Advanced DOCSIS Set-Top Gateway Application Guide

For System Release 3.5 and 4.0

Please Read

Important

Please read this entire guide. If this guide provides installation or operation instructions, give particular attention to all safety statements included in this guide.

Notices

Trademark Acknowledgments

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at **www.cisco.com/go/trademarks**.

DOCSIS is a registered trademark of Cable Television Laboratories, Inc.

Other third party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

Cisco Systems, Inc. assumes no responsibility for errors or omissions that may appear in this publication. We reserve the right to change this publication at any time without notice. This document is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in this document employs an invention claimed in any existing **or** later issued patent.

Copyright

Contents

About This Guide

Introduction

This application guide is specific to the operation of the Digital Broadband Delivery System (DBDS) network in an Advanced DOCSIS®* Set-top Gateway (ADSG) environment. This application guide provides the guidelines for configuring the DBDS for ADSG when single flow multicast (SFM) is enabled on the Digital Network Control System (DNCS).

** Data-Over-Cable Service Interface Specification*

Purpose

This guide provides guidelines and sample configurations for setting up your overall system and for configuring the DNCS for SFM in an ADSG environment. This document includes instructions for enabling ADSG within a given cable system.

Scope

The content of this document applies to sites that are using DNCS System Releases (SRs) 3.5 and 4.0. This document provides high-level information that applies to the configuration of the DBDS network, including the cable modem termination system (CMTS), for ADSG. This guide provides sample configurations; however, it does not include installation or troubleshooting procedures for ADSG.

Audience

This guide is written for the following personnel involved in setting up and operating a DBDS in an ADSG environment:

- DBDS and DNCS system administrators and operators
- IT system administrators
- Cisco Services engineers
- Call-center personnel

Related Publications

You may find the following publications useful as resources when you implement the procedures in this document. Check the copyright date on your resources to assure that you have the most current version. The publish dates for the following documents are valid as of this printing. However, some of these documents may have since been revised:

- *Digital Network Control System Online Help (PC) Version 3.5.0.3* (part number 4002881, published February 2005, released November 2005*)
- *DOCSIS Set-top Gateway (DSG) Specification*, CM-SP-DSG-I03-041124, (Available at www.cablelabs.com)
- *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems, RFC 2669* (Available at www.ietf.org)
- *Dynamic Host Control Protocol, RFC-2131*, (Available at www.ietf.org)
- *Host Extensions for IP Multicasting, RFC 1112* (Available at www.ietf.org)

* The SR 3.5 and 4.0 versions of the DNCS include online Help which you can access from the DNCS. However, if you would like to order a CD of the online Help separately, you can order the following PC version:

Digital Network Control System Online Help (PC) Version 3.5.0.3 (part number 4002881, published February 2005, released November 2005)

Document Version

This is the fourth release of this guide. In addition to minor text and graphic changes, the following table provides the technical changes to this guide.

Description	See Topic
Updated GUI and procedure for setting up ADSG in a single flow multicast environment	***DNCS Configuration for SFM*** (on page 4)

1

Assumptions About Your System

Introduction

This chapter includes assumptions that Cisco has made concerning your overall system. Use these assumptions only as a guideline when configuring your DBDS network for ADSG.

Important! The IP addresses used in this document are only examples. Cable service providers should determine their own IP addressing scheme.

In This Chapter

Assumptions

Cisco makes the following assumptions in respect to your overall system:

- All servers, including the DNCS, are connected to the headend router through Ethernet.
- In a private network scenario, DBDS network elements use the 172 network (172.16.0.0 - 172.31.255.255) and the 192 network (192.168.0.0 - 192.168.255.255).
- In a private network, the "entire 10 network" (10.0.0.0 - 10.255.255.255) is dedicated to end-user devices.
- The service provider will not use any subnets from the "private 10" network IP addresses that are currently used by existing DHCTs and DBDS network elements. This will eliminate any IP address conflicts.
- The network supports multicasting.
- The CMTS software supports ADSG.
- The DNCS release supports multicast and is streaming multicast traffic to the CMTS while it continues to unicast traffic to the existing quadrature phase shift key (QPSK) modulators, provided that each CMTS and QPSK modulator is defined as an out-of-band (OOB) bridge. Only a CMTS is interested in the multicast traffic streamed by the DNCS.
- The DHCP servers must implement the specifications as provided in *Dynamic Host Control Protocol, RFC 2131, March 1997*.
- The term DHCT CPE (customer premise equipment) is equivalent to eSTB (embedded set-top box). All current and planned ADSG-capable software images for Cisco based platforms (eSTB) will only operate in ADSG mode; therefore, ADSG-capable software images will not fall back to DAVIC (Digital Audio Visual Counsel).

