



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

This document describes the Advanced-mode DOCSIS Set-Top Gateway (A-DSG) Issue 1.1 on the Cisco Cable Modem Termination System (CMTS), commencing with Cisco IOS release 12.3(13a)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.

A-DSG 1.1 allows 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. A-DSG 1.1 introduces several additional and powerful enhancements to the Cisco CMTS and subscriber networks using DSG technology, described further in this document.



Note

Cisco IOS Release 12.3(13a)BC introduces a brand new command-line interface (CLI) and associated commands to support Advanced-mode DSG 1.1. These commands are not interoperable with the CLI commands supporting DSG Issue 1.0 and earlier issues prior to Cisco IOS Release 12.3(13a)BC.

When installed on the Cisco router, Cisco IOS Release 12.3(13a)BC converts any pre-existing DSG 1.0 configuration in the startup configuration to A-DSG 1.1 configuration in the running configuration. Cisco IOS 12.3(13a)BC does not support nor run DSG 1.0 configuration, nor does A-DSG 1.1 support the DSG 1.0 SNMP MIB on the 12.3(13a)BC IOS images.

Feature Specifications for Advanced-mode DOCSIS Set-Top Gateway

Feature History

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



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

© 2005-2007 Cisco Systems, Inc. All rights reserved.

Release 12.3(21)BC	The cable igmp static-group command was introduced. Information for the ip igmp static-group command was added.
Release 12.3(13a)BC	Advanced-mode DSG 1.1 (A-DSG) introduced for the following Cisco universal broadband routers: <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 and Cisco MC16C/S/E Cable Interface Line Cards – Cisco uBR-MC28U/X and Cisco MC28C Cable Interface Line Cards

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://tools.cisco.com/ITDIT/CFN/jsp/index.jsp>. 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 Advanced-mode DOCSIS Set-Top Gateway, page 3](#)
- [Restrictions for A-DSG 1.1, page 4](#)
- [Information About Advanced-mode DOCSIS Set-Top Gateway, page 7](#)
- [How to Configure Advanced-mode DOCSIS Set-Top Gateway 1.1 on the Cisco CMTS, page 15](#)
- [Configuring Additional Features for Advanced-mode DOCSIS Set-Top Gateway 1.1 on the Cisco CMTS, page 21](#)
- [How to Monitor the Advanced-mode DOCSIS Set-Top Gateway Feature, page 36](#)
- [Configuration Examples for Advanced-mode DOCSIS Set-Top Gateway, page 41](#)
- [Additional References, page 55](#)
- [System Messages, page 57](#)
- [Command Reference for Advanced-mode DSG Issue 1.1, page 59](#)
- [Glossary, page 89](#)

Prerequisites for Advanced-mode DOCSIS Set-Top Gateway

This section describes prerequisites for Advanced-mode DSG 1.1.

- [General Prerequisites for A-DSG 1.1, page 3](#)
- [IP Multicast Prerequisites for A-DSG 1.1, page 3](#)
- [IP Unicast Prerequisites for A-DSG 1.1, page 4](#)

General Prerequisites for A-DSG 1.1

- Cisco A-DSG 1.1 is supported on the Cisco uBR7246VXR router and the Cisco uBR10012 router with Performance Routing Engine (PRE) modules.
- Either Cisco CMTS requires 128MB in memory to support A-DSG 1.1.
- Cisco IOS release 12.3(13a)BC or a later 12.3 BC release are required.

Refer to the release notes for your Cisco CMTS for additional Cisco IOS information.

Advanced-mode DSG 1.1 (A-DSG 1.1) supports features that are currently described in the CableLabs® DOCSIS CM-SP-DSG-I03-041124 specification, which has a current state of “Issued.” Refer to the [“A-DSG 1.1 Features and Enhancements for the Cisco CMTS” section on page 7](#).

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

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

IP Multicast Prerequisites for A-DSG 1.1

- 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.
- To enable and configure the Advanced-mode DOCSIS Set-Top Gateway feature, Protocol Independent Multicast (PIM) must be enabled on the cable interface and all outgoing WAN interfaces using the **ip pim** interface command. The Advanced-mode DOCSIS Set-Top Gateway feature supports the following PIM modes:
 - **dense-mode**—Dense mode of operation.
 - **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.
- 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.



Note The **rate-limit** keyword is not supported on Cisco IOS Release 12.2(33)SCC and later.

- (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 55](#).

IP Unicast Prerequisites for A-DSG 1.1

- Network Address Translation (NAT) must be configured to support unicast for A-DSG 1.1 messaging on the Cisco CMTS. Refer to the [“Configuring NAT to Support Unicast Messaging \(optional\)” section on page 29](#) for additional information.
- The Cisco uBR10012 and Cisco uBR72436VXR routers support IP multicast that uses generic routing encapsulation (GRE) tunnels over IP unicast. In this case, the DSG server (the Cisco CMTS) or a router external to the Cisco CMTS encapsulates the IP multicast packet within an IP unicast packet. The DSG Agent then unencapsulates the IP unicast tunnel and forwards the IP multicast packet onto a DSG tunnel. Refer to the [“Using Point of Deployment Modules and DSG Tunnels” section on page 12](#).

Restrictions for A-DSG 1.1

This section describes restrictions for Advanced-mode DSG 1.1, as supported in Cisco IOS release 12.3(13a)BC:

- Cisco A-DSG 1.1 does not support the Cisco uBR7100 series routers.
- Cisco A-DSG 1.1 does not support Service Flow Quality of Service (QoS), which is available at Layer 3. The Multicast Quality of Service (MQoS) feature can be configured separately to provide QoS for DSG tunnels. Refer to the release notes for Cisco IOS Release 12.3(13a)BC for additional information.
- Cisco A-DSG 1.1 does not support subinterfaces.
- Cisco A-DSG 1.1 does not support SNMP MIBS for the prior DSG 1.0 feature.
- Cisco A-DSG 1.1 does not support tunnel security, but supports access control lists (ACLs); these must be configured to prevent cable modems or other CPE devices from sending traffic to the DSG tunnels.

Additional security configuration must be applied to verify packets in the upstream are valid. Such configurations should include the following steps:

1. **interface CableX/Y/Z**
2. **cable source-verify**
3. **ip verify unicast source reachable-via rx**
4. **ip access-group dsg out**
5. **exit**

In this configuration, the DSG access group should be as follows:

- **ip access-list extended dsg**
- **deny ip** *<cm network>* *<cm network mask XOR FFFFFFFF>* **host** *<dsg tunnel cfr multicast group 1>*
- **deny ip** *<cpe network>* *<cpe network mask XOR FFFFFFFF>* **host** *<dsg tunnel cfr multicast group 1>*

- **deny ip** <cm network> <cm network mask XOR FFFFFFFF> **host** <dsg tunnel cfr multicast group n>
- **deny ip** <cpe network> <cpe network mask XOR FFFFFFFF> **host** <dsg tunnel cfr multicast group n>
- **permit ip any any**

DSG Restrictions

The following restrictions apply when using DSG configuration:

DSG Configuration File Transfer Operations

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

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

DSG Configuration for Cable Per Physical Downstream Static Multicast Support

Cable Per Physical Downstream Static Multicast support was first enabled on DSG in Cisco IOS Release 12.3(13a)BC.

Beginning with Cisco IOS 12.3(21)BC, the following a new CLI is enabled for the Cable Per Physical Downstream Static Multicast feature:

```
cable igmp static-group <multicast group>
```

This CLI will only exist on Slave interfaces and, in order to eliminate any confusion with the DSG configuration, will only be display at “show run” if configured via a CLI. If this new CLI is configured by DSG, the CLI will remain hidden for that particular multicast group.



Note

If a subinterface is configured at a virtual bundle interface, the subinterface number option for this CLI must be configure to match up the desired subinterface devices.



Note

Any Multicast group being used by DSG (or CLI) within the same CMTS, should not be used for CLI (or DSG) configuration.

Resolved Caveats in Cisco IOS Release 12.3(13a)BC

This document will cite Caveats resolved in Cisco IOS release 12.3(13a)BC. However, such Caveats are listed in the following release note documents on Cisco.com:

- *Release Notes for Cisco uBR10012 Universal Broadband Router for Cisco IOS Release 12.3 BC*
http://www.cisco.com/en/US/prod/collateral/video/ps8806/ps5684/ps2209/prod_bulletin0900aecd80306ccc_ps2217_Products_Bulletin.html

- *Release Notes for Cisco uBR7200 Series for Cisco IOS Release 12.3 BC*
http://www.cisco.com/en/US/docs/cable/cmts/ubr7200/release/notes/12_3bc/123BCu72.html

Information About Advanced-mode DOCSIS Set-Top Gateway

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

- [A-DSG 1.1 Features and Enhancements for the Cisco CMTS, page 7](#)
- [General Feature Overview for DOCSIS Set-Top Gateway, page 10](#)
- [Primary Benefits of DOCSIS Set-Top Gateway, page 14](#)

A-DSG 1.1 Features and Enhancements for the Cisco CMTS

A-DSG 1.1 and Cisco IOS Release 12.3(13a)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 1.1 emphasize the following:

- [A-DSG 1.1 Tunnels, page 7](#)
- [A-DSG 1.1 Classifiers, page 8](#)
- [A-DSG 1.1 Downstream Channel Descriptor \(DCD\), page 8](#)
- [A-DSG 1.1 Process, page 9](#)
- [A-DSG 1.1 Rule, page 9](#)

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

Cisco IOS Release 12.3(13a)BC does not support the CISCO-CABLE-DSG-IF-MIB. Support for this MIB requires Cisco IOS Release 12.3(9a)BC.

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.

Multiple IP multicast addresses can be mapped to a single tunnel, but a specific IP multicast address can only be mapped to one tunnel.

A-DSG tunnels are configured in global configuration mode. Then, classifiers are created with tunnel associations, also in global configuration mode. The 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 15](#).

A-DSG 1.1 Classifiers

A classifier for A-DSG 1.1 is used to provide additional layer 3 and layer 4 filtering for the DSG tunnel. The A-DSG multicast software module applies the classifier parameters to incoming packets received from the A-DSG server in order to assign packets to the appropriate A-DSG tunnel.



Note

The A-DSG tunnel must be configured before a classifier can be associated with it.

Before changing the classifier tunnel association to another DSG tunnel, if a classifier is associated to a rule, then you must remove the classifier that is associated with the rule.

For configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 15.](#)

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 DSG Client to determine which tunnel and classifier to use.

The DCD has 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 tunnels.

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

- DSG rules and rule priority
- DSG classifiers
- DSG channel list type/length value (TLV)
- DSG client identifier (whether broadcast, CA System, application, or MAC-level)
- DSG timer list
- DSG upstream channel ID (UCID) list
- Vendor-specific information field

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

The DCD message provides several functions, such as the following:

- 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.
- Enables global changes to the DSG Client timers that allow operator-driven changes in DSG eCM performance.

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

A-DSG 1.1 supports the CableLabs® DOCSIS CM-SP-DSG-I03-041124 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 15](#).

For interface configuration information, refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS” section on page 18](#).

A-DSG 1.1 Process

The Advanced DSG 1.1 processor 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 the timer expires and handles the DCD processing.

For global and timer configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 15](#).

For interface configuration information, refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS” section on page 18](#).

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.

For global and timer configuration information, refer to the [“Configuring Global A-DSG 1.1 Settings for the Cisco CMTS” section on page 15](#).

For interface configuration information, refer to the [“Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS” section on page 18](#).

General Feature Overview for DOCSIS Set-Top Gateway

The Advanced-mode 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 to which a user is entitled
- 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 the A-DSG 1.1 Network

The Advanced-mode 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.

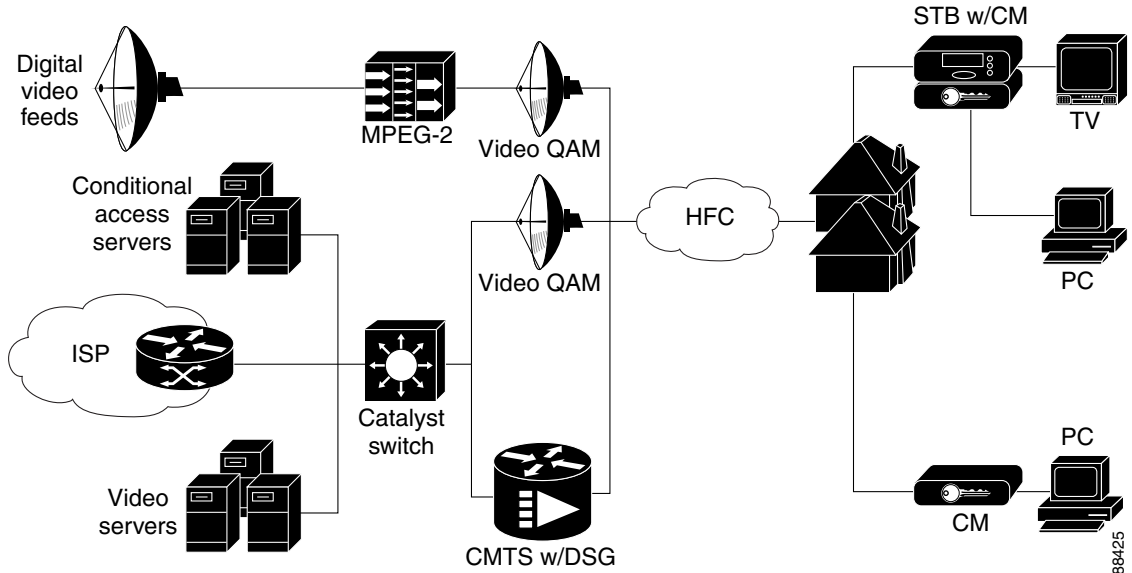
A typical DSG network contains the following components:

- 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 Advanced-mode 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 Releases *prior* to 12.3(13a)BC do not support one-to-many mappings (one IP multicast group per multiple MAC addresses/DSG tunnel). 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 downstream channels receive the packet and examine the MAC address, based on the tunnels identified for it in a DSG Rule for A-DSG 1.1, or based on the well-known MAC address of the device (for DSG Issues 1.0 and 0.9). The IP address is only examined if it is part of a classifier in the DCD.
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.

