Cisco cBR Series Converged Broadband Routers Application—Voice and Video Configuration Guide for Cisco IOS XE Gibraltar 16.12.x

First Published: 2019-07-15

Last Modified: 2019-12-09

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

CONTENTS

CHAPTER 1 **Unique Device Identifier Retrieval** 1

Hardware Compatibility Matrix for the Cisco cBR Series Routers 1

Unique Device Identifier Overview 2

Benefits of the Unique Device Identifier Retrieval Feature 3

Retrieving the Unique Device Identifier 3

Troubleshooting Tips 6

Additional References 6

Feature Information for Unique Device Identifier Retrieval 7

CHAPTER 2 **Advanced-Mode DOCSIS Set-Top Gateway 1.2 for the Cisco CMTS Routers** 9

Hardware Compatibility Matrix for the Cisco cBR Series Routers 10

Prerequisites for Advanced-Mode DSG Issue 1.2 10

Restrictions for Advanced-Mode DSG Issue 1.2 11

DSG Configuration File Transfer Operations 11

Multicast Configuration Restrictions 11

NAT for DSG Unicast-only Mapping 11

PIM and SSM for Multicast 11

Subinterfaces 11

Information About Advanced-Mode DSG Issue 1.2 12

DSG 1.2 Clients and Agents 12

FQDN Support 12

DSG Name Process and DNS Query 12

A-DSG Forwarding on the Primary Channel 13

DOCSIS 3.0 DSG MDF Support 13

Source Specific Multicast Mapping 13

How to Configure Advanced-Mode DSG Issue 1.2 14

Configuring the Default Multicast Quality of Service 14
Configuring DSG OPS Under MAC Domain Profile 15
Configuring Global Tunnel Group Settings for Advanced-Mode DSG 1.2 16
Global A-DSG 1.2 Tunnel Settings 17
Adding DSG Tunnel Group to a Subinterface 18
Configuring the DSG Client Settings for Advanced-Mode DSG 1.2 19
Configuring Downstream DSG 1.2 Settings for Advanced-Mode DSG 1.2 21
Configuring IP Multicast Operations 22
Enabling DNS Query and DSG Name Process 23
Configuring NAT to Support Unicast Messaging 24
Configuring WAN Interfaces for Multicast Operations 26
Configuring a Standard IP Access List for Packet Filtering 26
Configuring a Standard IP Access List for Multicast Group Filtering 28
Disabling A-DSG Forwarding on the Primary Channel 30
How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature 30
Displaying Global Configurations for Advanced-Mode DSG 1.2 30
show cable dsg cfr 30
show cable dsg host 31
show cable dsg tunnel 31
show cable dsg tg 31
show running-config interface 31
show cable dsg static-group bundle 32
Displaying Interface-level Configurations for Advanced-Mode DSG 1.2 32
show cable dsg tunnel interfaces 32
show interfaces cable dsg downstream 32
show interfaces cable dsg downstream dcd 32
show interfaces cable dsg downstream tg 32
show interfaces cable dsg downstream tunnel 32
Debugging Advanced-Mode DSG 33
Configuration Examples for Advanced-Mode DSG 33
Example: Enabling DNS Query 35
Example: Disabling A-DSG Forwarding on the Primary Channel 35
Additional References 36
Feature Information for Advanced-Mode DSG 1.2 for the Cisco CMTS Routers 36

CHAPTER 3 **Cisco Network Registrar for the Cisco CMTS Routers** 37

Hardware Compatibility Matrix for the Cisco cBR Series Routers 38

Servers Required on the HFC Network 39

Cisco Network Registrar Description 39

Overview of DHCP Using CNR 40

How Cisco Converged Broadband Routers and Cable Modems Work 41

DHCP Fields and Options for Cable Modems 42

Cisco Network Registrar Sample Configuration 43

Cable Modem DHCP Response Fields 45

DOCSIS DHCP Fields 45

DHCP Relay Option (DOCSIS Option 82) 45

Overview of Scripts 46

Two-way Cable Modem Scripts 46

Telco Return Cable Modem Scripts 46

Placement of Scripts 46

Windows NT 46

Solaris 47

Activating Scripts in Cisco Network Registrar 47

Configuring the Cisco CMTS Routers to Use Scripts 47

Configuring the System Default Policy 47

Cable Modems 48

PCs 48

Creating Selection Tag Scopes 48

General 48

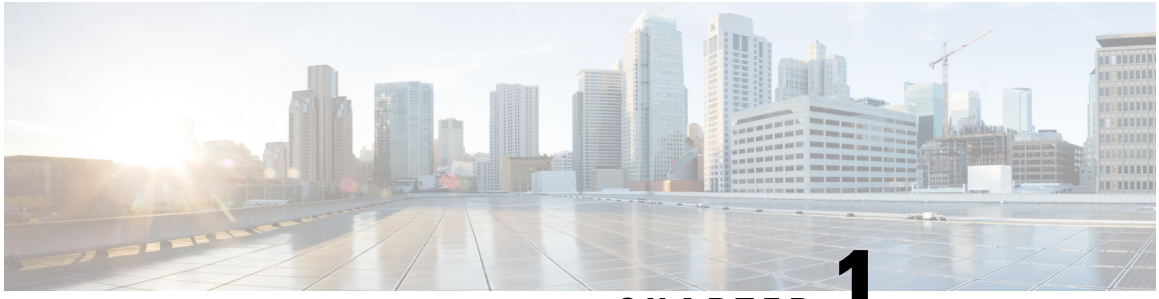
Telco Return for the Cisco cBR-8 Router 48

Creating Network Scopes 49

Creating Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images 49

CNR Steps to Support Subinterfaces 50

Additional References 51



CHAPTER 1

Unique Device Identifier Retrieval

The Unique Device Identifier (UDI) Retrieval feature provides the ability to retrieve and display the UDI information from any Cisco product that has electronically stored such identity information.

Finding Feature Information

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

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

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 1
- Unique Device Identifier Overview, on page 2
- Benefits of the Unique Device Identifier Retrieval Feature, on page 3
- Retrieving the Unique Device Identifier, on page 3
- Troubleshooting Tips, on page 6
- Additional References, on page 6
- Feature Information for Unique Device Identifier Retrieval , on page 7

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

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

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Unique Device Identifier Overview

Each identifiable product is an entity, as defined by the Entity MIB (RFC-2737) and its supporting documents. Some entities, such as a chassis, will have sub-entities like slots. An Ethernet switch might be a member of a super-entity like a stack. Most Cisco entities that can be ordered leave the factory with an assigned UDI. The UDI information is printed on a label that is affixed to the physical hardware device, and it is also stored electronically on the device in order to facilitate remote retrieval.

A UDI consists of the following elements:

- Product identifier (PID)
- Version identifier (VID)
- Serial number (SN)

The PID is the name by which the product can be ordered; it has been historically called the “Product Name” or “Part Number.” This is the identifier that one would use to order an exact replacement part.

The VID is the version of the product. Whenever a product has been revised, the VID will be incremented. The VID is incremented according to a rigorous process derived from Telcordia GR-209-CORE, an industry guideline that governs product change notices.

The SN is the vendor-unique serialization of the product. Each manufactured product will carry a unique serial number assigned at the factory, which cannot be changed in the field. This is the means by which to identify an individual, specific instance of a product.

Benefits of the Unique Device Identifier Retrieval Feature

- Identifies individual Cisco products in your networks.
- Reduces operating expenses for asset management through simple, cross-platform, consistent identification of Cisco products.
- Identifies PIDs for replaceable products.
- Facilitates discovery of products subject to recall or revision.
- Automates Cisco product inventory (capital and asset management).
- Provides a mechanism to determine the entitlement level of a Cisco product for repair and replacement service.

Product Item Descriptor for Cable Products

For information on the Product Item Descriptor (PID), see the product hardware installation guide available on Cisco.com.

Retrieving the Unique Device Identifier

To use UDI retrieval, the Cisco product in use must be UDI-enabled. A UDI-enabled Cisco product supports five required Entity MIB objects. The five Entity MIB v2 (RFC-2737) objects are:

- entPhysicalName
- entPhysicalDescr
- entPhysicalModelName
- entPhysicalHardwareRev
- entPhysicalSerialNum

Although the **show inventory** command may be available, using that command on devices that are not UDI-enabled will likely produce no output.