2

Guidelines for Configuring DBDS

Introduction

This chapter provides guidelines to help you configure the DBDS network to support DSG in an environment where the DNCS is streaming out-of-band data when enabled for SFM. In this environment, the CMTS is configured for Advanced DSG (ADSG) mode.

In This Chapter

DNCS Configuration for SFM

DNCS Overview

This section provides guidelines for configuring SFM on the DNCS. Prior to configuring SFM, please note the following definitions within this document concerning a logical CMTS bridge and a physical CMTS device:

- A logical CMTS bridge refers to the "logical" model of the CMTS bridge as configured and maintained on the DNCS GUI.
- A physical CMTS device refers to the physical CMTS hardware that resides in the headend or hub of a given cable system.
- The relationship between the DNCS GUI-configured logical CMTS bridge and the actual physical CMTS device is such that the logical CMTS bridge *may* represent one or many physical CMTS devices.

The SFM IP address is used by the DNCS to send out-of-band data to all DHCTs. A single multicast address (referred to as single-flow multicast) is entered for each set of out-of-band data that is sent to a logical CMTS bridge. Many physical CMTS devices may be configured to join a given set of out-of-band data.

A set of out-of-band data in an SFM environment comprises all out-of-band data using the same multicast Internet protocol (IP) address. The out-of-band data consists of the following message types:

- Out-of-band BFS data carousels
- UNConfigIndication (UNCI) messages
- UNPassThru (PT) messages
- System information (SI)
- Conditional access (CA) information

Note: These types of out-of-band data are distinguished by destination UDP ports.

Configure SFM on the DNCS

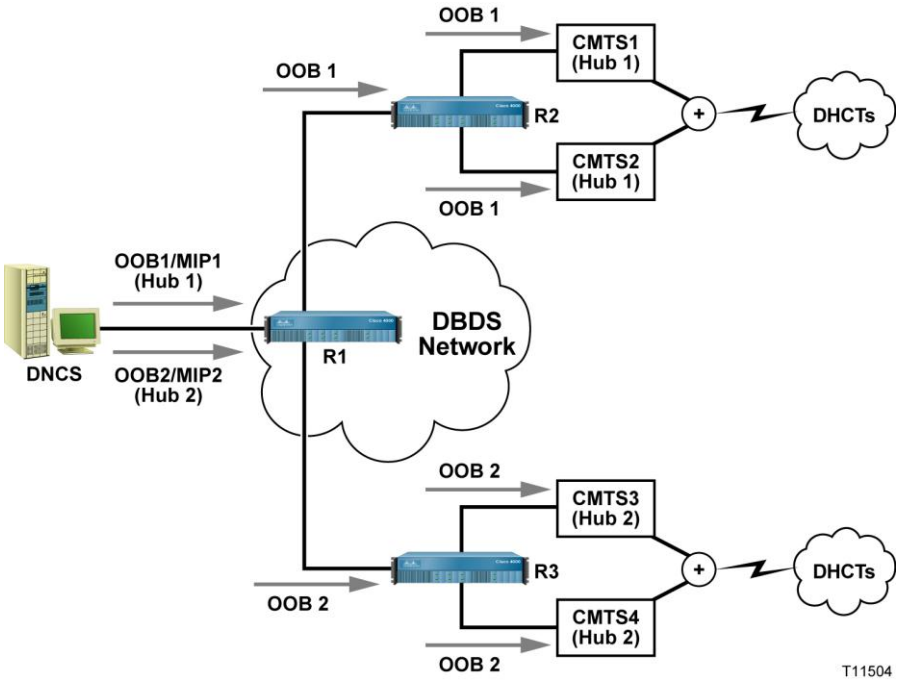
When configuring SFM on the DNCS, a single multicast address is entered for each CMTS bridge. When organizing and defining CMTS bridges, consider the following relationships:

- **CMTS Bridge and FIPS Code Area:** Typically, only one CMTS bridge is required for each hub. However, the system operator should ensure that a given CMTS does not include more than one Federal Information Processing Standards (FIPS) code area. This means that the system operator should maintain a relationship of one CMTS bridge per FIPS code area. This could result in more than one CMTS bridge defined per hub.
- **Hubs, CMTS Bridges, and Channel Lineups:** The DBDS associates channel lineups with hubs. The DBDS also associates at least one CMTS bridge per hub; therefore, there is at least one bridge per hub. It is important that the system operator determine the relationship between CMTS bridges and the hubs they belong to in order to properly configure SFM on the DNCS.