Primary Benefits of DOCSIS Set-Top Gateway

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

Part of CableLabs Specifications

The Advanced-mode 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 Advanced-mode 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 Advanced-mode 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 Advanced-mode 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 Advanced-mode 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 15](#)
- [Configuring A-DSG 1.1 Interface Settings for the Cisco CMTS, page 18](#)

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

These global A-DSG settings and 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> [enable | disable]**
4. **cable dsg cfr <cfr index> dest-ip <ipaddr> [tunnel <tunnel index>] | [dest-port <start> <end>] | [priority <priority>] | [src-ip <ipaddr>] | [src-prefix-len <len>] [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 } <value> | broadcast }**
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	<p>enable</p> <p>Example: Router> enable</p>	<p>Enables privileged EXEC mode.</p> <ul style="list-style-type: none"> Enter your password if prompted.
Step 2	<p>configure terminal</p> <p>Example: Router# configure terminal</p>	<p>Enters global configuration mode.</p>
Step 3	<p>cable dsg tunnel <tunnel-id> mac_addr <mac_addr> [enable disable]</p> <p>Example: Router(config)# cable dsg tunnel 1 mac_addr 0006.0006.0006 enable</p>	<p>Creates A-DSG 1.1 tunnels. The destination MAC address 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.</p> <ul style="list-style-type: none"> tunnel-id—This is an integer from 1-65535 that identifies the A-DSG tunnel in related show and configuration commands. mac_addr mac-addr—(Required) Destination MAC address. enable—Enables the specified A-DSG tunnel. disable—Disables the specified A-DSG tunnel.
Step 4	<p>cable dsg cfr <cfr index> dest-ip <ipaddr> [tunnel <tunnel index>] [dest-port <start> <end>] [priority <priority>] [src-ip <ipaddr> src-prefix-len <len>] [enable disable]</p> <p>Example: Router(config)# cable dsg cfr 1 dest-ip 224.10.10.101 tunnel 1 dest-port 0 65535 priority 1</p>	<p>Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS. This command creates a unique CFR index for the A-DSG 1.1 classifier. To remove the 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.</p> <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>—source IP address src-prefix-len <len>—prefix length enable—enable classifier disable—disable classifier

Command or Action	Purpose
<p>Step 5</p> <pre>cable dsg chan-list <list-index> index <entry-index> freq <freq></pre> <p>Example: Router(config)# cable dsg chan-list 1 index 1 freq 47000000</p>	<p>Configures the A-DSG 1.1 downstream channel list. The channel list is a list of DSG channels (downstream frequencies) that set-top boxes can search to find the DSG tunnel appropriate for their operation. To remove the A-DSG 1.1 channel list from the Cisco CMTS, use the no form of this command.</p> <ul style="list-style-type: none"> • <i>list-index</i>—an index used to indicate a group of channels (downstream frequencies) to include in the DCD messages for an interface. • <i>entry-index</i>—DSG channel frequency entry index. • <i>freq</i>—Center frequency of the downstream channel in Hz. This value must be a multiple of 62500 Hz.
<p>Step 6</p> <pre>cable dsg client-list <client-list-id> id-index <id> { application-id ca-system-id mac-addr } <value> broadcast }</pre> <p>Example: Router(config)# cable dsg client-list 1 id-index 1 broadcast</p>	<p>Configures additional client parameters. To remove this configuration, use the no form of the command.</p> <ul style="list-style-type: none"> • client-list <client-list-id>—an integer between 1-65535. • <i>id-index</i> <id>—References a specific client entry within the client list. • application-id <value>—DSG Client type Application ID • broadcast —DSG Client type broadcast • ca-system-id —DSG Client type CA system ID • mac-addr <value>—DSG Client type Mac address
<p>Step 7</p> <pre>cable dsg timer <index> [Tdsg1 <Tdsg1>] [Tdsg2 <Tdsg2>] [Tdsg3 <Tdsg3>] [Tdsg4 <Tdsg4>]</pre> <p>Example: Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4</p>	<p>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.</p> <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
<p>Step 8</p> <pre>cable dsg vendor-param <group-id> vendor <vendor-index> oui <oui> value <value-in-TLV></pre> <p>Example: Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB</p>	<p>Configures vendor-specific parameters for A-DSG 1.1. To remove this configuration from the Cisco CMTS, use the no form of this command.</p> <ul style="list-style-type: none"> • <i>vendor</i>—DSG vendor parameters vendor index setting. • <i>oui</i>—DSG vendor parameters vendor OUI setting. Includes the 0803<oui> tlv in the VSIF. • <i>value</i>—DSG vendor parameters vendor value setting.
<p>Step 9</p> <pre>Ctrl+Z</pre> <p>Example: Router(config)#</p>	<p>Returns to privileged EXEC mode.</p>

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 18.

For additional information about global configuration commands, refer to the [“Command Reference for Advanced-mode DSG Issue 1.1”](#) section on page 59.

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 <i>slot/subslot/port</i> Example: Router(config)# interface c8/0/1	Enters interface configuration mode for the specified interface.

	Command or Action	Purpose
Step 4	<pre> cable downstream dsg chan-list <list-index> Example: Router(config-if)# cable downstream dsg chan-list 2 </pre>	<p>Associates the A-DSG channel list entry to a downstream channel, to be included in the DCD message. To remove this setting, use the no form of this command.</p> <ul style="list-style-type: none"> • chan-list—Sets the downstream A-DSG 1.1 channel list. • <i>list-index</i>—This is an integer between 1 and 65535.
Step 5	<pre> cable downstream dsg timer <timer-index> Example: Router(config-if)# cable downstream dsg timer 3 </pre>	<p>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.</p> <ul style="list-style-type: none"> • <i>timer-index</i>—This is an integer between 1 and 65535.
Step 6	<pre> cable downstream dsg vendor-param <vsif-grp-id> Example: Router(config-if)# cable downstream dsg vendor-param 2 </pre>	<p>Associates A-DSG vendor parameters to a downstream, to be included in the DCD message. To remove this configuration from the Cisco CMTS, use the no form of this command.</p> <ul style="list-style-type: none"> • <i>vsif-grp-id</i>—Value identifies vendor-specific parameters by the specified ID.
Step 7	<pre> cable downstream dsg rule <rule-id> priority <priority> cable downstream dsg rule vendor-param <vsif-grp-id> cable downstream dsg rule <rule-id> ucid <ucid1> [<ucid1> <ucid2>...<ucidn>] cable downstream dsg rule <rule-id> cfr <cfr-index> [<cfr-index>] cable downstream dsg rule <rule-id> [enable disable] Example: Router(config-if)# cable downstream dsg rule 1 clients 1 tunnel 1 </pre>	<p>Defines and associates a rule for A-DSG to the downstream channel. Rules are disabled by default once they are created. To enable a rule you must use the enable form of this command. To disable a current configuration, use the disable form of this command.</p> <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 <p>Note For easy migration to future issues of A-DSG in upcoming Cisco IOS releases, A-DSG rules that associate with the same A-DSG tunnel must associate with the same list of classifiers.</p>
Step 8	<pre> cable downstream dsg [dcd-enable dcd-disable] Example: Router(config-if)# cable downstream dsg dcd-enable </pre>	<p>Enables DCD messages to be sent on a downstream channel. This command is used when there are no enabled rules or tunnels for A-DSG currently on the Cisco CMTS. To disable DCD messages, use the disable form of this command.</p>
Step 9	<pre> Ctrl^Z Example: Router(config)# </pre>	<p>Returns to privileged EXEC mode.</p>

Examples

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

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

Downstream 1

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

Downstream 2

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

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

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

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

Configuring Additional Features for Advanced-mode DOCSIS Set-Top Gateway 1.1 on the Cisco CMTS

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

- [Configuring Cable Per Physical Downstream Static Multicast Support \(optional\), page 21](#)
- [Configuring IP IGMP Static-Group, page 24](#)
- [Configuring IP Multicast Operations, page 26](#)
- [Configuring NAT to Support Unicast Messaging \(optional\), page 29](#)
- [Configuring WAN Interfaces for MultiCast Operations, page 31](#)
- [Configuring a Standard IP Access List for Packet Filtering \(Optional\), page 31](#)
- [Configuring a Standard IP Access List for Multicast Group Filtering \(Optional\), page 34](#)

Configuring Cable Per Physical Downstream Static Multicast Support (optional)

This section describes how to configure support for Cable per physical downstream Static Multicast on the Cisco CMTS. Doing so will enable the Cisco CMTS to control the replication of static IP multicast streams within a cable bundle.

SUMMARY STEPS

1. **configure terminal**
2. **ip multicast-routing**
3. **ip pim ssm**
4. **ip pim sparse-mode**
5. **ip igmp version 3**
6. **ip igmp static-group** *{* | group-address [source {source-address | ssm-map}] | class-map class-map-name}*
7. **cable igmp static-group** *[multicast group] source [source IP] [subinterface number]*
8. **cable bundle** *n*
9. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example: Router# configure terminal Router(config)#</p>	Enters global configuration mode.
Step 2	<p>ip multicast-routing</p> <p>Example: Router(config)# ip multicast-routing Router(config)#</p>	Enables multicast routing on the router.
Step 3	<p>ip pim ssm [vrf vrf-name] ssm {default range access-list}</p> <p>Example: Router(config)# ip pim ssm range 4</p>	<p>Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command.</p> <ul style="list-style-type: none"> vrf— (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance. vrf-name—(Optional) Name assigned to the VRF. default—Defines the SSM range access list to 232/8. range access-list—Specifies the standard IP access list number or name defining the SSM range. <p>Note When an SSM range of IP multicast addresses is defined by the ip pim ssm command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.</p> <p>For additional information about the ip pim ssm command, refer to the following document on Cisco.com:</p> <ul style="list-style-type: none"> <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i>, Release 12.3 T http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/ip3_m1g.html
Step 4	<p>ip pim {dense-mode sparse-mode sparse-dense-mode}</p> <p>Example: Router(config-if)# ip pim dense-mode Router(config-if)#</p>	<p>Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature:</p> <ul style="list-style-type: none"> dense-mode—Enables dense mode of operation. sparse-mode—Enables sparse mode of operation. sparse-dense-mode—The interface is treated in either sparse mode, sparse-dense mode, or dense mode of operation, depending on the mode in which the multicast group operates. <p>Note You must configure this command on each interface that forwards multicast traffic.</p>

	Command or Action	Purpose
Step 5	<pre>ip pim version 3</pre> <p>Example: Router(config-if)# ip igmp version 3 Router#</p>	Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2.
Step 6	<pre>ip igmp static-group [* group-address [source {source-address ssm-map}] class-map class-map-name]</pre> <p>Example: Router(config-if)# ip igmp static-group [* 232.1.1.7 [source {232 ssm-map}] class-map static1} Router#</p>	Configure static group membership entries on the cable interface.
Step 7	<pre>cable igmp static-group [multicast group] source [source IP] [subinterface number]</pre> <p>Example: Router(config-if)# cable igmp static-group 232.1.1.1 source 10.1.1.1</p>	<p>Controls the replication of static IP multicast streams within a cable bundle.</p> <p>This command can only be configured on cable physical interface as part of a Cable Bundle group.</p> <p>This command, by itself, does not take any effect. It must be configured with the ip igmp static-group command, which is configured at Bundle interface.</p> <p>The <i>[source IP]</i> option is used for SSM group range, as defined in ip pim ssm CLI. This is similar to the ip igmp static-group command usage.</p> <p>The <i>[subinteface number]</i> option must be used if there are multiple Bundle subinterfaces (Bundle1.1, Bundle 1.2, etc.)</p> <p>Note If a subinterfaces are configured on the virtual bundle interface, the subinterface number option for this CLI must be configure in order to match up the desired subinterface devices.</p>
Step 8	<pre>cable bundle n</pre> <p>Example: Router(config-if)# cable bundle 1 Router#</p>	<p>Configures the cable interface to be a slave bundle for the specified bundle group.</p> <ul style="list-style-type: none"> n = Bundle group number. The valid range is 1 to 255, with no default.
Step 9	<pre>exit</pre> <p>Example: Router(config-if)# exit Router#</p>	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring IP IGMP Static-Group

This section describes how to configure `ip igmp static-group` on the Cisco CMTS. Doing so will enable the Cisco CMTS to be a statically connected member of the specified group on the interface.

SUMMARY STEPS

1. `configure terminal`
2. `ip multicast-routing`
3. `ip pim ssm`
4. `ip pim sparse-mode`
5. `ip igmp version 3`
6. `ip igmp static-group` *{* | group-address* [`source` *{source-address | ssm-map}*] | `class-map` *class-map-name*}
7. `cable bundle n`
8. `exit`

DETAILED STEPS

	Command or Action	Purpose
Step 1	<code>configure terminal</code> Example: Router# <code>configure terminal</code> Router(config)#	Enters global configuration mode.
Step 2	<code>ip multicast-routing</code> Example: Router(config)# <code>ip multicast-routing</code> Router(config)#	Enables multicast routing on the router.