Enter the **show inventory** command to retrieve and display information about all of the Cisco products installed in the networking device that are assigned a PID, VID, and SN. If a Cisco entity is not assigned a PID, that entity is not retrieved or displayed.

```
Router# show inventory

NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0PR

NAME: "clc 3", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: TEST1234567
```

```
NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 3/0"
PID: CBR-D30-DS-MOD    , VID: V01, SN: CAT1725E1BZ

NAME: "Cable PHY Module", DESCR: "CLC Downstream PHY Module 3/1"
PID: CBR-D30-DS-MOD    , VID: V01, SN: CAT1725E1AT

NAME: "Cable PHY Module", DESCR: "CLC Upstream PHY Module 3/2"
PID: CBR-D30-US-MOD    , VID: V01, SN: CAT1717E0FF

NAME: "sup 1", DESCR: "Cisco cBR CCAP Supervisor Card"
PID: CBR-CCAP-SUP-60G  , VID: V01, SN: CAT1824E0MT

NAME: "harddisk 5/1", DESCR: "Hard Disk"
PID: UGB88RTB100HE3-BCU-DID, VID:    , SN: 11000066829

NAME: "sup-pic 5/1", DESCR: "Cisco cBR CCAP Supervisor Card PIC"
PID: CBR-SUP-8X10G-PIC , VID: V01, SN: CAT1720E0F4

NAME: "SFP+ module 5/1/0", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: A   , SN: FNS172720X6

NAME: "SFP+ module 5/1/1", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-LR   , VID: A   , SN: UGT085P

NAME: "SFP+ module 5/1/2", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-LR   , VID: A   , SN: UGT087Z

NAME: "SFP+ module 5/1/3", DESCR: "iNSI xcvr"
PID: SFP+ 10GBASE-SR   , VID: G4.1, SN: AVD1729A38T

NAME: "SFP+ module 5/1/7", DESCR: "iNSI xcvr"
PID: 10GE ZR           , VID: A   , SN: FNS11300AUH

NAME: "Power Supply Module 0", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM17370345

NAME: "Power Supply Module 2", DESCR: "Cisco cBR CCAP AC Power Supply"
PID: PWR-3KW-AC-V2     , VID: V02, SN: DTM173702KF
```

For diagnostic purposes, the **show inventory** command can be used with the **raw** keyword to display every RFC 2737 entity including those without a PID, UDI, or other physical identification.

Note The **raw** keyword option is primarily intended for troubleshooting problems with the **show inventory** command itself.

```
Router# show inventory raw

NAME: "Chassis", DESCR: "Cisco cBR-8 CCAP Chassis"
PID: CBR-8-CCAP-CHASS  , VID: V01, SN: FXS1739Q0PR

NAME: "slot 0/0", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 0/1", DESCR: "Chassis Slot"
PID:                   , VID:    , SN:

NAME: "slot 1/0", DESCR: "Chassis Slot"
```

```
PID:                    , VID:    , SN:

NAME: "slot 1/1", DESCR: "Chassis Slot"
PID:                    , VID:    , SN:

NAME: "slot 2/0", DESCR: "Chassis Slot"
PID:                    , VID:    , SN:

NAME: "slot 2/1", DESCR: "Chassis Slot"
PID:                    , VID:    , SN:

NAME: "slot 3/0", DESCR: "Chassis Slot"
PID:                    , VID:    , SN:

NAME: "clc 3", DESCR: "Cisco cBR CCAP Line Card"
PID: CBR-CCAP-LC-40G   , VID: V01, SN: TEST1234567

NAME: "12_CUR: Sens 3/0", DESCR: "12_CUR: Sens"
PID:                    , VID:    , SN:

NAME: "12_CUR: Vin 3/1", DESCR: "12_CUR: Vin"
PID:                    , VID:    , SN:

NAME: "12_CUR: ADin 3/2", DESCR: "12_CUR: ADin"
PID:                    , VID:    , SN:

NAME: "G0_CUR: Sens 3/3", DESCR: "G0_CUR: Sens"
PID:                    , VID:    , SN:

NAME: "G0_CUR: Vin 3/4", DESCR: "G0_CUR: Vin"
PID:                    , VID:    , SN:

NAME: "G0_CUR: ADin 3/5", DESCR: "G0_CUR: ADin"
PID:                    , VID:    , SN:

NAME: "G1_CUR: Sens 3/6", DESCR: "G1_CUR: Sens"
PID:                    , VID:    , SN:

NAME: "G1_CUR: Vin 3/7", DESCR: "G1_CUR: Vin"
PID:                    , VID:    , SN:

NAME: "G1_CUR: ADin 3/8", DESCR: "G1_CUR: ADin"
PID:                    , VID:    , SN:

NAME: "LB_CUR: Sens 3/9", DESCR: "LB_CUR: Sens"
PID:                    , VID:    , SN:

NAME: "LB_CUR: Vin 3/10", DESCR: "LB_CUR: Vin"
PID:                    , VID:    , SN:

NAME: "LB_CUR: ADin 3/11", DESCR: "LB_CUR: ADin"
PID:                    , VID:    , SN:

NAME: "Temp: CAPRICA 3/12", DESCR: "Temp: CAPRICA"
PID:                    , VID:    , SN:

NAME: "Temp: BASESTAR 3/13", DESCR: "Temp: BASESTAR"
PID:                    , VID:    , SN:

NAME: "Temp: RAIDER 3/14", DESCR: "Temp: RAIDER"
PID:                    , VID:    , SN:

NAME: "Temp: CPU 3/15", DESCR: "Temp: CPU"
PID:                    , VID:    , SN:
```

```
NAME: "Temp: INLET 3/16", DESCR: "Temp: INLET"
PID:                   , VID:    , SN:

NAME: "Temp: OUTLET 3/17", DESCR: "Temp: OUTLET"
PID:                   , VID:    , SN:

NAME: "Temp: DIGITAL 3/18", DESCR: "Temp: DIGITAL"
PID:                   , VID:    , SN:

NAME: "Temp: UPX 3/19", DESCR: "Temp: UPX"
PID:                   , VID:    , SN:
```

Troubleshooting Tips

If any of the Cisco products do not have an assigned PID, the output may display incorrect PIDs and the VID and SN elements may be missing, as in the following example.

```
NAME: "POS3/0/0", DESCR: "Skystone 4302 Sonet Framer"

PID: FastEthernet, VID: , SN:

NAME: "Serial1/0", DESCR: "M4T"

PID: M4T               , VID:    , SN:
```

In the sample output, the PID is exactly the same as the product description. The UDI is designed for use with new Cisco products that have a PID assigned. UDI information on older Cisco products is not always reliable.

Additional References

Related Documents

Related Topic	Document Title
Information about managing configuration files	Cisco IOS Configuration Fundamentals Configuration Guide
Commands for showing interface statistics	Cisco IOS Interface Command Reference

Standards and RFCs

Standard/RFC	Title
RFC 2737	*Entity MIB (Version 2)*

MIBs

MIB	MIBs Link
CISCO-ENTITY-ASSET-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

Technical Assistance

Description	Link
The Cisco Support website provides extensive online resources, including documentation and tools for troubleshooting and resolving technical issues with Cisco products and technologies. To receive security and technical information about your products, you can subscribe to various services, such as the Product Alert Tool (accessed from Field Notices), the Cisco Technical Services Newsletter, and Really Simple Syndication (RSS) Feeds. Access to most tools on the Cisco Support website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

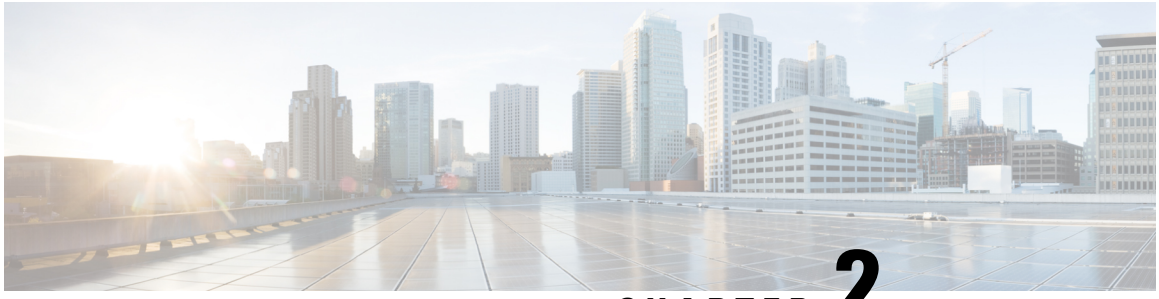
Feature Information for Unique Device Identifier Retrieval

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

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

Table 2: Feature Information for Unique Device Identifier Retrieval

Feature Name	Releases	Feature Information
Unique Device Identifier Retrieval	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 2

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

The Advanced-Mode DOCSIS Set-Top Gateway (A-DSG) Issue 1.2 introduces support for the latest DOCSIS Set-Top specification from CableLabs™, to include the following enhancements:

- *DOCSIS Set-top Gateway (DSG) Interface Specification*
- A-DSG 1.2 introduces support for the DOCS-DSG-IF MIB.