As a final configuration task, the system operator should identify each physical CMTS device that is associated with the logical CMTS bridge modeled on the DNCS.

Note: For the remainder of this section, only one logical CMTS bridge is assumed. This means that one multicast IP address is provisioned for each defined hub.

The following diagram illustrates how the DNCS transmits out-of-band data to each multicast address.



Using the Existing DNCS Interface for SFM

Introduction

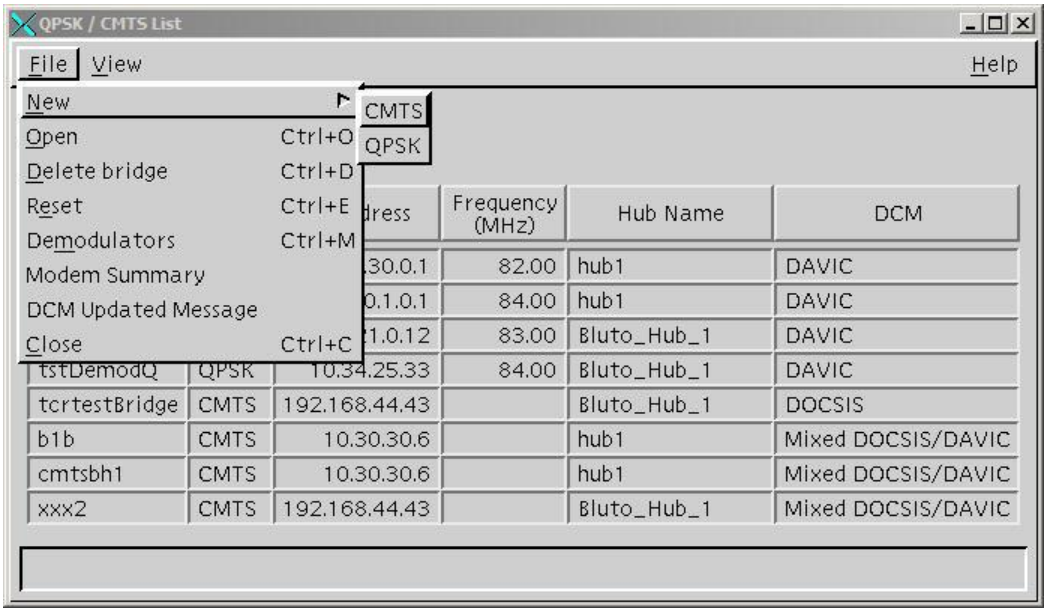
Using the DNCS GUI, a system operator will setup a CMTS and a CMTS bridge to provision a SFM IP address for a set of out-of-band data that is destined to a specific bridge. The system operator must provide the following information on the GUI interface:

- A hub to associate with the bridge
- A bridge name
- An IP flow scheme defined as SFM
- The name and IP address of the CMTS hosting the bridge (the presence of this field is dependent upon the DNCS software version)
- A multicast IP address
- A DHCT Communication Mode (DCM) defined as DOCSIS for set-tops that are using DSG; a DCM setting of DAVIC for set-tops that are not using DSG

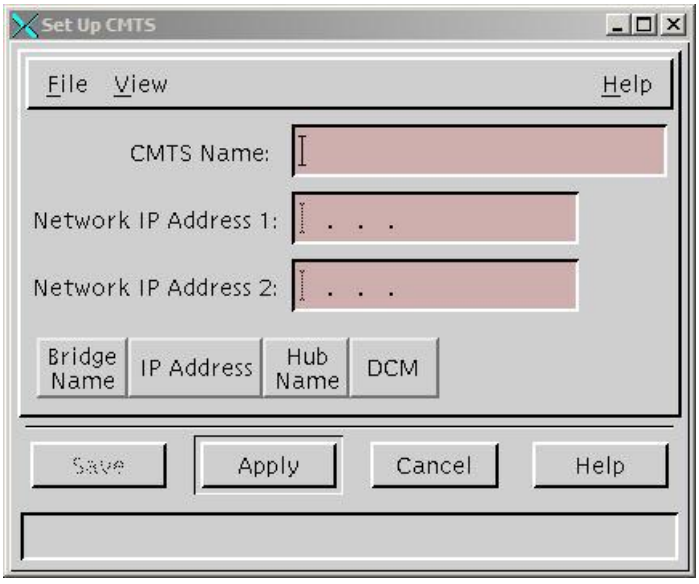
After the DNCS is configured, it starts sending out each out-of-band message type using a multicast destination IP address that was provided by the system operator. If a group of CMTSs share the same out-of-band traffic, the system operator must only provision one multicast IP address on the DNCS GUI.