Command or Action	Purpose
<p>Step 3</p> <pre>ip pim ssm [vrf vrf-name] ssm {default range access-list}</pre> <p>Example: Router(config)# ip pim ssm range 4</p>	<p>Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command.</p> <ul style="list-style-type: none"> vrf— (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance. vrf-name—(Optional) Name assigned to the VRF. default—Defines the SSM range access list to 232/8. range access-list—Specifies the standard IP access list number or name defining the SSM range. <p>Note When an SSM range of IP multicast addresses is defined by the ip pim ssm command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.</p> <p>For additional information about the ip pim ssm command, refer to the following document on Cisco.com:</p> <ul style="list-style-type: none"> <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i>, Release 12.3 T http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/ip3_m1g.html
<p>Step 4</p> <pre>ip pim {dense-mode sparse-mode sparse-dense-mode}</pre> <p>Example: Router(config-if)# ip pim dense-mode Router(config-if)#</p>	<p>Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature:</p> <ul style="list-style-type: none"> dense-mode—Enables dense mode of operation. sparse-mode—Enables sparse mode of operation. sparse-dense-mode—The interface is treated in either sparse mode, sparse-dense mode, or dense mode of operation, depending on the mode in which the multicast group operates. <p>Note You must configure this command on each interface that forwards multicast traffic.</p>
<p>Step 5</p> <pre>ip pim version 3</pre> <p>Example: Router(config-if)# ip igmp version 3 Router#</p>	<p>Enables IGMPv3 on this interface. The default version of IGMP is set to Version 2.</p>

	Command or Action	Purpose
Step 6	<pre>ip igmp static-group {* group-address [source {source-address ssm-map}] class-map class-map-name}</pre> <p>Example: Router(config-if)# ip igmp static-group {* 232.1.1.7 [source {232 ssm-map}] class-map static1} Router# </p>	Configure static group membership entries on the cable interface.
Step 7	<pre>cable bundle n</pre> <p>Example: Router(config-if)# cable bundle 1 Router# </p>	Configures the cable interface to be a slave bundle for the specified bundle group. <ul style="list-style-type: none"> n = Bundle group number. The valid range is 1 to 255, with no default.
Step 8	<pre>exit</pre> <p>Example: Router(config-if)# exit Router# </p>	Exits interface 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. **ip pim ssm**
4. **ip cef**
5. **interface interface**
6. **ip pim {dense-mode | sparsrse-mode | sparse-dense-mode}sparse-dense-mode | sparse-mode**
7. **ip mroute-cache**
8. **exit**

DETAILED STEPS

	Command or Action	Purpose
Step 1	<pre>configure terminal</pre> <p>Example: Router# configure terminal Router(config)# </p>	Enters global configuration mode.
Step 2	<pre>ip multicast-routing</pre> <p>Example: Router(config)# ip multicast-routing Router(config)# </p>	Enables multicast routing on the router.
Step 3	<pre>ip pim ssm [vrf vrf-name] ssm {default range access-list}</pre> <p>Example: Router(config)# ip pim ssm range 4 </p>	<p>Defines the Source Specific Multicast (SSM) range of IP multicast addresses. To disable the SSM range, use the no form of this command.</p> <ul style="list-style-type: none"> vrf— (Optional) Supports the multicast Virtual Private Network (VPN) routing and forwarding (VRF) instance. vrf-name—(Optional) Name assigned to the VRF. default—Defines the SSM range access list to 232/8. range access-list—Specifies the standard IP access list number or name defining the SSM range. <p>Note When an SSM range of IP multicast addresses is defined by the ip pim ssm command, no Multicast Source Discovery Protocol (MSDP) Source-Active (SA) messages will be accepted or originated in the SSM range.</p> <p>For additional information about the ip pim ssm command, refer to the following document on Cisco.com:</p> <ul style="list-style-type: none"> <i>Cisco IOS IP Command Reference, Volume 3 of 4: Multicast</i>, Release 12.3 T http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/ip3_m1g.html
Step 4	<pre>ip cef [distributed] [accounting type load-sharing algorithm algorithm table type traffic-statistics]</pre> <p>Example: Router(config)# </p>	<p>Enables Cisco Express Forwarding (CEF) on the route processor card. To disable CEF, use the no form of this command.</p> <p>For additional information about the ip cef command, refer to the following document on Cisco.com:</p> <ul style="list-style-type: none"> <i>Cisco IOS Switching Services Command Reference</i>, Release 12.3 http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swi_i1.html

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

For the Cisco uBR10012 router, A-DSG 1.1 can also use an external router that is close to the Cisco CMTS to support unicast messaging. In this case, the nearby router must support NAT, and then send the address-translated multicast IP packets to the Cisco CMTS.



Tip

This procedure should be performed after the cable interface has already been configured for DSG operations, as described in the [“A-DSG 1.1 Cable Interface Configuration Examples”](#) section on page 44.



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.

	Command or Action	Purpose
Step 3	<p>ip nat outside</p> <p>Example: Router(config-if)# ip nat outside Router(config-if)#</p>	Configures the WAN interface as the “outside” (public) NAT interface.
Step 4	<p>interface cable interface</p> <p>Example: Router(config-if)# interface cable 3/0 Router(config-if)#</p>	<p>Enters interface configuration mode for the specified cable interface.</p> <p>Note This cable interface should have previously been configured for DSG operations.</p>
Step 5	<p>ip address ip-address mask secondary</p> <p>Example: Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary Router(config-if)#</p>	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	<p>ip nat inside</p> <p>Example: Router(config-if)# ip nat inside Router(config-if)#</p>	Configures the cable interface as the “inside” NAT (private) interface.
Step 7	<p>exit</p> <p>Example: Router(config-if)# exit Router(config)#</p>	Exits interface configuration mode and returns to global configuration mode.
Step 8	<p>ip nat inside source static ip-multicast-address cable-ip-address</p> <p>Example: Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2 Router(config)#</p>	<p>Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.</p> <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. <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	<p>exit</p> <p>Example: Router(config)# exit Router#</p>	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Interfaces for MultiCast Operations

In addition to basic WAN interface configuration on the Cisco CMTS, described in other documents, the following WAN interface commands should be configured on the Cisco CMTS to support IP multicast operations with A-DSG 1.1, as required.

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

These commands are described in the “[Configuring IP Multicast Operations](#)” section on page 26, and in the following documents on Cisco.com.

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

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast*, Release 12.3
http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/ip3_m1g.html

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

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast*, Release 12.3 T
http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/ip3_m1g.html

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

- *Cisco IOS Switching Services Command Reference*, Release 12.3
http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swi_i1.html

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

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



Tip

This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the “[Additional References](#)” section on page 55.

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	<p>configure terminal</p> <p>Example: Router# configure terminal Router(config)#</p>	Enters global configuration mode.
Step 2	<p>access-list access-list permit group-ip-address [mask]</p> <p>Example: Router(config)# access-list 90 permit 228.1.1.1 Router(config)#</p>	<p>Creates an access list specifying that permits access to the specific multicast address that matches the specified <i>group-ip-address</i> and <i>mask</i>.</p> <ul style="list-style-type: none"> <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 3	<p>access-list access-list deny group-ip-address [mask]</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 access-list deny any</p> <p>Example: Router(config)# access-list 90 deny any Router(config)#</p>	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	<p>interface cable interface</p> <p>Example: Router(config)# interface cable 3/0 Router(config-if)#</p>	Enters interface configuration mode for the specified cable interface.

Command or Action	Purpose
<p>Step 6 <code>ip access-group access-list</code></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. <p>Note: Standard Access lists only allow one address to be specified in the earlier step. If you apply an outbound access-list with only the multicast address of the tunnel denied, then the DSG traffic is not allowed to pass.</p> <p>Note On the Cisco uBR10012 router, inbound access lists on the cable interface do not apply to multicast traffic, so they do not apply here. As a result, the Cisco uBR10012 requires that you use extended access lists that are blocked in the outbound direction for packets originating from the cable modem or CPE device on the network, and destined to the multicast group. The multicast group contains the classifiers associated with A-DSG 1.1 rules enabled on the interface.</p>
<p>Step 7 <code>exit</code></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 55](#).

SUMMARY STEPS

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

DETAILED STEPS

	Command or Action	Purpose
Step 1	configure terminal Example: Router# configure terminal Router(config)#	Enters global configuration mode.
Step 2	access-list <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 Advanced-mode DOCSIS Set-Top Gateway Feature

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

- [Displaying Advanced-mode DOCSIS Set-Top Gateway Tunnel Configurations, page 36](#)

Displaying Advanced-mode DOCSIS Set-Top Gateway Tunnel Configurations

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

Refer to the “[Configuration Examples for Advanced-mode DOCSIS Set-Top Gateway](#)” section on [page 41](#) for additional information.

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
0000.0000.0002
    230.0.0.2
      Cable8/1/0
0000.0000.0003
    230.0.0.3
      Cable8/1/0
0000.0000.0004
    230.0.0.4
      Cable8/1/0
0000.0000.0005
    230.0.0.5
      Cable8/1/0
0000.0000.0006
    230.0.0.6
      Cable8/1/0
0000.0000.0007
    230.0.0.7
      Cable8/1/0
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
0001.0002.0007
    229.1.2.7
      Cable8/1/0
0001.0002.0005
    229.1.2.5
      Cable8/1/0
0001.0002.0004
    229.1.2.4
      Cable8/1/0
0001.0002.0003
    229.1.2.3
      Cable8/1/0
0001.0002.0002
    229.1.2.2
      Cable8/1/0
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	Classifier	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	UCID Pri	Client Interface	Client Range	Tunnel ID	Vendor ID	Vendor ID	Classifier Dst-IP	Classifier Pri	Src-IP
1	1	C8/1/0	1-4	1	1	1	229.4.4.4	0	100.1.1.1 229.4.4.5 1 100.1.1.2

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

```
show cable dsg rule <interface>
```

```
=====
```

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

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

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

```
=====
```

```
0004.0004.0004 229.4.4.4 C8/1/0 DCD Sent: 99 DCD Change Count: 7
  Resolves: 10      Rcv/Fwd/Drp: 0/0/0
```

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

The following 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 Advanced-mode DOCSIS Set-Top Gateway

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

- [A-DSG 1.1 Global Configuration Examples, page 41](#)
- [A-DSG 1.1 Cable Interface Configuration Examples, page 44](#)
- [A-DSG 1.Subinterface Configuration Example, page 47](#)
- [Unicast Messaging Configuration Example, page 50](#)
- [Packet Filtering Access List Configuration Example, page 51](#)
- [IP Multicast Access List Configuration Example, page 52](#)
- [IP Multicast Rate-Limiting Access List Configuration Example, page 53](#)

A-DSG 1.1 Global Configuration Examples

show cable dsg tunnel

The following example illustrates configuration information with the **show cable dsg tunnel** command, to include tunnel MAC address, state, number of classifiers associated, number of interfaces to which tunnel is associated, number clients associated, and the QoS service class name for all the configured tunnels.

```

Router# show cab dsg tunnel
tunnel tunnel tunnel      cfr  cfr  tunnel in  rule rule  client service
id     state mac-addr id   state interface id  state listId class
1      en   0100.5e01.0114 1    en   Cable5/0  1  en   2
          11  en
          14  en
          20  en   2
          Cable5/1 7  dis  10
          8  dis  2
2      en   0100.5e01.0115 2    en   Cable5/0  2  en   2
          10  en
3      en   0100.5e01.0128 3    en   Cable5/0  3  en   3
4      en   0100.5e01.0133 4    en   Cable5/0  4  dis  4
5      en   0100.5e01.013c 5    en   Cable5/0  5  dis  5
          9    en

```

```

6      dis      0100.5e01.0146 6      en      Cable5/0 6      dis      6
7      dis      0100.5e01.0150
8      en       0100.5e01.0119
9      en       0100.5e01.0133
10     en       0100.5e01.0147
11     en       2222.2222.2222
12     en       3333.3333.3333

```

The following example illustrates information for a specified tunnel:

```

Router# show cab dsg tunnel 1
tunnel tunnel cfr      cfr      tunnel in  rule rule  client service
id      state mac-addr  id      state interface id  state listID class
1       en    0100.5e01.0114 1       en    Cable5/0 1  en    2
                               11      en
                               14      en
                               Cable5/1 7  dis   10
                               8       dis   2
                               20      en    2
                               Cable5/1 7  dis   10
                               8       dis   2
                               4       en    4
                               11      en    2

```

The following example illustrates information about all the classifiers associated with a given tunnel.

```

Router# show cab dsg tunnel 1 cfr
tunnel cfr  cfr  cfr destination ip  source ip  srcPre d_port d_port
id      id  state pri address          address    length start end
1       1  en   0  230.1.1.20      0.0.0.0   32     0     65535
        11 en   0  224.25.25.134  0.0.0.0   32     0     65535
        14 en   0  230.1.1.20      0.0.0.0   32     1000  2000

```

The following example illustrates information about all the clients associated with a given tunnel:

```

Router# show cab dsg tunnel 1 clients
tunnel client client client      client
id      listId id    id type      address
1       2     1     CA System ID: 0951
        3     Broadcast
        8     MAC Addr: 1111.1111.1111
10     1     Application ID: 0001

```

The following example illustrates information about all the interfaces and rules associated with a given tunnel:

```

Router# show cab dsg tunnel 1 interfaces
tunnel downstream  rule
id      interface  id
1       Cable5/0     1 7 8 20
        Cable5/1     7 8

```

The following example illustrates information about the packet statistics information for a given tunnel:

```

Router# show cab dsg tunnel 1 statistics
tunnel cfr  cfr  destination ip  source ip  total  total
id      id  state address          address    forwarded received
1       1  en   230.1.1.20      0.0.0.0   0      0
        11 en   224.25.25.134  0.0.0.0   0      0
        14 en   230.1.1.20      0.0.0.0   0      0

```

The following example illustrates detailed information about a given tunnel:

```

Router#show cab dsg tunnel 1 verbose
Tunnel ID                : 1
State                    : enable
MAC Addr                 : 0100.5e01.0114

Cfr Id                  : 1
State                   : enable
Priority                 : 0
Dest IP                 : 230.1.1.20
Src IP                  : 0.0.0.0
Src Prefix Length       : 32
Dest Port Start         : 0
Dest Port End           : 65535
Forwarded               : 0
Received               : 0

Cfr Id                  : 11
State                   : enable
Priority                 : 0
Dest IP                 : 224.25.25.134
Src IP                  : 0.0.0.0
Src Prefix Length       : 32
Dest Port Start         : 0
Dest Port End           : 65535
Forwarded               : 0
Received               : 0

Cfr Id                  : 14
State                   : enable
Priority                 : 0
Dest IP                 : 230.1.1.20
Src IP                  : 0.0.0.0
Src Prefix Length       : 32
Dest Port Start         : 1000
Dest Port End           : 2000
Forwarded               : 0
Received               : 0

Client List Id          : 2
Client Id               : 1
Client Id Type          : CA System ID: 0951
Client Id               : 3
Client Id Type          : Broadcast
Client Id               : 8
Client Id Type          : MAC Addr: 1111.1111.1111

Client List Id          : 10
Client Id               : 1
Client Id Type          : Application ID: 0001

Interface               : Cable5/0
Rule Id                 : 1
Rule Id                 : 7
Rule Id                 : 8
Rule Id                 : 20
Interface               : Cable5/1
Rule Id                 : 7
Rule Id                 : 8

```

A-DSG 1.1 Cable Interface Configuration Examples

The following examples illustrate cable interface configurations with the Advanced-mode 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.