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

Finding Feature Information

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

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

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 10
- Prerequisites for Advanced-Mode DSG Issue 1.2, on page 10
- Restrictions for Advanced-Mode DSG Issue 1.2, on page 11
- Information About Advanced-Mode DSG Issue 1.2, on page 12
- How to Configure Advanced-Mode DSG Issue 1.2, on page 14
- How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 30
- Configuration Examples for Advanced-Mode DSG, on page 33
- Additional References, on page 36
- Feature Information for Advanced-Mode DSG 1.2 for the Cisco CMTS Routers, on page 36

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

Table 3: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Prerequisites for Advanced-Mode DSG Issue 1.2

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

Restrictions for Advanced-Mode DSG Issue 1.2

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

DSG Configuration File Transfer Operations

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

Multicast Configuration Restrictions

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

See the Configuring the Default Multicast Quality of Service, on page 14 and the Configuring IP Multicast Operations, on page 22 for additional Multicast information and global configurations supporting DSG.

NAT for DSG Unicast-only Mapping

A-DSG 1.2 supports multicast IP addressing. However, it also supports unicast IP destination addresses. On the Cisco cBR-8 router, DSG 1.2 support is provided with the configuration of Network Address Translation (NAT) on the router, to include these settings:

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

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

PIM and SSM for Multicast

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

- **ip pim ssm**

Refer to the Configuring IP Multicast Operations, on page 22.

Subinterfaces

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

Information About Advanced-Mode DSG Issue 1.2

A-DSG 1.2 offers these new or enhanced capabilities:

- A-DSG client and agent modes
- Advanced-mode MIBs supporting DSG 1.2, including the DOCS-DSG-IF-MIB
- Advanced-mode tunnels with increased security
- Cable interface bundling through virtual interface bundling
- Downstream Channel Descriptor
- IP multicast support
- Quality of Service (QoS)

DSG 1.2 Clients and Agents

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

FQDN Support

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

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

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

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

DSG Name Process and DNS Query

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

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

can also specify the DNS query interval using the **cable dsg name-update-interval** command in global configuration mode.

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

A-DSG Forwarding on the Primary Channel

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

For example, assume the cable interface 7/1/1 has A-DSG enabled and has four modular channels attached to it. However, you want A-DSG forwarding enabled only on two of these four modular channels. You can exclude the channels of your choice using the cable downstream dsg disable command. For details on how to disable modular channels, see the Disabling A-DSG Forwarding on the Primary Channel, on page 30.

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

DOCSIS 3.0 DSG MDF Support

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

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

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

Source Specific Multicast Mapping

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

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

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

SSM mapping can be configured on Cisco CMTS routers.

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

How to Configure Advanced-Mode DSG Issue 1.2

Advanced-mode DSG Issue 1.2 entails support for DSG tunnel configuration, to include global, WAN-side, and interface-level settings in support of Multicast.

Configuring the Default Multicast Quality of Service

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

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

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

Procedure

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

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

Step 3	**cable multicast group-qos default scn** *service-class-name* **aggregate** **Example:** `Router(config)# cable multicast group-qos default scn name1 aggregate`	Configures a service class name for the QoS profile.
Step 4	**end** **Example:**	Returns to privileged EXEC mode.

	Command or Action	Purpose
	`Router(config)# end`	

What to do next

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

Configuring DSG OPS Under MAC Domain Profile

The DOCSIS Set-Top Gateway (DSG) OPS CLI automatically creates the DSG Tunnel Group (TG) channels to MAC domain when you apply the MAC domain profile with the DSG configuration. Use the following commands to configure DSG globally.

```
cable dsg client-list XXX  id-index Y freq 470000
cable dsg vendor-param X vendor Y oui Z
cable dsg timer X Tdsg1 2 Tdsg2 150 Tdsg3 10 Tdsg4 150
cable dsg tg XXX
cable dsg tg XXX default-prority Y
cable dsg tg XXX  channel Y priotity Z
cable dsg tg XXX  channel Y ucid Z
cable dsg tg XXX  channel Y vendor-param Z
```

The DSG TG channel generated with the MAC domain profile cannot be removed globally.

```
Router(config)#no cable dsg tg 4500 ch 1
% tg 4500 channel 1 is generated by profile,would not remove it.
CBR(config)#
```

Configure DSG Under Service Group Profile

```
Router(config)#cable profile service-group Y
Router(config-profile-sg)#mac-domain 0 profile MD0
Router(config-profile-sg-md)# cable downstream dsg ?
   chan-list     DSG Channel List Setting
   dcd-enable    Enable DSG DCD messages when no enabled rules/tunnels
   tg            DSG Tunnel group
   timer         DSG Timer Setting
   vendor-param  DSG vendor specific parameters


Router(config)#cable fiber-node X
Router(config-fiber-node)#service-group profile Y
```

Verify DSG TG Configuration

```
Router#show cabl dsg tg
TG     Chan   TG             Rule  Vendor UCID     Service-group  Profile
id     id     state   I/F    pri   Param  list     Profile        chan state
-----  -----  ----- -------  ----  ------ ------   -------------- ----------
2000   1       en    C1/0/0  0                      SG1            en
4500   1       en    C1/0/0  2     2       1 2      SG1            dis
4500   2       en            0                      --             --
```

Verify Service Group Profile

```
show cable profile service-group <name>
```

Remove OPS Commands by CLI

You can remove the OPS commands by CLI under the MAC domain. Use the following commands:

```
Router#interface Cable1/0/1
Router(config-if)#no cable downstream dsg tg 4500 channel 1
Tunnel group 4500 channel 1 is configured by profile.
Do you want to remove it?[confirm]
(config-if)#
```

or use the folowing command: **no cable downstream dsg tg 4500 channel 1 force**

Re apply OPS Commands by CLI

```
Router#interface Cable1/0/1
Router(config-if)#cable downstream dsg tg 4500 channel 1
Router(config-if)#
```

Example

```
cable dsg timer 1 Tdsg1 2 Tdsg2 600 Tdsg3 300 Tdsg4 1800
cable dsg chan-list 111 index 1 freq 47000000
cable dsg vendor-param 2 vendor 2 oui 00000B
cable dsg tg 4500
cable dsg tg 4500 channel 1

cable profile service-group SG1
 cable bundle 255
 mac-domain 0 profile MD1
  downstream sg-channel 2-3 profile DS1 upstream 2-3
  cable downstream dsg chan-list 111
  cable downstream dsg timer 1
  cable downstream dsg vendor-param 2
  cable downstream dsg tg 4500
  cable downstream dsg tg 4500 priority 2
  cable downstream dsg tg 4500 vendor-param 2
  cable downstream dsg tg 4500 ucid 1 2

cable fiber-node 1
 downstream Integrated-Cable 1/0/1
 upstream Upstream-Cable 1/0/0
 downstream sg-channel 0 15 integrated-cable 1/0/1 rf-channel 0 15
 upstream sg-channel 0 7 Upstream-Cable 1/0/0 us-channel 0 7
 service-group profile SG1

interface Cable1/0/1
 cable mac-domain-profile MD1
 cable bundle 255
 cable managed fiber-node 1
```

Configuring Global Tunnel Group Settings for Advanced-Mode DSG 1.2

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

Global A-DSG 1.2 Tunnel Settings

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

Before you begin

When DOCSIS Set-top Gateway (DSG) is configured to have quality of service (QoS) for tunnel, ensure that the default multicast QoS (MQoS) is also configured. For more information, see Configuring the Default Multicast Quality of Service, on page 14.

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

Procedure

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

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

Step 3	**cable dsg tg***group-id* [**channel***channel-id* |**priority***DSG-rule-priority*] [**enable**|**disable**] **Example:** `Router(config)# cable dsg tg 1 channel 1 priority 1 enable`	Command allows the association of a group of tunnels to one or more downstream interfaces on the Cisco CMTS.
Step 4	**cabledsg tg***group-id* [**channel** *channel-id* [**ucid** *ID1*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 ucid 1`	Sets the upstream channel or channels to which the DSG 1.2 tunnel applies.
Step 5	**cable dsg tg** *group-id* [**channel** *channel-id* [**vendor-param** *vendor-group-id*]] **Example:** `Router(config)# cable dsg tg 1 channel 1 vendor-param 1`	Sets the vendor-specific parameters for upstream DSG 1.2 channels.

