timer entry to be associated to the downstream channel, and encoded into the DCD message. To remove the cable DSG timer from the Cisco CMTS, use the no form of this command. <ul style="list-style-type: none"> <i>index</i>—Alphanumeric index identifier Tdsg1 <Tdsg1>—DSG Initialization Timeout (Tdsg1) setting Tdsg2 <Tdsg2>—DSG Operational Timeout (Tdsg2) setting Tdsg3 <Tdsg3>—DSG Two-Way Retry Timer (Tdsg3) setting Tdsg4 <Tdsg4>—DSG One-Way Retry Timer (Tdsg4) setting
Step 8 cable dsg vendor-param <group-id> vendor <vendor-index> oui <oui> value <value-in-TLV> Example: Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB	Configures vendor-specific parameters for A-DSG 1.1. To remove this configuration from the Cisco CMTS, use the no form of this command. <ul style="list-style-type: none"> <i>vendor</i>—DSG vendor parameters vendor index setting. <i>oui</i>—DSG vendor parameters vendor OUI setting. <i>value</i>—DSG vendor parameters vendor value setting.
Step 9 Ctrl^Z Example: Router(config)#	Returns to privileged EXEC mode.

What to Do Next

After global settings are defined for A-DSG 1.1, interface configurations must complete the configuration on the Cisco CMTS. Refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS”](#) section on page 17.

For additional information about global configuration commands, refer to the [“Command Reference” section on page 51](#).

Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS

A-DSG 1.1 parameters are uniquely identified by A-DSG indexes in global configuration mode. Then, those indexes are used with the interface commands in this section to define DCD messages. These interface commands define the DSG rules, tunnel traffic, and additional parameters to include in the DCD message.

Prerequisites

Global configurations for A-DSG 1.1 must be defined and enabled on the Cisco CMTS in order to complete A-DSG 1.1 interface configurations and A-DSG operation.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. [cable downstream dsg chan-list](#)
4. [cable downstream dsg timer](#)
5. [cable downstream dsg vendor-param](#)
6. [cable downstream dsg rule](#)
7. [cable downstream dsg dcd-enable](#)
8. **Ctrl^Z**

DETAILED STEPS

	Command or Action	Purpose
Step 1	enable Example: Router> enable	Enables privileged EXEC mode. <ul style="list-style-type: none">• Enter your password if prompted.
Step 2	configure terminal Example: Router# configure terminal	Enters global configuration mode.
Step 3	interface cable slot/subslot/port Example: Router(config)# interface c8/0/1	Enters interface configuration mode for the specified interface.

	Command or Action	Purpose
Step 4	cable downstream dsg chan-list <code><list-index></code> Example: Router(config-if)# cable downstream dsg chan-list 2	Associates the A-DSG channel list entry to a downstream channel, to be included in the DCD message. To remove this setting, use the no form of this command. <ul style="list-style-type: none"> chan-list—Sets the downstream A-DSG 1.1 channel list. list-index—Alphanumeric list index identifier.
Step 5	cable downstream dsg timer <code><timer-index></code> Example: Router(config-if)# cable downstream dsg timer 3	Associates the DSG timers entry to a downstream channel, to be included in the DCD message. To remove this setting, use the no form of this command. <ul style="list-style-type: none"> timer-index—Alphanumeric DSG timer setting
Step 6	cable downstream dsg vendor-param <code><vsif-grp-id></code> Example: Router(config-if)# cable downstream dsg vendor-param 2	To associate A-DSG vendor parameters to a downstream, to be included in the DCD message, use the downstream dsg vendor-param command in interface configuration mode. To remove this configuration from the Cisco CMTS, use the no form of this command. <ul style="list-style-type: none"> vsif-grp-id—Alphanumeric value that identifies vendor-specific parameters by the specified ID.
Step 7	cable downstream dsg rule <code><rule-id></code> priority <code><priority></code> clients <code><clnt-list-id></code> tunnel <code><tun-id></code> downstream dsg rule vendor-param <code><vsif-grp-id></code> downstream dsg rule <code><rule-id></code> ucid <code><ucid1></code> [<code><ucid1></code> <code><ucid2></code> ... <code><ucidn></code>] downstream dsg rule <code><rule-id></code> cfr <code><cfr-index></code> [<code><cfr-index></code>] downstream dsg rule <code><rule-id></code> disable Example: Router(config-if)# cable downstream dsg rule 1 priority 1 clients 1 tunnel 1	Defines and associates the A-DSG rule to the downstream channel. To disable a current configuration, use the disable form of this command. <ul style="list-style-type: none"> priority—DSG rule priority clients—DSG clients tunnel—DSG tunnel vendor-param—DSG vendor specific parameters ucid—DSG upstream channel id classifiers—DSG classifiers disable—DSG rule disable
Step 8	cable downstream dsg [dcd-enable dcd-disable] Example: Router(config-if)# cable downstream dsg dcd-enable	Enables DCD messages to be sent on a downstream channel. This command is used when there are no enabled rules or tunnels for A-DSG currently on the Cisco CMTS. To disable DCD messages, use the disable form of this command.
Step 9	Ctrl^Z Example: Router(config)#	Returns to privileged EXEC mode.