The following sample configuration requires IP PIM sparse mode for the Gigabit Ethernet interface:

```
...
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 sparse-mode
 ip igmp static-group 239.0.0.2
 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.

The following example illustrates syntax options for the **show interface cable dsg downstream** command for the specified interface:

```
Router# sh int c6/0 dsg downstream ?
dcd      Show DSG downstream dcd message
rule     Show DSG downstream rule
tunnel   Show DSG downstream tunnel
|        Output modifiers

```

The following example illustrates A-DSG 1.1 downstream configuration information and the number of tunnels, classifiers, clients and vender-specific parameters:

```
Router# show interfaces c5/0 dsg downstream
chan chFreq chan timer init oper twoWay oneWay num num num num num
list index freq index timeout timeout timer timer rule tunnel cfr client vsp
12 1 930 12 2 900 300 750 9 6 4 6 1
2 990
3 105

```

The following example illustrates DCD statistics for the given downstream interface. DCD TLV displays if the **debug cable dsg** command is enabled:

```
Router# show interfaces c5/0 dsg downstream dcd
dcd dcd num of dcd num of dcd num of dcd num of
state Tx sent fail change cnt fragment
en on 797148 0 28 1
```

```
Router# debug cable dsg
CMTS DSG debugging is on
Router# show interfaces c5/0 dsg downstream dcd
dcd dcd num of dcd num of dcd num of dcd num of
state Tx sent fail change cnt fragment
en on 797163 0 28 1
```

```
Router#
lw3d: DCD TLV last sent:
32290101 01020102 040E0302 09510100 02061111 11111111 05060100 5E010114
06020001 2B050803 00001117 0F020200 01050100 09060504 E6010114 32260101
02020100 040E0302 09510100 02061111 11111111 05060100 5E010115 06020002
0602000A 170F0202 00020501 00090605 04E60101 15170F02 02000A05 01000906
0504E601 010A321C 01010302 01000408 02063333 33333333 05060100 5E010128
06020003 170F0202 00030501 00090605 04E60101 28322901 01140201 00040E03
02095101 00020611 11111111 11050601 005E0101 14060200 012B0508 03000011
33290104 058B1140 010405E6 9EC00104 06422C40 02020002 03020384 0402012C
050202EE 2B050803 000011
```

The following example illustrates A-DSG 1.1 rule state, tunnels, classifiers, client information, upstream channel ID and the number of vendors associated to a DSG rule on a given downstream interface:

```
Router# show interfaces c5/0 dsg downstream rule
rule rule rule tunnel tunnel tunnel cfr cfr cfrIn client vsp
id state pri id state mac-addr id state rule listId index
1 en 2 1 en 0100.5e01.0114 1 en yes 2 1
11 en no
14 en no
2 en 0 2 en 0100.5e01.0115 2 en yes 2
10 en yes
3 en 0 3 en 0100.5e01.0128 3 en yes 3
4 dis 0 4 en 0100.5e01.0133 4 en no 4
5 dis 0 5 en 0100.5e01.013c 5 en no 5
9 en no
6 dis 0 6 dis 0100.5e01.0146 6 en no 6
7 dis 0 1 en 0100.5e01.0114 1 en no 10
11 en no
14 en no
8 dis 0 1 en 0100.5e01.0114 1 en no 2
11 en no
14 en no
20 en 0 1 en 0100.5e01.0114 1 en yes 2 1
11 en no
14 en no
```

The following example illustrates the same information as above for the given DSG rule:

```
Router# show interfaces c5/0 dsg downstream rule 1
rule rule rule tunnel tunnel tunnel cfr cfr cfrIn client vsp
id state pri id state mac-addr id state rule listId index
1 en 2 1 en 0100.5e01.0114 1 en yes 2 1
11 en no
```

The following example illustrates syntax options for the **show interface cable dsg downstream rule** command for the specified interface:

```
Router# sh int c6/0 dsg downstream rule 1 ?
  cfr      Show DSG downstream rule classifiers
  clients  Show DSG downstream rule clients
  verbose  Show DSG downstream rule detail information
  |
  Output modifiers
```

The following example illustrates the list of classifiers associated to the DSG rule:

```
Router# show interfaces c5/0 dsg downstream rule 1 cfr
rule cfr  cfr  cfrIn cfr destination ip  source ip      srcPre d_port  d_port
id  id   state rule  pri  address          address          length start  end
1   1    en   yes  0   230.1.1.20      0.0.0.0         32     0     65535
    11   en   no   0   224.25.25.134  0.0.0.0         32     0     65535
    14   en   no   0   230.1.1.20      0.0.0.0         32    1000  2000
```

The following example illustrates the list of clients associated to the DSG rule:

```
Router# show interfaces c5/0 dsg downstream rule 1 clients
rule rule client client client
id  state pri  listId id  id type      address
1   en   2   2     1   CA System ID  0x0951
                   3   Broadcast
                   8   MAC Addr      1111.1111.111
```

The following example illustrates detailed information about the DSG rule:

```
Router# show interfaces c5/0 dsg downstream rule 1 verbose
Rule ID          : 1
State           : enable
Priority        : 2

Tunnel ID       : 1
State          : enable
MAC Addr       : 0100.5e01.0114

Cfr Id         : 1
State         : enable
Priority      : 0
Dest IP      : 230.1.1.20
Src IP       : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End   : 65535

Cfr Id         : 11
State         : enable
Priority      : 0
Dest IP      : 224.25.25.134
Src IP       : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End   : 65535

Cfr Id         : 14
State         : enable
Priority      : 0
Dest IP      : 230.1.1.20
Src IP       : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 1000
Dest Port End   : 2000
```

```

Client List Id          : 2
Client Id              : 1
Client Id Type         : CA System ID    0x0951
Client Id              : 3
Client Id Type         : Broadcast
Client Id              : 8
Client Id Type         : MAC Addr       1111.1111.1111

vsif index             : 1
vsif oui               : 0X11
vsif value             : 0X

```

The following example illustrates the DSG tunnel information associated with the downstream interface:

```

Router# show interfaces c5/0 dsg downstream tunnel
tunnel tunnel tunnel      cfr  cfr  rule rule  client service
id      state mac-addr      id  state id  state listId class
1       en    0100.5e01.0114  1   en   1   en   2
          11   en   7   dis  10
          14   en   8   dis  2
          20   en   2
2       en    0100.5e01.0115  2   en   2   en   2
          10   en
3       en    0100.5e01.0128  3   en   3   en   3
4       en    0100.5e01.0133  4   en   4   dis  4
5       en    0100.5e01.013c  5   en   5   dis  5
          9    en
6       dis   0100.5e01.0146  6   en   6   dis  6

```

The following example illustrates DSG tunnel information associated with the downstream interface:

```

Router#show interfaces c5/0 dsg downstream tunnel 1
tunnel tunnel tunnel      cfr  cfr  rule rule  client service
id      state mac-addr      id  state id  state listId class
1       en    0100.5e01.0114  1   en   1   en   2
          11   en   7   dis  10
          14   en   8   dis  2
          20   en   2

```

A-DSG 1.Subinterface Configuration Example

The following example illustrates a more complex configuration with 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 sparse-mode
ip helper-address 1.8.35.200
cable downstream annex B
cable downstream modulation 256gam
cable downstream interleave-depth 32
cable downstream channel-id 0
cable downstream rf-shutdown
cable upstream 0 frequency 33008000
cable upstream 0 power-level 0
cable upstream 0 channel-width 1600000
cable upstream 0 minislot-size 4
cable upstream 0 modulation-profile 1
no cable upstream 0 shutdown
cable upstream 1 channel-width 1600000
cable upstream 1 minislot-size 4
cable upstream 1 modulation-profile 1
cable upstream 1 shutdown
cable upstream 2 channel-width 1600000
cable upstream 2 minislot-size 4
cable upstream 2 modulation-profile 1
cable upstream 2 shutdown
cable upstream 3 channel-width 1600000
cable upstream 3 minislot-size 4
cable upstream 3 modulation-profile 1
cable upstream 3 shutdown
!
interface Cable1/0.1
ip igmp static-group 224.11.11.1
ip igmp static-group 224.12.12.1
ip igmp static-group 224.3.3.2
ip igmp static-group 224.3.3.3
ip igmp static-group 224.3.3.6
ip igmp static-group 224.3.3.7
ip igmp static-group 224.3.3.8
ip igmp static-group 224.3.3.9
ip igmp static-group 224.3.3.18
ip igmp static-group 224.3.3.19
ip igmp static-group 224.3.3.20
ip igmp static-group 224.3.3.21
ip igmp static-group 224.3.3.22
ip igmp static-group 224.3.3.93
ip igmp static-group 224.3.3.97
ip igmp static-group 224.3.3.95
ip igmp static-group 224.3.3.98
ip igmp static-group 224.5.5.8
ip igmp static-group 224.5.5.10
ip igmp static-group 224.3.4.12
ip igmp static-group 224.3.3.25
ip igmp static-group 224.4.4.1
ip igmp static-group 224.5.5.5
ip igmp static-group 224.5.5.11
ip igmp static-group 224.5.5.12
ip igmp static-group 224.5.5.13
ip igmp static-group 224.5.5.14
ip igmp static-group 224.5.5.15
ip igmp static-group 224.5.5.16
ip igmp static-group 224.6.6.7
ip igmp static-group 224.6.6.9
ip igmp static-group 224.6.6.10
ip igmp static-group 224.6.6.11
ip igmp static-group 224.7.7.1
ip igmp static-group 224.8.8.1
ip igmp static-group 224.8.8.2
ip igmp static-group 224.8.8.10

```

```

ip igmp static-group 224.9.9.1
cable dsg 0009.0009.0009 224.12.12.1 science
cable dsg 0010.0010.0010 224.11.11.1 science
cable dsg 0001.0001.0001 224.3.3.97 cisco
cable dsg 0001.0001.0001 224.3.3.98 cisco
cable dsg 0001.0001.0001 224.3.3.93 cisco
cable dsg 0001.0001.0001 224.3.3.95 cisco
cable dsg 0006.0006.0006 224.9.9.1 microso
cable dsg 0005.0005.0005 224.8.8.1 ibm
cable dsg 0001.0001.0001 224.7.7.1 cisco
cable dsg 0001.0001.0002 224.4.4.1 cisco
cable dsg 0005.0005.0005 224.8.8.2 ibm
cable dsg 0001.0001.0001 224.3.3.2 cisco
cable dsg 0001.0001.0001 224.3.3.3 cisco
cable dsg 1234.1234.1234 224.5.5.5 cisco
cable dsg 0001.0001.0001 224.3.3.6 cisco
cable dsg 0001.0001.0001 224.3.3.7 cisco
cable dsg 00dd.0001.0001 224.6.6.7 cisco
cable dsg 0001.0001.0001 224.3.3.8 cisco
cable dsg 0001.0001.0001 224.5.5.8 cisco
cable dsg 0001.0001.0001 224.3.3.9 cisco
cable dsg 10dd.0001.0001 224.6.6.9 ibm
cable dsg 0000.0000.0000 224.8.8.10 science
cable dsg 0001.0001.0001 224.5.5.10 cisco
cable dsg 10dd.0002.0002 224.6.6.10 ibm
cable dsg 0001.0001.0001 224.3.4.12 cisco
cable dsg 0003.0001.0001 224.5.5.11 cisco
cable dsg 0000.0000.0001 224.6.6.11 ibm
cable dsg 0033.0001.0001 224.5.5.12 cisco
cable dsg 00cc.0001.0001 224.5.5.13 cisco
cable dsg 00cc.0001.0001 224.5.5.14 cisco
cable dsg 00cd.0001.0001 224.5.5.15 cisco
cable dsg 00dd.0001.0001 224.5.5.16 cisco
cable dsg 0001.0001.0001 224.3.3.18 cisco
cable dsg 0001.0001.0001 224.3.3.19 cisco
cable dsg 0001.0001.0001 224.3.3.20 cisco
cable dsg 0001.0001.0001 224.3.3.21 cisco
cable dsg 0001.0001.0001 224.3.3.22 cisco
cable dsg 0001.0001.0001 224.3.3.25 cisco
!
interface Cable1/0.2
ip igmp static-group 224.11.11.2
ip igmp static-group 224.13.13.1
cable dsg 0009.0009.0009 224.13.13.1 science
cable dsg 0011.0011.0011 224.11.11.2 science
!
interface Ethernet3/0
ip address 10.0.0.2 255.0.0.0
ip pim sparse-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 illustrates 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 sparse-mode
ip igmp static-group 239.0.0.2
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 minislots-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 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
 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-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



Note

Rate-limit is not supported in Cisco IOS Release 12.2(33)SCC and later releases.

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

```

■ Configuration Examples for Advanced-mode DOCSIS Set-Top Gateway

```
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 Advanced-mode 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/en/US/docs/ios/cable/command/reference/cbl_book.html
Cisco IOS Release 12.2 Command Reference	Cisco IOS Release 12.2 configuration guides and command references, on Cisco.com: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.html
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/en/US/docs/cable/cmts/feature/guide/ufg_docs.html
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/en/US/docs/ios/12_2/ip/configuration/guide/1cfip.html
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/en/US/docs/ios/12_2/ipaddr/command/reference/fipras_r.html
IP Multicast Configuration Guide	<i>Cisco IOS IP Configuration Guide</i> , Release 12.3 on Cisco.com: http://www.cisco.com/en/US/docs/ios/12_3/featlist/ip_vcg.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/en/US/docs/ios/12_2/ipmulti/command/reference/fiprnc_r.html

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, version 1.1</i>
SP-DSG-I01-020228	CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification

1. Not all supported standards are listed.

MIBs

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

1. Not all supported MIBs are listed.

RFCs

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

1. Not all supported RFCs are listed.

Technical Assistance

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

System Messages

Cisco IOS Release 12.3(13a)BC System Messages

This section describes system messages that support the Advanced-mode DSG 1.1 feature. These include debugging, DCD messages, DSG tunnels, IP Multicast messages, and several additional functions of A-DSG 1.1.

Debug System Messages

```
%DSG: a mapping entry created for 0001.0002.0003 235.5.5.5 on Cable5/1
```

```
%DSG: a mapping entry has been added on the interface Cable5/1
```

Explanation A DSG mapping entry is created for the interface and MAC address indicated.

Recommended Action No action is required.