	Command or Action	Purpose
Step 6	**cable dsg vendor-param** *group-id* **vendor** *vendor-index* **oui** *oui* **value** *value-in-TLV* **Example:** `Router(config)# cable dsg vendor-param 1 vendor 1 oui ABCDEA value 0101AB`	Configures vendor-specific parameters for A-DSG 1.2. To remove this configuration from the Cisco CMTS, use the no form of this command.
Step 7	**cable dsg chan-list** *list-index* **index** *entry-index* **freq** *freq* **Example:** `Router(config)# cable dsg chan-list 1 index 1 freq 47000000`	Configures the A-DSG 1.2 downstream channel list. The channel list is a list of DSG channels (downstream frequencies) that set-top boxes can search to find the DSG tunnel appropriate for their operation. To remove the A-DSG 1.2 channel list from the Cisco CMTS, us the no form of this command.
Step 8	**cable dsg timer inde** [**Tdsg1** *Tdsg1*] | [**Tdsg2** *Tdsg2*] | [**Tdsg3** *Tdsg3*] | [**Tdsg4** *Tdsg4*] **Example:** `Router(config)# cable dsg timer 1 Tdsg1 1 Tdsg2 2 Tdsg3 3 Tdsg4 4`	Configures the A-DSG 1.2 timer entry to be associated to the downstream channel, and encoded into the Downstream Channel Descriptor (DCD) message. To remove the cable DSG timer from the Cisco CMTS, use the no form of this command.
Step 9	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

What to do next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 30.

Adding DSG Tunnel Group to a Subinterface

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

Before you begin

The downstream DSG should exist to create IGMP static joins.

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

Procedure

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

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

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

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

Configuring the DSG Client Settings for Advanced-Mode DSG 1.2

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

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

Procedure

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

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**cable dsg client-list** *client-list-id* **id-index** *id* {**application-id** *app-id* | **ca-system-id** *sys-id* | **mac-addr** *mac-addr* | **broadcast** [*broadcast-id*]} **Example:** `Router(config)# cable dsg client-list 1 id-index 1 mac-addr abcd.abcd.abcd`	Sets the DSG client parameters. This command is changed from earlier Cisco IOS Releases, and for DSG 1.2, this command specifies the optional broadcast ID to client ID broadcast type and vendor specific parameter index.
Step 4	**cable dsg client-list** *client-list-id* **id-index** *id* [**vendor-param** *vendor-group-id*] **Example:** `Router(config-if)# cable dsg client-list 1 id-index 1 vendor-param 1`	Sets vendor-specific parameters for the DSG client.
Step 5	**cable dsg tunnel** *tunnel id* **mac_addr** *mac addr* **tg** *tunnel-group* **clients** *client-list-id* [**enable** | **disable**] **Example:** `Router(config)# cable dsg tunnel mac-addr abcd.abcd.abcd tg 1 clients 1 enable`	This command is changed to associate a tunnel group and client-list ID to a DSG tunnel. Also, an optional QoS service class name can be associated to the tunnel. **Note** To associate a cable service class with an A-DSG tunnel on a Cisco CMTS router, use the cable dsg tunnel srv-class command in global configuration mode.
Step 6	**cable dsg cfr** *cfr index* [**dest-ip** {*ipaddr* |*hostname}]* [**tunnel** *tunnel-index*][**dest-port** *start end*]| [**priority** *priority*][**src-ip** {*ipaddr* |*hostname}* [**src-prefix-len** *length*]] [**enable | disable**] [**in-dcd {yes** | **no | ignore}**] **Example:** `Router(config)# cable dsg cfr 1 dest-ip 224.225.225.225 tunnel 1 dest-port 40 50 priority 2 src-ip ciscovideo.com src-prefix-len 24 enable`	Specifies the DSG classifier index, with optional support for the DCD parameter, indicating whether or not to include the classifier in the DCD message. **Note** When you use the **ignore** option, the DSG classifier is not included in the DCD message.

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

What to do next

Troubleshooting Tips

Refer to **debug** and **show** commands in the How to Monitor and Debug the Advanced-mode DOCSIS Set-Top Gateway Feature, on page 30.

Configuring Downstream DSG 1.2 Settings for Advanced-Mode DSG 1.2

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

Procedure

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

	Command or Action	Purpose
Step 8	**cable downstream dsg** [**dcd-enable** | **dcd-disable**] **Example:** `Router(config-if)# cable downstream dsg dcd-enable`	Enables DCD messages to be sent on a downstream channel. This command is used when there are no enabled rules or tunnels for A-DSG currently on the Cisco CMTS. To disable DCD messages, use the **disable** form of this command.
Step 9	**end** **Example:** `Router(config-if)# end`	Returns to privileged EXEC mode.

Configuring IP Multicast Operations

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

Procedure

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

	Command or Action	Purpose
		• *Cisco IOS Switching Services Command Reference* , Release 12.3 http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for each interface bundle being used for DSG traffic.
Step 6	**ip pim** {**dense-mode** | **sparse-mode** | **sparse-dense-mode**} **Example:** `Router(config-if)# ip pim dense-mode`	Enables Protocol Independent Multicast (PIM) on the cable interface, which is required to use the DSG feature: **Note** You must configure this command on each interface that forwards multicast traffic.
Step 7	Repeat Step 5, on page 23 and Step 6, on page 23 for each cable interface that is being used for DSG traffic. Also repeat these steps on each W AN interface that is forwarding IP multicast traffic from the DSG network controllers and Conditional Access (CA) servers.	
Step 8	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Enabling DNS Query and DSG Name Process

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

Before you begin

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

Procedure

	Command or Action	Purpose
Step 1	**configureterminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**ip domain-name** *name* **Example:** `Router(config)# ip domain-name cisco.com`	Sets the IP domain name that the Cisco IOS software uses to complete unqualified host names

	Command or Action	Purpose
Step 3	r **ip name-serve***server-address*[**multiple-server-addresses**] **Example:** `Router(config)# ip name-server 131.108.1.111`	Sets the server IP address.
Step 4	**cable dsg name-update-interval***minutes* **Example:** `Router(config)# cable dsg name-update-interval 10`	Sets the interval to check the DNS server for any FQDN classifier changes.
Step 5	**end** **Example:** `Router(config)# end`	Returns to privileged EXEC mode.

Configuring NAT to Support Unicast Messaging

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

For the Cisco cBR-8 router, A-DSG 1.2 can use an external router that is close to the Cisco CMTS to support unicast messaging. In this case, the nearby router must support NAT, and then send the address-translated multicast IP packets to the Cisco CMTS.

Tip This procedure should be performed after the cable interface has already been configured for DSG operations, as described in the Configuration Examples for Advanced-Mode DSG, on page 33.

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

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**interface** *wan-interface* **Example:**	Enters interface configuration mode for the specified WAN interface.

	Command or Action	Purpose
	`Router(config)# interface FastEthernet0/0`	
Step 3	**ip nat outside** **Example:** `Router(config-if)# ip nat outside`	Configures the WAN interface as the "outside" (public) NAT interface.
Step 4	**interface bundle** *bundle-number* **Example:** `Router(config-if)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle. **Note** This interface bundle should have previously been configured for DSG operations.
Step 5	**ip address** *ip-address mask* **secondary** **Example:** `Router(config-if)# ip address 192.168.18.1 255.255.255.0 secondary`	Configures the cable interface with an IP address and subnet that should match the unicast address being used for DSG traffic. This IP address and its subnet must not be used by any other cable interfaces, cable modems, or any other types of traffic in the cable network.
Step 6	**ip nat inside** **Example:** `Router(config-if)# ip nat inside`	Configures the cable interface as the "inside" (private) NAT interface.
Step 7	**exit** **Example:** `Router(config-if)# exit`	Exits interface configuration mode and returns to global configuration mode.
Step 8	**ip nat inside source static** *ip-multicast-address cable-ip-address* **Example:** `Router(config)# ip nat inside source static 224.3.2.1 192.168.18.2`	Maps the unicast IP address assigned to the cable interface to the multicast address that should be used for the DSG traffic.
Step 9	Repeat Step 2, on page 24 and Step 8, on page 25 for each cable interface to be configured for DSG unicast traffic.	
Step 10	**end** **Example:** `Router(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring WAN Interfaces for Multicast Operations

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

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

These commands are described in the Configuring IP Multicast Operations, on page 22, and in the following documents on Cisco.com.

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

- *Cisco IOS IP Command Reference, Volume 3 of 4* : Multicast, Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/ipmulti/command/reference/iprmc_r.html

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

- *Cisco IOS IP Command Reference, Volume 3 of 4: Multicast* , Release 12.3 T

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

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

- *Cisco IOS Switching Services Command Reference* , Release 12.3

http://www.cisco.com/en/US/docs/ios/12_3/switch/command/reference/swtch_r.html

Configuring a Standard IP Access List for Packet Filtering

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

Tip This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the Additional References, on page 36.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* .

	Command or Action	Purpose
		• *access-list* —Number or name of a standard IP access list. The number can range from 1 to 99 with no default. • *group-ip-address* —IP address to be used as a base for this access list. It should be based on the group IP address used for DSG tunnels of the interface. • *mask* —(Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* . • *access-list* —Number or name of a standard IP access list. The number can range from 1 to 99 with no default. • *group-ip-address* —IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels. • *mask* —(Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface bundle** *bundle-number* **Example:** `Router(config)# interface bundle 10`	Enters interface configuration mode for the specified interface bundle.
Step 6	**ip access-group** *access-list* **Example:** `Router(config-if)# ip access-group 90`	(Optional, but recommended) Configures the interface with the access list, so that packets are filtered by the list before being accepted on the interface. • *access-list* —Number or name of a standard IP access list. The number can range from 1 to 99 and should be the same list created in Step 3. **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.