How to Configure DOCSIS Set-Top Gateway 1.0 on the Cisco CMTS

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

- [Enabling and Configuring the DOCSIS Set-Top Gateway Feature, page 19](#)
- [Configuring IP Multicast Operations, page 22](#)
- [Configuring NAT to Support Unicast Messaging \(optional\), page 24](#)
- [Disabling the DOCSIS Set-Top Gateway Feature, page 26](#)
- [Configuring a Standard IP Access List for Packet Filtering \(Optional\), page 27](#)
- [Configuring a Standard IP Access List for Multicast Group Filtering \(Optional\), page 29](#)

**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.
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: <ul style="list-style-type: none"> <i>tunnel-MAC-address</i> = 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. <i>group-ip-address</i> = 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). <i>CA-vendor-name</i> = 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.

	Command or Action	Purpose
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 <i>interface</i> 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: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • 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 37](#).



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 <i>wan-interface</i> 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 19 .
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. <ul style="list-style-type: none"> <i>ip-multicast-address</i> = 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 19. <i>cable-ip-address</i> = 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 <i>interface</i> Example: Router(config)# interface cable 3/0 Router(config-if)#	Enters interface configuration mode for the specified cable interface.
Step 3	no cable dsg <i>tunnel-MAC-address group-ip-address CA-vendor-name</i> 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 45](#).

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 <i>access-list</i> permit <i>group-ip-address</i> [<i>mask</i>] 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 <i>group-ip-address</i> and <i>mask</i> . <ul style="list-style-type: none"> • <i>access-list</i> = Number or name of a standard IP access list. The number can range from 1 to 99 with no default. • <i>group-ip-address</i> = IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels. • <i>mask</i> = (Optional) Bitmask that determines which addresses in the <i>group-ip-address</i> will be allowed access. The default is 255.255.255.255.

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

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

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



Tip

This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the [“Additional References” section on page 45](#).

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

I

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

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

How to Monitor the DOCSIS Set-Top Gateway Feature

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

- [Displaying DOCSIS Set-Top Gateway Tunnel Configurations, page 31](#)

Displaying DOCSIS Set-Top Gateway Tunnel Configurations

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.

Examples from A-DSG 1.1 and Cisco IOS Release 12.3(13)BC

The following example displays the mapping table for all DSG 1.1 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 statistics for all DSG 1.1 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 illustrates the **show cable dsg tunnel** command for A-DSG 1.1 on the Cisco uBR10012 router:

```

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

```

Tunnel	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 ID	Pri	UCID Interface	Client Range	Tunnel ID	Vender ID	Classifier Dst-IP	Pri	Src-IP
1	1	C8/1/0	1-4	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 rule <interface>
=====
```

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

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 example displays the statistics for the specified DSG 1.0 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.

The following example displays the mapping table for the specified DSG 1.0 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 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:

```
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

```
Router# 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

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 keepalive 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