```
%DSG: remove and free tunnel 0001.0002.0003
```

Explanation A DSG tunnel entry has been removed for the interface indicated.

Recommended Action No action is required.

```
%DSG: vendor entry BBB is freed
```

Explanation Vendor entry is removed

Recommended Action No action is required.

```
%DSG: a mapping entry freed for 235.5.5.5 0001.0002.0003 Cable5/1
```

```
%DSG: the specified DSG entry has been removed
```

Explanation DSG mapping is removed.

Recommended Action No action is required.

```
%DSG: cmts_dsg_resolve_mac 225.2.2.2 on Cable5/0
```

```
%DSG: cmts_dsg_resolve_mac is successful
```

Explanation CMTS is resolving a MAC address from DSG table.

Recommended Action No action is required.

```
%DSG: cmts_dsg_group2mac on Cable5/1
```

```
%DSG: cmts_dsg_group2mac 0001.0002.0003 is successful
```

Explanation CMTS is finding mac address for a group from DSG table.

Recommended Action No action is required.

%DSG: cmts_dsg_mac2group

%DSG: cmts_dsg_mac2group is successful

Explanation CMTS is finding group address for a mac address from DSG table.

Recommended Action No action is required.

%DSG: unexpected event for CMTS DSG process

Explanation When an unexpected event is sent to DSG keepalive process

Recommended Action No action is required.

%DSG: interface Cable5/0 joined the igmp static group 229.2.2.2.

Explanation If DSG entry is added

Recommended Action No action is required.

%DSG: interface Cable5/1 left the igmp static group 225.2.2.2.

Explanation Removed the entry successfully

Recommended Action No action is required.

%DSG: all tunnels have been removed on interface Cable5/1 and its subinterfaces.

Explanation If no more dsg entry on a hardware interface

Explanation No action is required.

%DSG: All DSG tunnels are removed on interface cable 5/1 and its subinterfaces.

Explanation An operator has removed a subinterface and all mapping entries on a physical interface.

Recommended Action No action is required.

Command Reference for Advanced-mode DSG Issue 1.1

This section describes the following new Cisco IOS commands that configure, monitor and troubleshoot the Advanced-mode Advanced-mode DOCSIS Set-Top Gateway (A-DSG) feature through Issue 1.1. These commands are supported in Cisco IOS Release 12.3(13a)BC and later releases in the 12.3BC release train.

Global Configuration Commands for A-DSG 1.1

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

- A-DSG clients
- A-DSG 1.1 tunnels
- 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 following global configuration commands are used with A-DSG 1.1 on the Cisco CMTS:

- [cable dsg cfr](#)
- [cable dsg chan-list](#)
- [cable dsg client-list](#)
- [cable dsg timer](#)
- [cable dsg vendor param](#)
- [cable dsg tunnel](#)
- [cable igmp static-group](#)

Interface Configuration Commands for A-DSG 1.1

A-DSG 1.1 indexes that are defined in global configuration mode are subsequently used in the following interface configurations and commands. These interface commands define the DSG rules, tunnel traffic, and parameters to include in the DCD message.

- [cable downstream dsg chan-list](#)
- [cable downstream dsg dcd-enable](#)
- [cable downstream dsg rule](#)
- [cable downstream dsg timer](#)
- [cable downstream dsg vendor-param](#)
- [ip igmp static-group](#)

Debug Commands for A-DSG 1.1

- [debug cable dsg](#)

Show Commands for A-DSG 1.1

- [show cable dsg tunnel](#)
- [show interface cable dsg downstream](#)

**Tip**

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

http://www.cisco.com/en/US/docs/ios/cable/command/reference/cbl_book.html

All other commands used with this feature are documented in the Cisco IOS Release 12.2 and 12.3 Mainline command reference publications.

cable dsg cfr

To define and enable A-DSG 1.1 classifiers on the Cisco CMTS, use the **cable dsg cfr** command in global configuration mode. 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.

```

cable dsg <cfr index> dest-ip <ipaddr>
    [tunnel <tunnel index>] |
    [dest-ports <start> <end>] |
    [priority <priority>] |
    [src-ip <ipaddr>] | src-prefix-len
    [enable | disable]
no cable dsg cfr <cfr index>
  
```

Syntax Description		
cfr index		Creates the DSG index, with index identifier.
dest-ip <ipaddr>		Defines the destination IP address.
tunnel <tunnel index>		Defines the tunnel index.
dest-port <start> <end>		Defines the destination TCP/UDP ports range.
priority <priority>		Defines the classifier priority.
src-ip <ipaddr>] src-prefix-len		Defines the source IP address and prefix length, if desired. src-prefix-len is optional.
enable		Enables this classifier.
disable		Disables this classifier.

Defaults A-DSG 1.1 classifiers are undefined by default on the Cisco CMTS, and remain disabled by default once configured until they are enabled with the **enable** keyword.

Command Modes Global configuration mode

Command History	Release	Modification
	12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines A-DSG 1.1 classifiers can only be mapped to one DSG tunnel, but multiple classifiers can be mapped to one tunnel. The Cisco CMTS router applies the classifier parameters to the packets received from the DSG server in order to assign the packet to the appropriate DSG tunnel. The classifiers are also associated to the DSG rule to encode in the DCD message.

Examples

The following example illustrates A-DSG 1.1 CFR global configurations on the Cisco CMTS:

```
cable dsg cfr 1 dest-ip 224.10.10.101 tunnel 1 dest-port 0 65535 priority 1
cable dsg cfr 2 dest-ip 224.10.10.102 tunnel 2 dest-port 0 65535 priority 1
cable dsg cfr 3 dest-ip 224.10.10.103 tunnel 3 dest-port 0 65535 priority 1
cable dsg cfr 4 dest-ip 224.10.10.104 tunnel 4 dest-port 0 65535 priority 1
cable dsg cfr 5 dest-ip 224.10.10.105 tunnel 1 dest-port 0 65535 priority 1
cable dsg cfr 6 dest-ip 224.10.10.106 tunnel 2 dest-port 0 65535 priority 1
```

Related Commands

Command	Description
cable dsg chan-list	Configures the A-DSG 1.1 downstream channel list.
cable dsg client-list	Configures the A-DSG 1.1 client parameters and the associated DSG rule.
cable dsg timer	Configures the A-DSG 1.1 timer.
cable dsg vendor param	Configures vendor-specific parameters for A-DSG 1.1.
cable dsg tunnel	Creates A-DSG 1.1 tunnels, with entry mapped to a destination MAC address.

cable dsg chan-list

To configure the A-DSG 1.1 downstream channel list, use the **cable dsg chan-list** command in global configuration mode. To remove the A-DSG 1.1 channel list from the Cisco CMTS, use the **no** form of this command.

```
cable dsg chan-list <list-index> index <entry-index> freq <freq>
```

```
no cable dsg chan-list <list-index> index <entry-index> freq <freq>
```

Syntax Description

chan-list <i>list-index</i>	Defines the DSG channel list and index identifier.
index <i>entry-index</i>	Defines the DSG channel frequency entry index.
freq <i>freq</i>	Defines the center frequency of the downstream channel in Hz.

Defaults

A-DSG 12.1 channel lists are disabled and undefined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

The channel list entry created with this command can be associated to the downstream to be included in the DSG message.

Examples

The following example illustrates A-DSG 1.1 channel list global configurations on the Cisco CMTS:

```
cable dsg chan-list 1 index 1 freq 47000000
cable dsg chan-list 1 index 2 freq 125000000
cable dsg chan-list 1 index 3 freq 555000000
cable dsg chan-list 2 index 1 freq 47000000
cable dsg chan-list 2 index 2 freq 125000000
cable dsg chan-list 2 index 3 freq 555000000
```

Related Commands

Command	Description
cable dsg cfr	Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS.
cable dsg client-list	Configures the A-DSG 1.1 client parameters and the associated DSG rule.
cable dsg timer	Configures the A-DSG 1.1 timer.
cable dsg vendor param	Configures vendor-specific parameters for A-DSG 1.1.
cable dsg tunnel	Creates A-DSG 1.1 tunnels, with entry mapped to a destination MAC address.

cable dsg client-list

To configure client parameters for Advanced-mode DSG (A-DSG 1.1), use the **cable dsg client-list** command in global configuration mode. This command configures the client parameters and the associated DSG rule. To remove this configuration, use the **no** form of the command.

```
cable dsg client-list <client-list-id> id-index <id> {application-id | ca-system-id | mac-addr | broadcast} <value>
```

```
no cable dsg client-list <client-list-id> id-index <id> {application-id | ca-system-id | mac-addr | broadcast} <value>
```

Syntax Description

client-list <client-list-id>	Defines and names the DSG client list.
id-index <id>	Defines the DSG client index identifier.
application-id <value>	Defines the DSG client type application identifier.
broadcast <value>	Defines the DSG client type broadcast value.
ca-system-id <value>	Defines the DSG client type CA system identifier.
mac-addr <value>	Defines the DSG client type MAC address.

Defaults

Client lists for A-DSG are not configured by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

The same DSG client identifier may be used by multiple DSG rules.

Examples

The following sample configuration illustrates global parameters for four A-DSG 1.1 client lists:

```
cable dsg client-list 1 id-index 1 broadcast
cable dsg client-list 2 id-index 2 application-id FFFF
cable dsg client-list 3 id-index 3 ca-system-id EEEE
cable dsg client-list 4 id-index 4 mac-addr 0100.5e0a.0a04
```

Related Commands

Command	Description
cable dsg cfr	Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS.
cable dsg chan-list	Configures the A-DSG 1.1 downstream channel list.
cable dsg timer	Configures the A-DSG 1.1 timer.
cable dsg vendor param	Configures vendor-specific parameters for A-DSG 1.1.
cable dsg tunnel	Creates A-DSG 1.1 tunnels, with entry mapped to a destination MAC address.

cable dsg timer

To configure the A-DSG 1.1 timer entry to be associated to the downstream channel, and encoded into the DCD message, use the **cable dsg timer** command in global configuration mode. To remove the cable dsg timer from the Cisco CMTS, use the **no** form of this command.

```
cable dsg timer <index> [Tdsg1 <Tdsg1>] | [Tdsg2 <Tdsg2>] | [Tdsg3 <Tdsg3>] | [Tdsg4 <Tdsg4>]
```

```
no cable dsg timer <index> [Tdsg1 <Tdsg1>] | [Tdsg2 <Tdsg2>] | [Tdsg3 <Tdsg3>] | [Tdsg4 <Tdsg4>]
```

Syntax Description

timer <i>index</i>	Defines the DSG timer and associates to the index for the downstream channel.
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.

Defaults

The A-DSG 1.1 timer is not defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

The A-DSG 1.1 timer entry can associated to the downstream to encode into the DCD message.

Examples

The following sample configuration illustrates global parameters for three A-DSG 1.1 timers:

```
cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4
cable dsg timer 2 Tdsg1 2 Tdsg2 22 Tdsg3 33 Tdsg4 44
cable dsg timer 3 Tdsg1 2 Tdsg2 600 Tdsg3 300 Tdsg4 1800
```

Related Commands

Command	Description
cable dsg cfr	Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS.
cable dsg chan-list	Configures the A-DSG 1.1 downstream channel list.
cable dsg client-list	Configures the A-DSG 1.1 client parameters and the associated DSG rule.
cable dsg vendor param	Configures vendor-specific parameters for A-DSG 1.1.
cable dsg tunnel	Creates A-DSG 1.1 tunnels, with entry mapped to a destination MAC address.

cable dsg vendor param

To configure vendor-specific parameters for A-DSG 1.1, use the **cable dsg vendor-param** command in global configuration mode. To remove this configuration from the Cisco CMTS, use the **no** form of this command.