	Command or Action	Purpose
		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.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to Privileged EXEC mode.

Configuring a Standard IP Access List for Multicast Group Filtering

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

Tip This procedure assumes a basic knowledge of how access lists use an IP address and bitmask to determine the range of IP addresses that are allowed access. For full details on configuring access lists, see the documents listed in the Additional References, on page 36.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 2	**access-list** *access-list* **permit** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 permit 228.1.1.1`	Creates an access list specifying that permits access to the specific multicast address that matches the specified *group-ip-address* and *mask* . • *access-list* —Number or name of a standard IP access list. The number can range from 1 to 99 with no default. • *group-ip-address* —IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels.

	Command or Action	Purpose
		• *mask* —(Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.
Step 3	**access-list** *access-list* **deny** *group-ip-address* [*mask*] **Example:** `Router(config)# access-list 90 deny 224.0.0.0 15.255.255.255`	Configures the access list that denies access to any multicast address that matches the specified *group-ip-address* and *mask* . • *access-list* —Number or name of a standard IP access list. The number can range from 1 to 99 with no default. • *group-ip-address* —IP address to be used as a base for this access list. It should be based on the group IP address used for the interface's DSG tunnels. • *mask* —(Optional) Bitmask that determines which addresses in the *group-ip-address* will be allowed access. The default is 255.255.255.255.
Step 4	**access-list** *access-list* **deny any** **Example:** `Router(config)# access-list 90 deny any`	Configures the access list so that it denies access to any IP addresses other than the ones previously configured.
Step 5	**interface cable** *interface* **Example:** `Router(config)# interface cable 3/0`	Enters interface configuration mode for the specified cable interface.
Step 6	**ip igmp access-group** *access-list* [*version*] **Example:** `Router(config-if)# ip igmp access-group 90`	(Optional, but recommended) Configures the interface to accept traffic only from the associated access list, so that only authorized devices are allowed to access the DSG tunnels. • *access-list* —Number or name of a standard IP access list. The number can range from 1 to 99 and should be the same list created in Step 3. • *version* —(Optional) Specifies the IGMP version. The default is 2.
Step 7	**end** **Example:** `Router(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Disabling A-DSG Forwarding on the Primary Channel

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

Procedure

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

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

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

Displaying Global Configurations for Advanced-Mode DSG 1.2

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

show cable dsg cfr

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

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

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

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

show cable dsg host

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

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

show cable dsg tunnel

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

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

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

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

show cable dsg tg

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

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

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

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

show running-config interface

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

```
Router# show running-config interface bundle 11.2
!
interface Bundle11.2
 ip address 4.4.2.1 255.255.255.0
 no ip unreachables
 ip pim sparse-mode
```

```
 ip igmp static-group 230.1.1.30
 no cable ip-multicast-echo
 cable dsg tg 61
end
```

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

show cable dsg static-group bundle

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

Displaying Interface-level Configurations for Advanced-Mode DSG 1.2

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

show cable dsg tunnel interfaces

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

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

show interfaces cable dsg downstream

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

show interfaces cable dsg downstream dcd

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

show interfaces cable dsg downstream tg

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

show interfaces cable dsg downstream tunnel

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

Debugging Advanced-Mode DSG

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

Configuration Examples for Advanced-Mode DSG

This configuration example illustrates a sample DSG network featuring these components:

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

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

CMTS Headend 1

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

CMTS Headend 2

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

Example of Two DSG Tunnels with MAC DA Substitution

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

These settings apply to DSG #1 and two downstreams:

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

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

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

DSG Example with Regionalization Per Downstream

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

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

DSG Example with Regionalization Per Upstream

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

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

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

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

These settings apply to DSG #1:

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

- UDP DP—8000

These settings apply to DSG Rule #2:

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

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

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

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

Example: Enabling DNS Query

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

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

Example: Disabling A-DSG Forwarding on the Primary Channel

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

```
Router# configure terminal
Router(config)# interface modular-cable 1/0/0:0
```

```
Router(config-if)# cable downstream dsg disable
Router(config-if)# end
```

Additional References

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

Technical Assistance

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

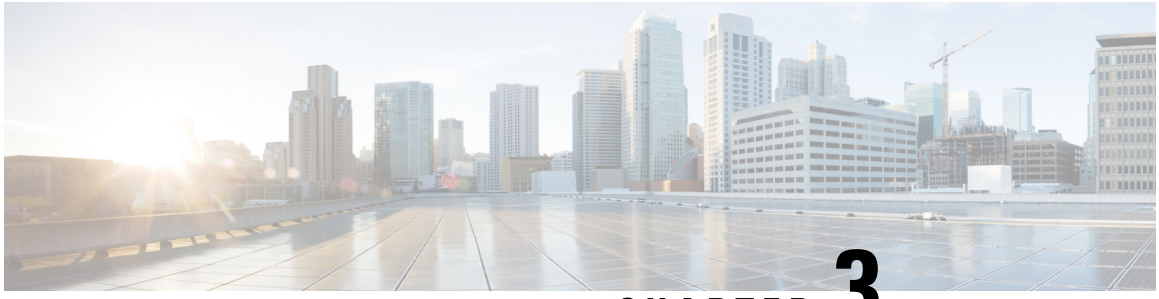
Feature Information for Advanced-Mode DSG 1.2 for the Cisco CMTS Routers

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

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

Table 4: Feature Information for DOCSIS Set-Top Gateway and A-DSG for the Cisco CMTS Routers

Feature Name	Releases	Feature Information
DOCSIS Set-Top Gateway for the Cisco CMTS Routers	Cisco IOS XE Everest 16.6.1	This feature was integrated into Cisco IOS XE Everest 16.6.1 on the Cisco cBR Series Converged Broadband Routers.



CHAPTER 3

Cisco Network Registrar for the Cisco CMTS Routers

This chapter supplements the Cisco Network Registrar (CNR) documentation by providing additional cable-specific instructions to provision a hybrid fiber-coaxial (HFC) network using Cisco universal broadband routers as CMTSs at the headend of the network.

Note For information about the IPv6 provisioning on CNR server, please refer to IPv6 on Cable.

Finding Feature Information

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

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

Contents

- Hardware Compatibility Matrix for the Cisco cBR Series Routers, on page 38
- Servers Required on the HFC Network, on page 39
- Cisco Network Registrar Description, on page 39
- Overview of DHCP Using CNR, on page 40
- How Cisco Converged Broadband Routers and Cable Modems Work, on page 41
- DHCP Fields and Options for Cable Modems, on page 42
- Cisco Network Registrar Sample Configuration, on page 43
- Overview of Scripts, on page 46
- Placement of Scripts, on page 46
- Activating Scripts in Cisco Network Registrar, on page 47
- Configuring the Cisco CMTS Routers to Use Scripts, on page 47
- Configuring the System Default Policy, on page 47
- Creating Selection Tag Scopes, on page 48

• Creating Network Scopes, on page 49
• Creating Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images, on page 49
• CNR Steps to Support Subinterfaces, on page 50
• Additional References, on page 51

Hardware Compatibility Matrix for the Cisco cBR Series Routers

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

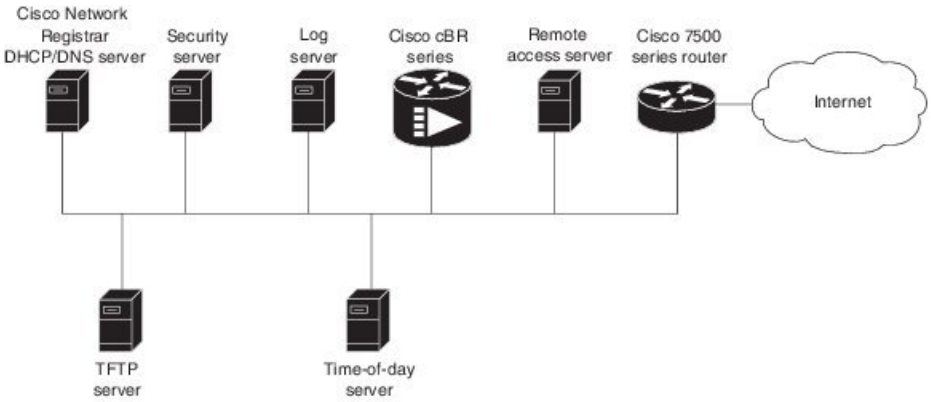
Table 5: Hardware Compatibility Matrix for the Cisco cBR Series Routers

Cisco CMTS Platform	Processor Engine	Interface Cards
Cisco cBR-8 Converged Broadband Router	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 Supervisor: • PID—CBR-SUP-250G • PID—CBR-CCAP-SUP-160G • PID—CBR-CCAP-SUP-60G	**Cisco IOS-XE Release 16.5.1 and Later Releases** Cisco cBR-8 CCAP Line Cards: • PID—CBR-LC-8D30-16U30 • PID—CBR-LC-8D31-16U30 • PID—CBR-RF-PIC • PID—CBR-RF-PROT-PIC • PID—CBR-CCAP-LC-40G • PID—CBR-CCAP-LC-40G-R • PID—CBR-CCAP-LC-G2-R • PID—CBR-SUP-8X10G-PIC • PID—CBR-2X100G-PIC Digital PICs: • PID—CBR-DPIC-8X10G • PID—CBR-DPIC-2X100G Cisco cBR-8 Downstream PHY Module: • PID—CBR-D31-DS-MOD Cisco cBR-8 Upstream PHY Modules: • PID—CBR-D31-US-MOD

Servers Required on the HFC Network

A TFTP server, DHCP server, and time-of-day (TOD) server are required to support two-way data cable modems on an HFC network. A cable modem will not boot if these servers are not available. The log server and security servers are not required to configure and operate a cable modem. If the log server or security servers are not present, a cable modem will generate warning messages, but it will continue to boot and function properly.