```
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

```

**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, page 37](#)
- [Subinterface Configuration Example, page 38](#)
- [Unicast Messaging Configuration Example, page 41](#)
- [Packet Filtering Access List Configuration Example, page 41](#)
- [IP Multicast Access List Configuration Example, page 42](#)
- [IP Multicast Rate-Limiting Access List Configuration Example, page 44](#)

DSG Configuration Example

The following example illustrates the cable interface configuration on a Cisco uBR7246VXR router with the DOCSIS Set-Top Gateway (DSG) 1.0 feature enabled:



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 DSG 1.0 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 minislots-size 4
 cable upstream 0 modulation-profile 1
 no cable upstream 0 shutdown
 cable upstream 1 channel-width 1600000
 cable upstream 1 minislots-size 4
 cable upstream 1 modulation-profile 1
 cable upstream 1 shutdown
 cable upstream 2 channel-width 1600000
 cable upstream 2 minislots-size 4
 cable upstream 2 modulation-profile 1
 cable upstream 2 shutdown
 cable upstream 3 channel-width 1600000
 cable upstream 3 minislots-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 basic DSG 1.0 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 37](#), 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 basic DSG 1.0 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
Broadband Cable Command Reference	<i>Cisco Broadband Cable Command Reference Guide</i> , on Cisco.com: 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, on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/index.htm
Cisco IOS Release 12.3 Command Reference	<i>Cisco IOS Software Release 12.3 Mainline Command References</i> , on Cisco.com: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_command_reference_list.html
Cisco DOCSIS Set-top Technology White Paper	<i>Cisco DOCSIS Set-top Gateway White Paper</i> , on Cisco.com: http://www.cisco.com/en/US/products/hw/cable/ps2217/products_white_paper09186a00801b3f0f.shtml
DOCSIS 1.1 on the Cisco CMTS	<i>Configuring DOCSIS 1.1 on the Cisco CMTS</i> , in the <i>CMTS Feature Guide</i> , on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/cable/cab_rout/cmtsfg/ufg_docs.htm
IP Access Lists Configuration Guide	<i>Configuring IP Services, IP Addressing and Services, Cisco IOS IP Configuration Guide</i> , Release 12.2, on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipr_c/ipcprt1/1cfip.htm

Additional References

Related Topic	Document Title
IP Access Lists Command Reference Guide	<i>IP Services Commands, Cisco IOS IP Command Reference, Volume 1, Addressing and Services</i> , Release 12.2, on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fipras_r/index.htm
IP Multicast Configuration Guide	<i>Cisco IOS IP Configuration Guide</i> , Release 12.3 on Cisco.com: http://www.cisco.com/en/US/products/sw/iosswrel/ps5187/prod_configuration_guide09186a008017d581.html
IP Multicast Command Reference	<i>Cisco IOS IP Command Reference, Volume 3 of 3: Multicast</i> , Release 12.2 on Cisco.com: http://www.cisco.com/univercd/cc/td/doc/product/software/ios122/122cgcr/fiprnc_r/index.htm

Standards

Standards ¹	Title
CM-SP-DSG-I03-041124	CableLabs <i>DOCSIS Set-top Gateway (DSG) Interface Specification SP-DSG-I03-041124</i>
SP-RFIV1.1-I09-020830	CableLabs <i>Data-over-Cable Service Interface Specifications Radio Frequency Interface Specification</i> , version 1.1
SP-DSG-I01-020228	CableLabs <i>DOCSIS Set-top Gateway (DSG) Interface Specification</i>

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

RFCs ¹	Title
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 The specified 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 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.

```
%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

The following commands are introduced or modified in the feature or features documented in this module. For information about these commands, see the *Cisco IOS Cable Command Reference* at http://www.cisco.com/en/US/docs/ios/cable/command/reference/cmts_book.html. For information about all Cisco IOS commands, go to the Command Lookup Tool at <http://tools.cisco.com/Support/CLILookup> or to the *Cisco IOS Master Commands List*.

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

- **cable dsg cfr**
- **cable dsg chan-list**
- **cable dsg client-list**
- **cable dsg timer**
- **cable dsg vendor**
- **cable dsg tunnel**
- **cable downstream dsg chan-list**
- **cable downstream dsg dcd-enable**
- **cable downstream dsg rule**
- **cable downstream dsg timer**
- **cable downstream dsg vendor-param**
- **debug cable dsg**
- **show cable dsg tunnel**
- **show interface cable dsg downstream**

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.

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

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

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

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

DSG 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. A POD module is more frequently referred to as a Cable Card.

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).

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2007 Cisco Systems, Inc. All rights reserved.