```
cable dsg vendor-param <group-id> vendor <vendor-index> oui <oui> value <value-in-TLV>
no cable dsg vendor-param <group-id> vendor <vendor-index> oui <oui> value <value-in-TLV>
```

Syntax Description

vendor-param <group-id>	Defines the DSG vendor parameter and associates with a DSG group.
vendor <vendor-index>	Selects the DSG vendor and associated DSG index.
oui <oui>	Selects the DSG OUI setting.
value <value-in-TLV>	Sets the type/length value for the defined DSG vendor.

Defaults

The A-DSG 1.1 vendor is not defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

The vendor-specific parameters can be associated to the downstream to encode into the DCD message.

Examples

The following sample configuration illustrates global vendor parameters for A-DSG 1.1:

```
cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB
cable dsg vendor-param 2 vendor 1 oui ABCDEB value 0101AB
cable dsg vendor-param 3 vendor 1 oui ABCDEC value 0101AB
```

Related Commands

Command	Description
cable dsg cfr	Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS.
cable dsg chan-list	Configures the A-DSG 1.1 downstream channel list.
cable dsg client-list	Configures the A-DSG 1.1 client parameters and the associated DSG rule.
cable dsg timer	Configures the A-DSG 1.1 timer.
cable dsg tunnel	Creates A-DSG 1.1 tunnels, with entry mapped to a destination MAC address.

cable dsg tunnel

To create A-DSG 1.1 tunnels, use the **cable dsg tunnel** command in global configuration mode. 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.

```
cable dsg tunnel <tunnel-id> mac_addr <mac addr> | [enable | disable]
```

```
no cable dsg tunnel <tunnel-id> mac_addr <mac addr> [srv-class <service-class-name>] |
```

Syntax Description

tunnel <tunnel-id>	Defines the DSG tunnel, and names with alphanumeric string to identify the DSG tunnel in related show and configuration commands.
mac_addr <mac-addr>	(Required) Sets the destination MAC address.
enable	Enables the specified A-DSG tunnel.
disable	Disables the specified A-DSG tunnel.

Defaults

A-DSG 1.1 tunnels are not configured by default, and are disabled by default when configured.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Each tunnel is mapped to the destination MAC address and is associated with the QoS service class name.

Examples

The following sample configuration illustrates A-DSG 1.1 tunnels on the Cisco CMTS:

```
cable dsg tunnel 1 mac-addr 0100.5e0a.0a01
cable dsg tunnel 2 mac-addr 0100.5e0a.0a02
cable dsg tunnel 3 mac-addr 0100.5e0a.0a03
cable dsg tunnel 4 mac-addr 0100.5e0a.0a04
```

Related Commands

Command	Description
cable dsg cfr	Defines and enables A-DSG 1.1 classifiers on the Cisco CMTS.
cable dsg chan-list	Configures the A-DSG 1.1 downstream channel list.
cable dsg client-list	Configures the A-DSG 1.1 client parameters and the associated DSG rule.
cable dsg timer	Configures the A-DSG 1.1 timer.
cable dsg vendor param	Configures vendor-specific parameters for A-DSG 1.1.

cable igmp static-group

To configure Cable per physical downstream Static Multicast support on the Cisco CMTS, use the **cable igmp static-group** command in global configuration mode.

```
cable igmp static-group [multicast group] source [source IP] [subinterface number]
```

Syntax Description

<i>multicast group</i>	Multicast IP address of the group.
Source [<i>source IP</i>]	(Optional) Source IP address for SSM.
<i>Subinterface number</i>	Subinterface number: <ul style="list-style-type: none"> • default: 0 for the main interface
Note If the subinterface is configured at the virtual bundle interface, the subinterface number option for this CLI must be configure to match up with the desired subinterface devices.	

Command Default

Cable per physical downstream Static Multicast support is not defined by default.

Command Modes

Global configuration mode

Command History

Release	Modification
12.3(21)BC	This command was introduced for the Cisco uBR10012 series routers.

Usage Guidelines

The Cable per physical downstream Static Multicast Support feature introduces the concept of a physical IGMP Static-Group, which is an extension of the existing logical IGMP Static-Group. The differences between the two IGMP Static-Group are as follows:

- A Cable Bundle Logical IGMP Static-Group creates the IGMP Static-Group for the logical IP domain and forwards multicast traffics for the configured multicast group to every Slave interfaces in the same bundle.
- A Cable Bundle Physical IGMP Static-Group creates the IGMP Static-Group on per-physical Slave interface basis and will only forwards multicast traffics to only configured Slave interfaces.

When an IGMP Static-Group is configured on a Master interface, the IGMP Static-Group will perform a check for each Slave interface in the multicast group. If the multicast group is configured as a Physical Static-Group, then only the corresponding Slave interfaces will be added to the Cable Bundle Forwarding Table. If the multicast group is configured as a Logical Static-Group, then all Slave interfaces will be added to the Cable Bundle Forwarding Table.



Note

When all remaining Physical Static-Groups are un-configured from the Slave interface for a particular multicast group on a particular bundle, the Cisco CMTS will revert back to the Logical Static-Group for that multicast group on that bundle.

DSG Usage

The **cable igmp static-group** command CLI will only be display at “show run” if it is configured via the CLI. If it is configured by DSG, the **cable igmp static-group** command CLI will remain hidden for a particular multicast group. This is done in order to eliminate any confusion with the current DSG configurations.

**Note**

Any Multicast group being used by DSG (or CLI) within the same CMTS, should not be used for CLI (or DSG) configuration.

Examples

The following sample configuration illustrates the **cable igmp static-group** command on the Cisco CMTS:

```
Router(config-if)# cable igmp static-group 230.1.1.1
```

The following sample configuration illustrates the **cable igmp static-group** command with the **source** option Cisco CMTS:

```
Router(config-if)# cable igmp static-group 232.1.1.1 source 10.1.1.1
```

Related Commands

Command	Description
ip igmp static-group	Configure static group membership entries on an interface.

cable downstream dsg chan-list

To associate the DSG channel list entry to a downstream channel, to be included in the DCD message, use the cable **downstream dsg chan-list** command in interface configuration mode. To remove this setting from the Cisco CMTS, use the **no** form of this command.

cable downstream dsg chan-list <list-index>

no cable downstream dsg chan-list <list-index>

Syntax Description

chan-list	Sets the downstream A-DSG 1.1 channel list.
<i>list-index</i>	Alphanumeric list index identifier.

Defaults

Channel lists are not defined by default.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Global configurations for A-DSG 1.1 must be complete before configuring interface definitions.

Examples

The following downstream interface settings illustrate A-DSG 1.1 configurations on the Cisco CMTS:

```
interface Cable6/0
 cable downstream dsg dcd-enable
 cable downstream dsg chan-list 2
 cable downstream dsg timer 3
 cable downstream dsg vendor-param 2
 cable downstream dsg rule 1 clients 1 tunnel 1
 cable downstream dsg rule 1 priority 1
 cable downstream dsg rule 1 vendor-param 1
 cable downstream dsg rule 1 classifiers 1 5
 cable downstream dsg rule 2 clients 2 tunnel 2
 cable downstream dsg rule 2 priority 1
```

Related Commands

Command	Description
cable downstream dsg dcd-enable	Enables or disables DCD messages to be sent on a downstream channel.
cable downstream dsg rule	Allows and associates DSG clients, vendor specific parameters, classifiers, DSG tunnel address, UCID range, and rule priority.
cable downstream dsg timer	Allows and associates DSG timers to a downstream, with entry to be included in the DCD message.
cable downstream dsg vendor-param	Allows and associates the DSG vendor parameters to a downstream, with entry to be included in the DCD message.

cable downstream dsg dcd-enable

To enable DCD messages to be sent on a downstream channel, use the **downstream dsg dcd-enable** command in interface configuration mode. This command is used when there are no enabled rules or tunnels for A-DSG on the Cisco CMTS. To disable DCD messages, use the **disable** form of this command.

```
cable downstream dsg [ dcd-enable | dcd-disable ]
```

Defaults

This setting (DCD messages) is not configured by default. Once the **dcd-disable** keyword is configured this command remains disabled even if a rule is configured.

Command Modes

Interface configuration

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Global configurations for A-DSG 1.1 must be complete before configuring interface definitions.

Examples

The following downstream interface settings illustrate A-DSG 1.1 configurations on the Cisco CMTS:

```
interface Cable6/0
  cable downstream dsg dcd-enable
  cable downstream dsg chan-list 2
  cable downstream dsg timer 3
  cable downstream dsg vendor-param 2
  cable downstream dsg rule 1 priority 1 clients 1 tunnel 1
  cable downstream dsg rule 1 vendor-param 1
  cable downstream dsg rule 1 classifiers 1 5
  cable downstream dsg rule 2 priority 1 clients 2 tunnel 2
```

Related Commands

Command	Description
cable downstream dsg chan-list	Associates a DSG channel list to a downstream channel.
cable downstream dsg rule	Allows and associates DSG clients, vendor specific parameters, classifiers, DSG tunnel address, UCID range, and rule priority.
cable downstream dsg timer	Allows and associates DSG timers to a downstream, with entry to be included in the DCD message.
cable downstream dsg vendor-param	Allows and associates the DSG vendor parameters to a downstream, with entry to be included in the DCD message.

cable downstream dsg rule

To define and associate an A-DSG rule to the downstream channel, use the **downstream dsg rule** command in interface configuration mode. To disable a current configuration, use the **disable** form of this command. This command has the following forms:

```

cable downstream dsg rule <rule-id> clients <clnt-list-id> tunnel <tun-id>
cable downstream dsg rule <rule-id> priority <priority>
cable downstream dsg rule <rule-id> vendor-param <vsif-grp-id>
cable downstream dsg rule <rule-id> ucid <ucid1> | [<ucid1> <ucid2>...<ucidn>]
cable downstream dsg rule <rule-id> cfr <cfr-index> [ <cfr-index>...]
cable downstream dsg rule <rule-id> disable

```

Rules are disabled by default when they are created, and rules must be enabled using the following command:

```

no cable downstream dsg rule <rule-id> disable

```

Syntax Description		
dsg rule <rule-id>		Sets the DSG rule to be associated with a downstream channel, and defines the DSG rule identifier. Additional parameters are set for the DSG rule with this command.
clients <clnt-list-id>		Sets the DSG clients and associates the clients with the channel list identifier for this DSG rule.
tunnel <tun-id>		Sets the DSG tunnel to be associated with this rule, and defines the DSG tunnel identifier.
priority <priority>		Sets the priority of the DSG rule.
vendor-param <vsif-grp-id>		Associates DSG vendor-specific parameters with the specified DSG rule.
ucid <ucid1> [<ucid1> <ucid2>...<ucidn>]		Sets the upstream channel identifier for the DSG rule.
cfr <cfr-index> [<cfr-index>...]		Sets the index for the CFR value associated with the DSG rule.
disable		DSG rule disable

Defaults This command is not configured by default.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Global configurations for A-DSG 1.1 must be complete before configuring interface definitions. This configuration allows association of DSG clients, vendor specific parameters, classifiers, DSG tunnel address, upstream channel identifier range, and rule priority. The downstream can be associated with more than one rule. All configured rules are included in the DCD message.

Examples

The following downstream interface settings illustrate A-DSG 1.1 configurations on the Cisco CMTS:

```
interface Cable6/0
  cable downstream dsg dcd-enable
  cable downstream dsg chan-list 2
  cable downstream dsg timer 3
  cable downstream dsg vendor-param 2
  cable downstream dsg rule 1 clients 1 tunnel 1
  cable downstream dsg rule 1 priority 1
  cable downstream dsg rule 1 vendor-param 1
  cable downstream dsg rule 1 classifiers 1 5
  cable downstream dsg rule 2 clients 2 tunnel 2
  cable downstream dsg rule 2 priority 1
```

Related Commands

Command	Description
cable downstream dsg chan-list	Associates a DSG channel list to a downstream channel.
cable downstream dsg dcd-enable	Enables or disables DCD messages to be sent on a downstream channel.
cable downstream dsg timer	Allows and associates DSG timers to a downstream, with entry to be included in the DCD message.
cable downstream dsg vendor-param	Allows and associates the DSG vendor parameters to a downstream, with entry to be included in the DCD message.

cable downstream dsg timer

To associate the DSG timers entry to a downstream channel, and to be included in the DCD message, use the *downstream dsg timer* command in interface configuration mode. To remove this setting, use the **no** form of this command.

cable downstream dsg timer <timer-index>

Syntax Description

<i>timer-index</i>	Identifier for the DSG timer setting in the index.
--------------------	--

Defaults

The downstream DSG timer is not configured or enabled by default.

Command Modes

Interface configuration mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Global configurations for A-DSG 1.1 must be complete before configuring interface definitions.

Examples

The following downstream interface settings illustrate A-DSG 1.1 configurations on the Cisco CMTS:

```
interface Cable6/0
 cable downstream dsg dcd-enable
 cable downstream dsg chan-list 2
 cable downstream dsg timer 3
 cable downstream dsg vendor-param 2
 cable downstream dsg rule 1 priority 1 clients 1 tunnel 1
 cable downstream dsg rule 1 vendor-param 1
 cable downstream dsg rule 1 classifiers 1 5
 cable downstream dsg rule 2 priority 1 clients 2 tunnel 2
```

Related Commands

Command	Description
cable downstream dsg chan-list	Associates a DSG channel list to a downstream channel.
cable downstream dsg dcd-enable	Enables or disables DCD messages to be sent on a downstream channel.
cable downstream dsg rule	Allows and associates DSG clients, vendor specific parameters, classifiers, DSG tunnel address, UCID range, and rule priority.
cable downstream dsg vendor-param	Allows and associates the DSG vendor parameters to a downstream, with entry to be included in the DCD message.

cable downstream dsg vendor-param

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.