Figure 1: Servers Required on a Two-Way HFC Network



The servers shown here can exist on the same platform. For example, the time-of-day server and the TFTP server can run on the same platform.

384545

In this provisioning model, TOD and TFTP servers are standard Internet implementations of the RFC 868 and RFC 1350 specifications. Most computers running a UNIX-based operating system supply TOD and TFTP servers as a standard software feature. Typically, the TOD server is embedded in the UNIX *inetd* and it requires no additional configuration. The TFTP server is usually disabled in the standard software but can be enabled by the user. Microsoft NT server software includes a TFTP server that can be enabled with the services control panel. Microsoft NT does not include a TOD server. A public domain version of the TOD server for Microsoft NT can be downloaded from several sites.

The DHCP and Domain Name System (DNS) server shown in Figure above must be the DHCP/DNS server available in Cisco Network Registrar version 2.0 or later. CNR is the only DHCP server that implements policy-based assignment of IP addresses. The headend must be a Cisco cBR-8 converged broadband router. The remote access server is only required on HFC networks that are limited to one-way (downstream only) communication. In a one-way HFC network, upstream data from a PC through the headend to the Internet is carried over a dialup connection. This dialup connection for upstream data is referred to as telco return. For simplification, the model will not include a log or security server. Cable modems can be set up to use the logging and security servers by including the appropriate DHCP options in the cable modem policy as described in the *Cisco Network Registrar User Manual*.

Cisco Network Registrar Description

CNR is a dynamic IP address management system, running on Windows or Solaris, that uses the Dynamic Host Configuration Protocol (DHCP) to assign IP addresses to cable interfaces, PCs, and other devices on the broadband network. The CNR tool includes script extensions that allow a cable system administrator to define

and view individual DHCP options, define the identity or type of device on the network, and assign the device to a predefined class or group.

Using the CNR tool, a cable system administrator can specify policies to provide:

- Integrated DHCP and Domain Name Server (DNS) services
- Time of Day (ToD) and Trivial File Transfer Protocol (TFTP) server based on the size of the network
- DHCP safe failover and dynamic DNS updates

Note This is available only in CNR 3.0 or higher.

Using the CNR tool and the extension scripts identified in the Overview of Scripts, on page 46 section, a cable system administrator can specify scopes, policies, and options for the network and each cable interface based on the services and configuration to support at each subscriber site.

Note Scopes refer to the administrative grouping of TCP/IP addresses; all IP addresses within a scope should be on the same subnet.

The cable system administrator defines system default policies for all standard options and uses scope-specific policies for options related to particular subnets, such as cable interfaces. This allows DHCP to send the information with the IP address.

Seven entry points exist for scripts:

- post-packet-decode
- pre-client-lookup
- post-client-lookup—Examines and takes action on results of the client-class process, places data items in the environment dictionary to use at the pre-packet-encode extension point, includes DHCP relay option
- check-lease-acceptable
- pre-packet-encode
- post-sent-packet
- pre-dns-add-forward

Overview of DHCP Using CNR

Cisco Network Registrar (CNR) is a dynamic IP address management system that uses the Dynamic Host Configuration Protocol (DHCP) and assigns IP addresses to PCs and other devices on a network based on a predefined set of policies, such as class of service. CNR assigns available IP addresses from address pools based on the identity or type of the requesting device and the policies in effect. For example, CNR can distinguish between registered devices, unregistered devices, and registered devices that have been assigned to a particular class of service.

CNR also provides extensions that can be customized (via programming or a script) so that you can view individual DHCP options, determine the identity or type of a device based on the content of the options, and assign a device to a predefined class or group. Using these extensions, you can determine the difference between PCs and cable modems and assign them IP addresses from different address pools.

In typical data-over-cable environments, service providers are interested in simplifying provisioning to limit the amount of information that must be collected about subscribers' customer premise equipment (CPEs). To support current provisioning models, a field technician must be sent to a subscriber's home or business to install and setup a cable modem. During this site visit, the technician might register the serial number and MAC address of the cable modem in the customer account database. Because a field technician must go to a subscriber's site to replace a cable modem, you can easily track modem information.

Manually registering and tracking information about a cable subscriber's PC is more difficult. A subscriber might purchase a new PC or exchange the network interface card (NIC) without notifying you of the change. Automatic provisioning with CNR reduces the amount of customer service involvement needed to track customer equipment. To use the provisioning model described in this document, you must still track serial numbers and MAC addresses for cable modems, but you do not need to track information about the PC or NIC cards installed at a subscriber site.

The remainder of this document describes how to configure CNR to support this model. The following sections describe the equipment and servers required for the cable headend, provide an overview of the interaction between DOCSIS-compatible cable modems and the Cisco universal broadband routers, and provide a guide on how to configure CNR to support this provisioning model.

How Cisco Converged Broadband Routers and Cable Modems Work

Cisco converged broadband routers and cable modems are based on the Data Over Cable Service Interface Specification (DOCSIS) standards. These standards were created by a consortium of cable service providers called Multimedia Cable Network Systems, Ltd. (MCNS) to that cable headend and cable modem equipment produced by different vendors will interoperate. The key DOCSIS standards provide the basis for a cable modem to communicate with any headend equipment and headend equipment to communicate with any cable modem.

Cable modems are assigned to operate on specific cable channels so activity can be balanced across several channels. Each Cisco cBR-8 router installed at the headend serves a specific channel. Part of network planning is to decide which channel each cable modem can use.

A cable modem cannot connect to the network until the following events occur:

- The cable modem initializes and ranges through available frequencies until it finds the first frequency that it can use to communicate to the headend. The cable modem might be another vendor's DOCSIS-compatible device and the headend might have a Cisco cBR-8 router installed. At this point on the initial connection, the cable modem cannot determine if it is communicating on the correct channel.
- The cable modem goes through the DHCP server process and receives a configuration file from the server.
- One of the parameters in the configuration file tells the cable modem which channel it can use.
- If the assigned channel is not available on the Cisco cBR-8 router to which the cable modem is currently connected, it resets itself and comes up on the assigned channel.
- During this second DHCP process, the modem will be connected to the correct CMTS. This time, the configuration file will be loaded. For a DOCSIS-compatible cable modem to access the network, it might go through the DHCP server two times on two different networks; therefore, one-lease-per-client IP addressing is critical.

DHCP Fields and Options for Cable Modems

DHCP options and packet fields are required to enable cable modems to boot and operate properly. Table below lists the required DHCP options and fields.

Table 6: Required DHCP Fields and Options

Required Field/Option	Field/Option In Cisco Network Registrar	Value/Description
Fields		
giaddr	-	IP address. As a DHCP packet passes through the relay agent to the DHCP server, the relay agent supplies a unique IP address to the packet and stores it in this field. The relay agent is a cBR-8 router with the iphelper attribute defined.
subnet-mask	-	Subnet mask for the IP address stored in the giaddr field. This value is also stored in the DHCP packet by the relay agent.
file	Packet-file-name	Name of the cable modem configuration file that will be read from a TFTP server.
siaddr	Packet-siaddr	IP address of the TFTP server where configuration files are stored.
Options		
Time-servers	-	List of hosts running the time server specified in the RFC 868 standard.
Time-offset	-	Time offset of a cable modem internal clock from Universal Time Coordinated (UTC). This value is used by cable modems to calculate the local time that is stored in time-stamping error logs.
MCNS-security-server	-	IP address of the security server. This should be set if security is required. See RFC 1533 for details.