```
cable downstream dsg vendor-param <vsif-grp-id>
```

Syntax Description	<i>vsif-grp-id</i>	Associates a vendor parameter with a group identifier.
---------------------------	--------------------	--

Defaults This command is not configured by default.

Command Modes Interface configuration mode

Command History	Release	Modification
	12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines Global configurations for A-DSG 1.1 must be complete before configuring interface definitions.

Examples The following downstream interface settings illustrate A-DSG 1.1 configurations on the Cisco CMTS:

```
interface Cable6/0
  cable downstream dsg dcd-enable
  cable downstream dsg chan-list 2
  cable downstream dsg timer 3
  cable downstream dsg vendor-param 2
  cable downstream dsg rule 1 priority 1 clients 1 tunnel 1
  cable downstream dsg rule 1 vendor-param 1
  cable downstream dsg rule 1 classifiers 1 5
  cable downstream dsg rule 2 priority 1 clients 2 tunnel 2
```

Related Commands	Command	Description
	cable downstream dsg chan-list	Associates a DSG channel list to a downstream channel.
	cable downstream dsg dcd-enable	Enables or disables DCD messages to be sent on a downstream channel.
	cable downstream dsg rule	Allows and associates DSG clients, vendor specific parameters, classifiers, DSG tunnel address, UCID range, and rule priority.
	cable downstream dsg timer	Allows and associates DSG timers to a downstream, with entry to be included in the DCD message.

ip igmp static-group

To configure static group membership entries on an interface, use the `ip igmp static-group` command in interface configuration mode. To delete static group membership entries, use the `no` form of this command.

```
ip igmp static-group [* | group-address [source {source-address | ssm-map}] | class-map class-map-name]
```

```
no ip igmp static-group [* | group-address [source {source-address | ssm-map}] | class-map class-map-name]
```

Syntax Description		
	*	Places the interface into all created multicast route (mroute) entries.
	<i>group-address</i>	IP multicast group address to configure as a static group member on the interface.
	source	(Optional) Statically forwards a (S, G) channel out of the interface.
	<i>source-address</i>	(Optional) IP address of a system where multicast data packets originate.
	ssm-map	(Optional) Configures Source Specific Multicast (SSM) mapping to be used on the interface to determine the source associated with this group. The resulting (S, G) channels are statically forwarded.
	class-map	<i>class-map-name</i> Attaches an Internet Group Management Protocol (IGMP) static group range class map to the interface.

Command Default No static group membership entries are configured on interfaces.

Command Modes Interface configuration.

Command History	Release	Modification
	11.2	This command was introduced.
	12.3(2)T	The ssm-map keyword was added.
	12.2(18)S	The ssm-map keyword was added.
	12.2(18)SXD3	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(27)SBC	This command was integrated into Cisco IOS Release 12.2(27)SBC.
	12.2(18)SXF	The class-map keyword and <i>class-map-name</i> argument were added.

Usage Guidelines

Use the **ip igmp static-group** command to configure static group membership entries on an interface. When you configure the **ip igmp static-group** command, packets to the group are fast-switched out the interface, provided that packets were received on the correct reverse path forwarding (RPF) interface. Once configured, static group membership entries are added to the IGMP cache and mroute table.

Configuring the **ip igmp static-group** command is unlike configuring the **ip igmp join-group** command, which allows the router to join the multicast group. This configuration of the **ip igmp static-group** command would cause the upstream routers to maintain the multicast routing table information for that group, which would ensure that all the paths to that multicast group are active.

If you configure the **ip igmp join-group** command for the same group address as the **ip igmp static-group** command, the **ip igmp join-group** command takes precedence, and the group behaves like a locally joined group.

Use the **ip igmp static-group** command with the **ssm-map** keyword to configure static traffic forwarding with SSM mapping on the last hop router. Static traffic forwarding can be used in conjunction with SSM mapping to statically forward SSM traffic for certain groups. When static traffic forwarding with SSM mapping is configured, the last hop router uses Domain Name System (DNS)-based SSM mapping to determine the sources associated with a group. The resulting (S, G) channels are then statically forwarded.

Use the **ip igmp static-group class-map** command with the **class-map** keyword and class-map-name argument to attach an IGMP static group class map to an interface. Once attached, all groups entries that are defined in the class map become static members on the interface and are added to the IGMP cache and to the mroute table.

Examples

The following example shows how to configure group address 239.100.100.101 on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.100.100.101
```

The following example shows how to configure group address 239.1.2.1 to use SSM mapping for statically forwarded groups on Ethernet interface 0:

```
interface ethernet 0
 ip igmp static-group 239.1.2.1 source ssm-map
```

The following example shows how to attach an IGMP static group range class map named static1 to GigabitEthernet interface 1/1:

```
interface GigabitEthernet1/1
 ip igmp static-group class-map static1
```

Related Commands

Command	Description
class-map type multicast-flow	Enters multicast-flows class-map configuration mode to create or modify IGMP static group class maps.
ip igmp join-group	Causes the router to join a multicast group.
ip igmp ssm-map enable	Enables SSM mapping for groups in a configured SSM range.
ip igmp ssm-map query dns	Configures DNS-based SSM mapping.
ip igmp ssm-map static	Enables static SSM mapping.
ip igmp static-group	Configure static group membership entries on an interface.
ip pim ssm	Defines the SSM range of IP multicast addresses.

debug cable dsg

To enable general, DCD or packet-related debugging for A-DSG 1.1 on the Cisco CMTS, use the **debug cable dsg** command in privileged EXEC mode. To disable A-DSG 1.1 debugging, use the **no** form of this command.

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

```
no debug cable dsg
```

Syntax Description

dcd	(Optional) Enables DCD related debugging. Can be combined with pkt .
pkt	(Optional) Enables packet related debugging. Can be combined with dcd .

Defaults

A-DSG 1.1 debugging is disabled by default.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Global configurations for A-DSG 1.1 must be complete before configuring interface definitions. Refer to examples for illustrative variations in using this command.

Examples

If using the **debug cable dsg dcd** command, it shows DCD counters. If the configuration is changed, the whole DCD message content is displayed, including the MAC header. This display is derived from running information. The following sample illustrates one example:

```
Router# debug cable dsg dcd
23:30:45: Constructing DCD for Cable4/1
23:30:45: Cable4/1 DCD change_count 9
23:30:45: Cable4/1 DCD datagram size 626, msg len 624, ehdr type_or_len 606,
tlv size 597
23:30:45: Cable4/1 84485 DCD msg sent, 9 change count increased, 0 fails

23:30:46: Constructing DCD for Cable4/1
23:30:46: Cable4/1 DCD change_count 9
23:30:46: Cable4/1 DCD datagramsize 626, msg len 624, ehdr type_or_len 606,
tlv size 597
23:30:46: Cable4/1 84486 DCD msg sent, 9 change count increased, 0 fails

23:31:27: DSG VSIF group id 1, vendor index 1, sense 1

23:31:27: vendor 1 value len 1

23:31:27: Cable4/1 DCD is config dirty.

23:30:47: DSG VSIF group id 1, vendor index 1, sense 1
```

```

23:30:47: vendor 1 value len 1
23:30:47: Cable4/1 DCD is config dirty.
23:30:47: Constructing DCD for Cable4/1
23:30:47: client list 1 tlv length 2, clnts_tlv_size 4
23:30:47: Rule 1 all cfr IDs tlv size 4
23:30:47: Rule 1 VSIF tlv size = 36
23:30:47: Encode Cable4/1 rule 1 with tunnel 1,tlv size 60
23:30:47: client list 2 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 2 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 2 with tunnel 2,tlv size 26
23:30:47: client list 3 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 3 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 3 with tunnel 3,tlv size 26
23:30:47: client list 4 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 4 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 4 with tunnel 4,tlv size 26
23:30:47: client list 5 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 5 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 5 with tunnel 5,tlv size 26
23:30:47: client list 6 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 6 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 6 with tunnel 6,tlv size 26
23:30:47: client list 7 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 7 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 7 with tunnel 7,tlv size 26
23:30:47: client list 8 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 8 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 8 with tunnel 8,tlv size 26
23:30:47: client list 9 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 9 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 9 with tunnel 9,tlv size 26
23:30:47: client list 10 tlv length 4, clnts_tlv_size 6
23:30:47: Rule 10 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 10 with tunnel 10,tlv size 26
23:30:47: client list 11 tlv length 8, clnts_tlv_size 10
23:30:47: Rule 11 all cfr IDs tlv size 4
23:30:47: Encode Cable4/1 rule 11 with tunnel 11,tlv size 30
23:30:47: Cable4/1 TLV size for all rules 324
23:30:47: Encode Cable4/1 cfr 1, tlv size 17
23:30:47: Encode Cable4/1 cfr 2, tlv size 17
23:30:47: Encode Cable4/1 cfr 3, tlv size 17
23:30:47: Encode Cable4/1 cfr 4, tlv size 17
23:30:47: Encode Cable4/1 cfr 5, tlv size 17
23:30:47: Encode Cable4/1 cfr 6, tlv size 17
23:30:47: Encode Cable4/1 cfr 7, tlv size 25
23:30:47: Encode Cable4/1 cfr 8, tlv size 17
23:30:47: Encode Cable4/1 cfr 9, tlv size 17
23:30:47: Encode Cable4/1 cfr 10, tlv size 17
23:30:47: Encode Cable4/1 cfr 11, tlv size 17
23:30:47: Cable4/1 DSG Addr Table tlv size = 519
23:30:47: Cable4/1 downstream VSIF tlv size = 36
23:30:47: Cable4/1 clnt cfg tlv size = 38
23:30:47: Cable4/1 DCD change_count 10
23:30:47: Cable4/1 DCD datagramsize 586, msg len 584, ehdr type_or_len 566,
tlv size 557
23:30:47: Cable4/1 DCD msg 0x62463F8C, size=586
C2000248 000001E0 2F000001 000C31F6 F4710236 00000303 20000A01 01323A01
01010201 01040201 00050601 005E0101 14060200 012B0608 03ABCABC AB2B1A08
03000DF9 0A043030 30310B0D 45363031 30313238 3A303532 32321801 01020201
01040403 02095105 0601005E 01011E06 02000232 18010103 02010104 04040200
01050601 005E0101 28060200 03321801 01040201 01040403 02070105 0601005E
01013206 02000432 18010105 02010104 04040200 02050601 005E0101 3C060200
05321801 01060201 01040403 02000605 0601005E 01014606 02000632 18010107
02010104 04040200 03050601 005E0101 50060200 07321801 01080201 01040404
02000405 0601005E 01011906 02000832 18010109 02010104 04040200 05050601
005E0101 33060200 09321801 010A0201 01040404 02000605 0601005E 01014706
02000A32 1C01010B 02010104 08020600 504D0000 01050600 504D0000 01060200
0B170F02 02000105 01010906 0504E601 0114170F 02020002 05010109 060504E6
01011E17 0F020200 03050101 09060504 E6010128 170F0202 00040501 01090605

```

■ debug cable dsg

```

04E60101 32170F02 02000505 01010906 0504E601 013C170F 02020006 05010109
060504E6 01014617 17020200 07050101 090E0504 E6010150 090203E8 0A021388
170F0202 00080501 01090605 04E60101 19170F02 02000905 01010906 0504E601

23:30:45: DSG VSIF group id 1, vendor index 1, sense 1

23:30:45: vendor 1 value len 1
0133170F 0202000A 05010109 060504E6 01014717 0F020200 0B050101 09060504
E0191986 33242B06 0803ABCA BCAB2B1A 0803000D F90A0430 3030310B 0D453630
31303132 383A3035 3232

23:30:47: Cable4/1 84487 DCD msg sent, 10 change count increased, 0 fails

23:30:48: Constructing DCD for Cable4/1
23:30:48: Cable4/1 DCD change_count 10
23:30:48: Cable4/1 DCD datagramsize 586, msg len 584, ehdr type_or_len 566,
tlv size 557
23:30:48: Cable4/1 84488 DCD msg sent, 10

```

Related Commands

Command	Description
show cable dsg tunnel	Displays information about Advanced-mode DSG 1.1 on the Cisco CMTS, to include tunnel MAC address, state, number of classifiers associated, and additional information.
show interface	Displays general interface information for the specified or all interfaces. Use also the show interface cable dsg downstream command.

show cable dsg tunnel

To display information about Advanced-mode DSG 1.1 on the Cisco CMTS, to include tunnel MAC address, state, number of classifiers associated, number of interfaces to which tunnel is associated, number clients associated, and the Qos service class name for all the configured tunnels, use the **show cable dsg tunnel** command in privileged EXEC mode.

```
show cable dsg tunnel <tunnel-id> [ cfr | clients | interfaces | statistics | verbose ]
```

Syntax Description		
	<i>tunnel-id</i>	(Optional) Alphanumeric identifier for a specified tunnel, as previously configured with the cable dsg tunnel command.
	cfr	Show DSG tunnel classifiers
	clients	Show DSG tunnel clients
	interfaces	Show DSG tunnel interfaces
	stats	Show DSG tunnel statistics
	verbose	Show DSG tunnel detail information

Defaults No default behaviors or values

Command Modes Privileged EXEC mode

Command History	Release	Modification
	12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines Global configurations for A-DSG 1.1 must be complete before configuring interface definitions. Refer to the following examples for illustrative usage guidelines.

Examples The following example displays CLI help for **show cable dsg tunnel** command syntax.

```
Router# show cable dsg tunnel 1 ?
cfr          Show DSG tunnel classifiers
clients      Show DSG tunnel clients
interfaces   Show DSG tunnel interfaces
statistics   Show DSG tunnel statistics
verbose      Show DSG tunnel detail information
|           Output modifiers
<cr>
```

■ **show cable dsg tunnel**

The following command displays all configured tunnels for Advanced-mode DSG 1.1 on the Cisco CMTS:

```
Router# show cable dsg tunnel

tunnel tunnel tunnel      cfr cfr  tunnel in  rule rule  client service
id      state mac-addr  id  state interface id  state listId class
1       en    0100.5e01.0114  1   en   Cable6/0  1   en   2     SI
                    5   en
                    11  en
                    14  en
                    Cable6/1  1   en   4
                    3   en   3
                    4   en   4
                    11  en   2
2       en    0100.5e01.011e  2   en   Cable6/0  2   en   2     NDS-CA
                    10  en
3       en    0100.5e01.0128  3   en   Cable6/0  3   en   3     NDS-APP
4       en    0100.5e01.0132  4   en   Cable6/0  4   en   4     MOTO-CA
5       en    0100.5e01.013c  9   en   Cable6/0  5   en   5     MOTO-APP
                    Cable6/1  5   en   5
6       dis   0100.5e01.0146  6   en   Cable6/0  6   en   6     SA-CA
                    Cable6/1  6   en   6
7       dis   0100.5e01.0150  7   en   Cable6/1  8   en   7     SA-APP
                    13  dis
8       en    0100.5e01.0119  8   en
9       en    0100.5e01.0133
10      en    0100.5e01.0147
11      en    2222.2222.2222
12      en    3333.3333.3333  12  en
```

The following example displays the same information as above but for the specified tunnel.

```
Router# show cable dsg tunnel 1

tunnel tunnel tunnel      cfr cfr  tunnel in  rule rule  client service
id      state mac-addr  id  state interface id  state listId class
1       en    0100.5e01.0114  1   en   Cable6/0  1   en   2     SI
                    5   en
                    11  en
                    14  en
                    Cable6/1  1   en   4
                    3   en   3
                    4   en   4
                    11  en   2
```

The following example displays detailed information about all the classifiers associated with the specified tunnel.

```
Router# show cable dsg tunnel 1 cfr

tunnel cfr  cfr  cfr destination ip      source ip      srcPre d_port d_port
id      id  state pri address             address        length start end
1       1   en   1   230.1.1.20          0.0.0.0        32     0     65535
        5   en   1   230.1.1.60          0.0.0.0        32     0     65535
        11  en   1   224.25.25.134      0.0.0.0        32     0     65535
        14  en   0   230.1.1.20          0.0.0.0        32     1000 2000
```

The following example displays detailed information about all the clients associated with the specified tunnels.

```
Router# show cable dsg tunnel 1 clients

tunnel client client client      client
id      listId id    id type      address
1       2     1     CA System ID 0X951
        3     Broadcast
        8     MAC Addr     1111.1111.1111
        3     1     Application ID 0X1
        4     1     CA System ID 0X701
        10    1     Application ID 0X6
```

The following example displays all the interfaces and rules associated with the specified tunnel.

```
Router# sh cab dsg tunnel 1 interfaces
tunnel downstream rule
id interface id
1 Cable6/0 1 7 8 20
Cable6/1 1 3 4 11
```

The following example displays the packets statistics information about the specified tunnel.

```
Router# sh cab dsg tunnel 1 statistics
tunnel cfr cfr destination ip source ip total total
id id state address address forwarded received
1 1 en 230.1.1.20 0.0.0.0 0 0
5 en 230.1.1.60 0.0.0.0 0 0
11 en 224.25.25.134 0.0.0.0 0 0
14 en 230.1.1.20 0.0.0.0 0 0
```

The following example shows all the detailed information about the specified tunnel.

```
Router# sh cab dsg tunnel 1 verbose

Tunnel ID : 1
MAC Addr : 0100.5e01.0114
State : enable

Cfr Id : 1
State : enable
Priority : 1
Dest IP : 230.1.1.20
Src IP : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End : 65535
Forwarded : 0
Received : 0

Cfr Id : 5
State : enable
Priority : 1
Dest IP : 230.1.1.60
Src IP : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End : 65535
Forwarded : 0
Received : 0

Cfr Id : 11
State : enable
Priority : 1
Dest IP : 224.25.25.134
Src IP : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End : 65535
Forwarded : 0
Received : 0

Cfr Id : 14
State : enable
Priority : 0
Dest IP : 230.1.1.20
Src IP : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 1000
Dest Port End : 2000
Forwarded : 0
Received : 0

Client List Id : 2
Client Id : 1
```

■ show cable dsg tunnel

```

Client Id Type      : CA System ID: 0951
Client Id          : 3
Client Id Type     : Broadcast
Client Id          : 8
Client Id Type     : MAC Addr: 1111.1111.1111

Client List Id     : 3
Client Id          : 1
Client Id Type     : Application ID: 0001

Client List Id     : 4
Client Id          : 1
Client Id Type     : CA System ID: 0701

Client List Id     : 10
Client Id          : 1
Client Id Type     : Application ID: 0006

Interface          : Cable6/0
Rule Id            : 1
Rule Id            : 7
Rule Id            : 8
Rule Id            : 20
Interface          : Cable6/1
Rule Id            : 1
Rule Id            : 3
Rule Id            : 4
Rule Id            : 11

```

Related Commands

Command	Description
debug cable dsg	Enables general, DCD or packet-related debugging.
show interface	Displays general interface information for the specified or all interfaces. Use also the show interface cable dsg downstream command.

show interface cable dsg downstream

To display interface configuration and status information for Advanced-mode DSG 1.1, use the **show interface cable dsg downstream** command in privileged EXEC mode.

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

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

```
show interface cable {slot/port | slot/subslot/port} dsg downstream rule rule-id [ cfr | clients | verbose ]
```

```
show interface cable {slot/port | slot/subslot/port} dsg downstream tunnel tunnel-id]
```

Syntax Description

cable <i>slot/port</i>	(Optional) Displays the A-DSG information for a particular cable interface on the Cisco uBR7200 series routers. On the Cisco uBR7200 series router, <i>slot</i> can range from 3 to 6, and <i>port</i> can be 0 or 1, depending on the cable interface.
cable <i>slot/subslot/port</i>	(Optional) Displays the A-DSG information for a particular cable interface on the Cisco uBR10012 router. The following are the valid values: <ul style="list-style-type: none"> • <i>slot</i> = 5 to 8 • <i>subslot</i> = 0 or 1 • <i>port</i> = 0 to 4 (depending on the cable interface)
dcd	Displays downstream DCD messages for the A-DSG interface.
rule <i>rule-id</i>	Displays interface-level information for A-DSG rules on the Cisco CMTS, such as rule state, tunnels, classifiers, client information, upstream channel identifier, and the number of vendors associated to a rule on a given downstream.
cfr	Displays the list of classifiers associated to the A-DSG rule, such as classifiers associated with the rule-id under the interface.
clients	Displays clients associated with the rule-id under the interface
verbose	Displays A-DSG downstream rule detail information
tunnel	Displays interface-level A-DSG downstream tunnel information.

Defaults

No default behaviors or values.

Command Modes

Privileged EXEC mode

Command History

Release	Modification
12.3(13a)BC	This command was introduced to support A-DSG 1.1 on the Cisco uBR10012 and Cisco uBR7200 Series routers.

Usage Guidelines

Global configurations for A-DSG 1.1 must be complete before configuring interface definitions. Refer to the following examples for illustrative usage guidelines.

show interface cable dsg downstream

Examples

The following example illustrates A-DSG downstream configuration information and the number of DSG tunnels, classifiers, clients and vender specific parameters.

```
Router# sh interfaces c6/0 dsg downstream
```

chan list	chFreq index	chan freq	timer index	init timeout	oper timeout	twoWay timer	oneWay timer	num rule	num tunnel	num cfr	num client	num vsp
1	2	666	1	1	2	3	4	9	6	4	6	2
	3	500										

The following example illustrates the DCD statistics for the given downstream channel. DCD TLV information displays if the **debug cable dsg** command is active.

```
Router# sh int c6/0 dsg downstream dcd
```

dcd state	num of dcd sent	num of dcd fail	num of dcd change cnt	num of fragment
en	282	0	1	1

```
Router# sh int c6/0 dsg downstream dcd
```

dcd state	num of dcd sent	num of dcd fail	num of dcd change cnt	num of fragment
en	2139	0	1	1

```
Router#
```

```
00:35:58: DCD TLV last sent:
```

```
32390101 01020102 040E0302 09510100 02061111 11111111 05060100 5E010114
06020001 2B150803 12345612 3456789A BCDEF012 3456789A BCDEF032 26010102
02010104 0E030209 51010002 06111111 11111105 0601005E 01011E06 02000206
02000A32 18010103 02010104 04040200 01050601 005E0101 28060200 03321401
01040201 01040403 02070105 0601005E 01013232 14010105 02010104 04040200
02050601 005E0101 3C321401 01070201 01040404 02000605 0601005E 01011432
1E010108 02010104 0E030209 51010002 06111111 11111105 0601005E 01011432
35010114 02010104 0E030209 51010002 06111111 11111105 0601005E 0101142B
```

```
Router# 15080312 34561234 56789ABC DEF01234 56789ABC DEF01715 02020001 05010109
0C0504E6 6F6F6F03 046F6F6F 6F170F02 02000205 01010906 0504E601 0141170F
02020003 05010109 060504E6 01012817 0F020200 0A050101 09060504 E6010147
33230104 27B25A80 01041DCD 65000202 00010302 00020402 00030502 00042B05
08030022 22
```

```
Router# sh int c6/0 dsg downstream rule
```

rule id	rule state	rule pri	rule tunnel id	tunnel state	tunnel mac-addr	cfr id	cfr state	cfrIn dcd	client listId	vsp index
1	en	2	1	en	0100.5e01.0114	1	en	yes	2	1
						5	en	no		
						11	en	no		
						14	en	no		
2	en	1	2	en	0100.5e01.011e	2	en	yes	2	
						10	en	yes		
3	en	1	3	en	0100.5e01.0128	3	en	yes	3	
4	en	1	4	en	0100.5e01.0132	4	en	no	4	
5	en	1	5	en	0100.5e01.013c	9	en	no	5	
6	en	1	6	dis	0100.5e01.0146				6	2
7	en	1	1	en	0100.5e01.0114	1	en	no	10	
						5	en	no		
						11	en	no		
						14	en	no		
8	en	1	1	en	0100.5e01.0114	1	en	no	2	
						5	en	no		
						11	en	no		
						14	en	no		
20	en	1	1	en	0100.5e01.0114	1	en	no	2	1
						5	en	no		
						11	en	no		
						14	en	no		
						65535	dis	yes		

The following example displays the same information as above for the given rule.

```
Router# sh int c6/0 dsg downstream rule 1
```

rule id	rule state	rule pri	tunnel id	tunnel state	tunnel mac-addr	cfr id	cfr state	cfrIn dcd	client listId	vsp index
1	en	2	1	en	0100.5e01.0114	1	en	yes	2	1
						5	en	no		
						11	en	no		
						14	en	no		

```
Router# sh int c6/0 dsg downstream rule 1 cfr
```

rule id	cfr id	cfr state	cfrIn dcd	cfr pri	destination address	ip address	source ip address	srcPre length	d_port start	d_port end
1	1	en	yes	1	230.111.111.111	111.111.111.111	111.111.111.111	32	0	65535
	5	en	no	1	230.1.1.60	0.0.0.0	0.0.0.0	32	0	65535
	11	en	no	1	224.25.25.134	0.0.0.0	0.0.0.0	32	0	65535
	14	en	no	0	230.1.1.20	0.0.0.0	0.0.0.0	32	1000	2000

```
Router# sh int c6/0 dsg downstream rule 1 clients
```

rule id	rule state	rule pri	client listId	client id	client id type	client address
1	en	2	2	1	CA System ID	0951
				3	Broadcast	
				8	MAC Addr	1111.1111.1111

```
Router# sh int c6/0 dsg downstream rule 1 verbose
```

```
Rule ID : 1
State : enable
Priority : 2

Tunnel ID : 1
State : enable
MAC Addr : 0100.5e01.0114

Cfr Id : 1
State : enable
Priority : 1
Dest IP : 230.111.111.111
Src IP : 111.111.111.111
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End : 65535
Forwarded : 0
Received : 0

Cfr Id : 5
State : enable
Priority : 1
Dest IP : 230.1.1.60
Src IP : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End : 65535
Forwarded : 0
Received : 0

Cfr Id : 11
State : enable
Priority : 1
Dest IP : 224.25.25.134
Src IP : 0.0.0.0
Src Prefix Length : 32
Dest Port Start : 0
Dest Port End : 65535
Forwarded : 0
Received : 0
```

■ **show interface cable dsg downstream**

```

Cfr Id                : 14
State                 : enable
Priority              : 0
Dest IP               : 230.1.1.20
Src IP                : 0.0.0.0
Src Prefix Length    : 32
Dest Port Start      : 1000
Dest Port End        : 2000
Forwarded             : 0
Received              : 0

Client List Id       : 2
Client Id            : 1
Client Id Type       : CA System ID    0951
Client Id            : 3
Client Id Type       : Broadcast
Client Id            : 8
Client Id Type       : MAC Addr      1111.1111.111

vsif index           : 1
vsif oui             : 0X123456
vsif value           : 0X123456789ABCDEF0123456789ABCDEF0

```

Router# **sh int c6/0 dsg downstream tunnel**

tunnel id	tunnel state	tunnel mac-addr	cfr id	cfr state	rule id	rule state	client listId	service class
1	en	0100.5e01.0114	1	en	1	en	2	SI
			5	en	7	en	10	
			11	en	8	en	2	
			14	en	20	en	2	
2	en	0100.5e01.011e	2	en	2	en	2	NDS-CA
			10	en				
3	en	0100.5e01.0128	3	en	3	en	3	NDS-APP
4	en	0100.5e01.0132	4	en	4	en	4	MOTO-CA
5	en	0100.5e01.013c	9	en	5	en	5	MOTO-APP
6	dis	0100.5e01.0146			6	en	6	SA-CA

Router# **sh int c6/0 dsg downstream tunnel 1**

tunnel id	tunnel state	tunnel mac-addr	cfr id	cfr state	rule id	rule state	client listId	service class
1	en	0100.5e01.0114	1	en	1	en	2	SI
			5	en	7	en	10	
			11	en	8	en	2	
			14	en	20	en	2	

Related Commands

Command	Description
debug cable dsg	Enables general, DCD or packet-related debugging.
show interface	Displays general interface information for the specified or all interfaces. Use also the show interface cable dsg downstream command.

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)