Cisco Network Registrar Sample Configuration

You can use the following information to set up Cisco Network Registrar in a trial configuration. The configuration describes DHCP-related setup only; it does not cover setting up DNS or configuring dynamic DNS (DDNS). You should be familiar with important CNR concepts including scopes, primary and secondary scopes, scope selection tags, client classes, and CNR policies. See the Using Network Registrar publication for detailed information on these concepts.

In the trial configuration, you can configure CNR to perform the following operations:

- Receive DHCP requests from a cable modem and a PC on an HFC network via a port supporting multiple network numbers. The Cisco cBR-8 router at the headend must be configured as a forwarder (iphelper is configured).
- Serve IP addresses on two networks; a net-10 network (non-Internet routable) and a net-24 network (Internet routable).
- Tell the difference between a cable modem and a PC based on the MAC address of the device and provide net-24 addresses to the PC and net-10 addresses to the cable modem.
- Refuse to serve IP addresses to MAC addresses that it does not recognize.

To perform these options, you must implement the following CNR configuration items:

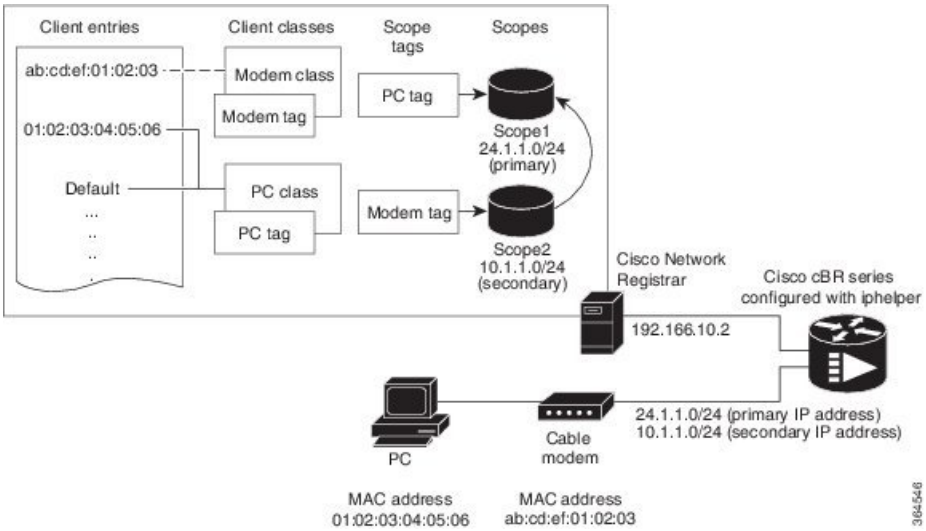
- Create two scope selection tags; one for PCs, one for cable modems.
- Create two client-classes; one for PCs , one for cable modems.
- Create a lease policy appropriate for the cable modem devices.
- Create a lease policy appropriate for the PC devices.
- Create a scope containing Class A net-24 (routable) addresses.
- Create a scope containing Class A net-10 (nonroutable) addresses.
- Identify the scope containing the net-24 addresses as the primary scope and configure the other scope containing the net-10 addresses as secondary to the net-24 scope.

Note The Cisco cBR-8 router upstream ports must be configured with the primary network address on the net-24 network; such as 24.1.1.1.

- Assign the policies to the appropriate scope.
- Add the MAC address of the cable modem and the PC to the client-entry list.
- Associate the PC tag with the scope containing routable addresses.
- Associate the cable modem tag with the scope containing nonroutable addresses.
- Associate the cable modem tag with the cable modem client-class.
- Associate the PC tag with the PC client-class.
- Assign the PC MAC to the PC class.
- Assign the cable modem MAC to the cable modem class.
- Enable client-class processing.

Figure below shows the trial CNR configuration in an HFC network.

Figure 2: Trial Configuration in an HFC Network



These configuration items and their associations can be created using either the CNR management graphical user interface (GUI) or command-line interface (CLI). The following sample script configures DHCP for a sample server:

```
File: cabledemo.rc
Command line: nrcmd -C <cluster> -N <user name> -P <password> -b < cabledemo.rc
-------------------------------------------------------------------------------------
scope-selection-tag tag-CM create
scope-selection-tag tag-PC create
client-class create class-CM
client-class class-CM set selection-criteria=tag-CM
client-class create class-PC
client-class class-PC set selection-criteria=tag-PC
policy cmts-cisco create
policy cmts-cisco setleasetime 1800
policy cmts-cisco setoption domain-name-servers 192.168.10.2
policy cmts-cisco setoption routers 10.1.1.1
policy cmts-cisco setoption time-offset  604800
policy cmts-cisco setoption time-servers 192.168.10.20
policy cmts-cisco set packet-siaddr=192.168.10.2
policy cmts-cisco setoption log-servers 192.168.10.2
policy cmts-cisco setoption mcns-security-server 192.168.10.2
policy cmts-cisco set packet-file-name=golden.cfg
policy cmts-cisco set dhcp-reply-options=packet-file-name,packet-siaddr,mcns-security-server
policy pPC create
policy pPC set server-lease-time 1800
policy pPC setleasetime 1800
policy pPC setoption domain-name-servers 192.168.10.2
policy pPC setoption routers 24.1.1.1
scope S24.1.1.0 create 24.1.1.0 255.255.255.0
scope S24.1.1.0 addrange 24.1.1.5 24.1.1.254
scope S24.1.1.0 set policy=pPC
scope S24.1.1.0 set selection-tags=tag-PC
scope S10.1.1.0 create 10.1.1.0 255.255.255.0
scope S10.1.1.0 addrange 10.1.1.5 10.1.1.254
scope S10.1.1.0 set policy=cmts-cisco
scope S10.1.1.0 set selection-tags=tag-CM
scope S10.1.1.0 set primary-scope=S24.1.1.0
client 01:02:03:04:05:06 create client-class-name=class-PC
```

```
client ab:cd:ef:01:02:03 create client-class-name=class-CM
client default create action=exclude
dhcp enable client-class
dhcp enable one-lease-per-client
save
dhcp reload
```

In addition to the DHCP server setup, you might want to enable packet-tracing. When packet-tracing is enabled, the server parses both requests and replies, and then adds them to the logs. If you do enable tracing, performance will be adversely affected, and the logs will roll over quickly.

Use the following nrcmd command to set packet tracing.

DHCP set log-settings=incoming-packet-detail,outgoing-packet-detail

Cable Modem DHCP Response Fields

Each cable interface on the broadband network requires the following fields in the DHCP response:

- CM's IP address
- CM's subnet mask

Note For cable operators with less experience in networking, you can fill in a guess based on the network number and indicate how your IP network is divided.

- Name of the DOCSIS configuration file on the TFTP server intended for the cable interface
- Time offset of the cable interface from the Universal Coordinated Time (UTC), which the cable interface uses to calculate the local time when time-stamping error logs
- Time server address from which the cable interface obtains the current time

DOCSIS DHCP Fields

DOCSIS DHCP option requirements include:

- IP address of the next server to use in the TFTP bootstrap process; this is returned in the siaddr field
- DOCSIS configuration file that the cable interface downloads from the TFTP server

Note If the DHCP server is on a different network that uses a relay agent, then the relay agent must set the gateway address field of the DHCP response.

- IP address of the security server should be set if security is required

DHCP Relay Option (DOCSIS Option 82)

DOCSIS Option82 modifies DHCPDISCOVER packets to distinguish cable interfaces from the CPE devices or "clients" behind them. The DOCSIS Option82 is comprised of the following two suboptions:

- Suboption 1, Circuit ID:

```
Type 1 (1 byte)
Len 4 (1 byte)
Value (8 bytes)
<bit 31,30,....................0)
<xYYYYYYYYYYYYYYYYYYYYYYYYYYYYY>
```

where the MSB indicates if the attached device is a cable interface.

x=1 Cable Modem REQ

x=0 CPE device (Behind the cable interface with the cable interface MAC address shown in suboption 2.)

The rest of the bits make up the SNMP index to the CMTS interface.

Y=0xYYYYYYY is the SNMP index to the CMTS interface.

- Suboption 2, MAC address of the cable interface:

```
Type 2 (1 byte)
Len 6 (1 byte)
Value xxxx.xxxx.xxxx (6 bytes)
```

Overview of Scripts

This section lists the scripts applicable to cable interface configuration.

Two-way Cable Modem Scripts

To support two-way configurations at a subscriber site, use these scripts:

- **Relay.tcl**
- **SetRouter.tcl**

Telco Return Cable Modem Scripts

To support telco return and two-way cable interface configurations on the same cable interface card or chassis, use these scripts:

- **PostClientLookup.tcl**
- **PrePacketEncode.tcl**

Placement of Scripts

Windows NT

For CNR running on Windows NT, place the appropriate scripts in the following directory:

```
\program files\network registrar\extensions\dhcp\scripts\tcl
```

Solaris

For CNR running on Solaris, place the appropriate scripts in the following directory:

```
/opt/nwreg2/extensions/dhcp/scripts/tcl
```

Activating Scripts in Cisco Network Registrar

To activate the scripts after you have placed them in the appropriate directory:

Step 1 Open up a text editor.

Step 2 Open one of the scripts at the nrcmd> command prompt.

Step 3 Create the extension points and attach them to the system.

Note The easiest way to do this is to simply cut and paste the command lines from the scripts to the nrcmd> command line.

Step 4 After you have created and attached the extension points, do a dhcp reload.

The scripts are active.

Configuring the Cisco CMTS Routers to Use Scripts

Each cable interface must be set up as a BOOTP forwarder and have the relay option enabled. The primary and secondary IP addresses for each cable interface must be in sync with the CNR tool.

To properly communicate with scripts in the system, use the following commands on the Cisco CMTS router:

- To enable option 82, use the **ip dhcp relay info option** command.
- To disable the validation of DHPC relay agent information in forwarded BOOTREPLY messages, use the **no ip dhcp relay information option check** command.

Note You can also use the cable dhcp-giaddr command in cable interface configuration mode to modify the GIADDR field of DHCPDISCOVER and DHCPREQUEST packets to provide a relay IP address before packets are forwarded to the DHCP server. Use this command to set a “policy” option such that primary addresses are used for CMs and secondary addresses are used for hosts behind the CMs.

Configuring the System Default Policy

Add these options to the system default policy for:

- Cable modems to support on your network
- PCs to support behind each cable interface on your network

Cable Modems

Define these settings following the CNR tool documentation:

- TFTP server (IP address) for those cable interfaces using BOOTP
- Time-server (IP address)
- Time-offset (Hex value, 1440 for Eastern Standard Time)
- Packet-siaddr (IP address of CNR)
- Router (set to 0.0.0.0)
- Boot-file (name of .cm file for those cable interfaces using BOOTP)
- Packet-file-name (.cm file name)

PCs

Define these settings following the CNR tool documentation:

- Domain name
- Name servers (IP address of DNS servers)

Creating Selection Tag Scopes

General

When you create your scope selection tags:

Step 1 Cut and paste the scope selection tag create commands from the scripts into the nrcmd> command line.

Note These names have to be exactly as they appear in the scripts.

Step 2 Then attach the selection tags to the appropriate scripts:

Example:

CM_Scope tagCablemodem

PC_Scope tagComputer

Telco Return for the Cisco cBR-8 Router

Before you begin

Note If you are using the prepacketencode and postclientlookup .tcl scripts for telco return, the telco return scope does not have a selection tag associated to the scope.

SUMMARY STEPS

1. Put the tag Telcocablemodem on the primary cable interface scope to pull addresses from that pool instead.
2. Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

DETAILED STEPS

Step 1 Put the tag Telcocablemodem on the primary cable interface scope to pull addresses from that pool instead.

Step 2 Follow the same procedure as above, but use a telco return policy which has a different .cm file with telco-specific commands in it.

Creating Network Scopes

Following is an example for creating scopes for your network. This example assumes two Cisco cBR-8 converged broadband routers in two locations, with one cable interface card on one Cisco cBR-8 configured for telco return.

```
cm-toledo1_2-0 10.2.0.0 255.255.0.0 assignable 10.2.0.10-10.2.254.254 tagCablemodem
tagTelcomodem Default GW=10.2.0.1 (assigned by scripts)
cm-toledo1_3-0 10.3.0.0 255.255.0.0 assignable 10.3.0.10-10.3.254.254 tagCablemodem
tagTelcomodem Default GW=10.3.0.1 (assigned by scripts)
pc-toledo1_2-0 208.16.182.0 255.255.255.248 assignable 208.16.182.2-208.16.182.6 tagComputer
 Default GW=208.16.182.1 (assigned by scripts)
pc-toledo1_3-0 208.16.182.8 255.255.255.248 assignable 208.16.182.10-208.16.182.14 tagComputer
 Default GW=208.16.182.9 (assigned by scripts)
telco_return_2-0 192.168.1.0 255.255.255.0 (No assignable addresses, tag was put on cable
modem primary scope to force telco-return cable modem to pull address from primary scope)
cm-arlington1_2-0 10.4.0.0 255.255.0.0 assignable 10.4.0.10-10.4.254.254 tagCablemodem
Default GW=10.4.0.1 (assigned by scripts)
cm-arlington1_3-0 10.5.0.0 255.255.0.0 assignable 10.5.0.10-10.5.254.254 tagCablemodem
Default GW=10.5.0.1 (assigned by scripts)
pc-arlington1_2-0 208.16.182.16 255.255.255.248 assignable 208.16.182.17-208.16.182.22
tagComputer Default GW=208.16.182.17 (assigned by scripts)
pc-toledo1_3-0 208.16.182.24 255.255.255.248 assignable 208.16.182.2-208.16.182.30 tagComputer
 Default GW=208.16.182.25 (assigned by scripts)
```

Note Remember the last valid address in the .248 subnet range is the broadcast address; do not use this.

Creating Policies for Class of Service or for Upgrading Cable Modem Cisco IOS Images

To support Class of Service (CoS), define:

- Scope selection tags—Identifiers that describe types of scope configurations

Note This is needed for Option82.

- Client classes—Class with which a group of clients is associated

Note Scope selection tags are excluded from or included in client-classes.

- Client—Specific DHCP clients and the defined class to which they belong

To assign the CoS or use Option82, make a client entry with a MAC address and point to the appropriate policy. To use client-based MAC provisioning, add a client entry "default - exclude," then put in MAC addresses for all devices (for example, cable interfaces and PCs) in the client tab and select the policy to use, including the appropriate tag.

CNR Steps to Support Subinterfaces

The CNR configuration is done differently if subinterfaces are configured. Here is an example. If you have configured two ISP subinterfaces and one management subinterface on a Cisco cBR-8 router, make sure that the management subinterface is the first subinterface that is configured. If cable interface three—c3/0/0—is being used, create c3/0/0.1, c3/0/0.2 and c3/0/0.3 as three subinterfaces and c3/0/0.1 as the first subinterface configured as the management subinterface.

Note The Cisco cBR-8 router requires management subinterfaces to route DHCP packets from CMs when they first initialize because the Cisco cBR-8 router does not know the subinterfaces they belong to until it has seen the IP addresses assigned to them by gleaning DHCP reply message from CNR.

In CNR, complete the following steps for such a configuration:

SUMMARY STEPS

1. Create two scope selection tags such as: isp1-cm-tag and isp2-cm-tag
2. Configure three scopes; for example, mgmt-scope, isp1-cm-scope, and isp2-cm-scope such that isp1-cm-scope and isp2-cm-scope each define mgmt-scope to be the primary scope
3. Also configure two scopes for PCs for each of the ISPs; isp1-pc-scope and isp2-pc-scope. For scope isp1-cm-scope, configure isp1-cm-tag to be the scope selection tag. For scope isp2-cm-scope, configure isp2-cm-tag to be the scope selection tag
4. Configure two client classes; for example, isp1-client-class and isp2-client-class
5. Create client entries with their MAC addresses for CMs that belong to ISP1 and assign them to isp1-client-class. Also assign the scope selection tag isp1-cm-tag
6. Create client entries for CMs that belong to ISP2 and assign them to isp2-client-class. Also assign the scope selection tag isp2-cm-tag
7. Enable client class processing from the scope-selection-tag window

DETAILED STEPS

Step 1 Create two scope selection tags such as: isp1-cm-tag and isp2-cm-tag

Step 2 Configure three scopes; for example, mgmt-scope, isp1-cm-scope, and isp2-cm-scope such that isp1-cm-scope and isp2-cm-scope each define mgmt-scope to be the primary scope

Step 3 Also configure two scopes for PCs for each of the ISPs; isp1-pc-scope and isp2-pc-scope. For scope isp1-cm-scope, configure isp1-cm-tag to be the scope selection tag. For scope isp2-cm-scope, configure isp2-cm-tag to be the scope selection tag

Step 4 Configure two client classes; for example, isp1-client-class and isp2-client-class

Step 5 Create client entries with their MAC addresses for CMs that belong to ISP1 and assign them to isp1-client-class. Also assign the scope selection tag isp1-cm-tag

Step 6 Create client entries for CMs that belong to ISP2 and assign them to isp2-client-class. Also assign the scope selection tag isp2-cm-tag

Step 7 Enable client class processing from the scope-selection-tag window

Overlapping address ranges cannot be configured on these subinterfaces because software gleans the DHCP reply to figure out the subinterface it really belongs to. Although CNR can be configured with overlapping address range scopes, it cannot be used to allocate addresses from these scopes.

Additional References

The following sections provide references related to Cisco Network Registrar for use with the Cisco CMTS routers.

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