Configuring SFM on the DNCS

1 From the DNCS Administrative Console, click **Element Provisioning** and then click **QPSK/CMTS**. The QPSK/CMTS List window opens.



2 From the File menu, click **New** and select **CMTS**. The Set Up CMTS window opens.



3 Click in the CMTS Name field and enter a name to describe the CMTS.

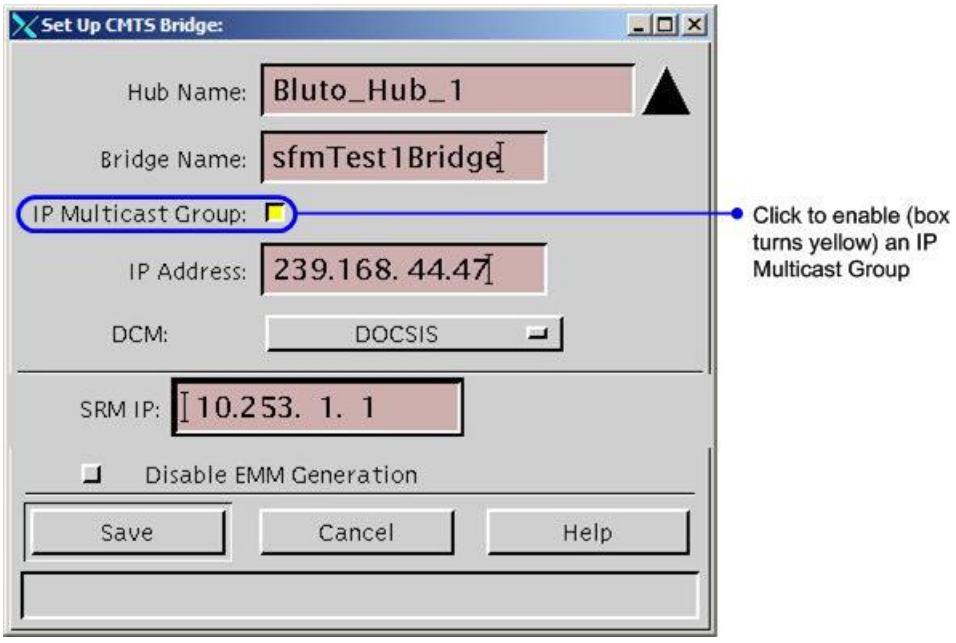
4 Click in the Network IP Address 1 field and enter the IP address for the CMTS chassis.

Important! When entering this address, make certain that the address is unique and is outside of the range of IP addresses reserved for multicasting. Network IP addresses have no bearing on operation and are for information only.

Note: It is not necessary to enter a second IP address in the Network IP Address 2 field. However, you may enter one if you wish. If you do enter a second IP address, make certain that it is unique and is outside the range of addresses reserved for multicasting.

5 Click **Apply**. The DNCS saves this information and a message at the bottom of the Set Up CMTS window prompts you to add bridges to the CMTS chassis.

6 From the Set Up CMTS window, click the **File** menu, choose **New**, and select **CMTS Bridge**. The Set Up CMTS Bridge window opens.



7 Click the Hub arrow and select the hub to which the CMTS bridge is connected.

Note: If needed, you can assign a different hub to each CMTS bridge.

8 Click in the **Bridge Name** field and enter a name for the bridge.

9 Click the **IP Multicast Group** option. The option is enabled when the selection box is yellow in color.

10 Click in the **IP Address** field and enter an IP address for this bridge that is unique and is within the range of IP addresses reserved for multicasting.

Note: The range of IP addresses 224.0.0.0 to 239.255.255.255 is reserved for multicasting. The range of IP addresses 239.192.0.0 to 239.251.255.255 is the local administrative range of IP addresses reserved for multicasting and is recommended.

11 Click the **DCM** option and select **DOCSIS**.

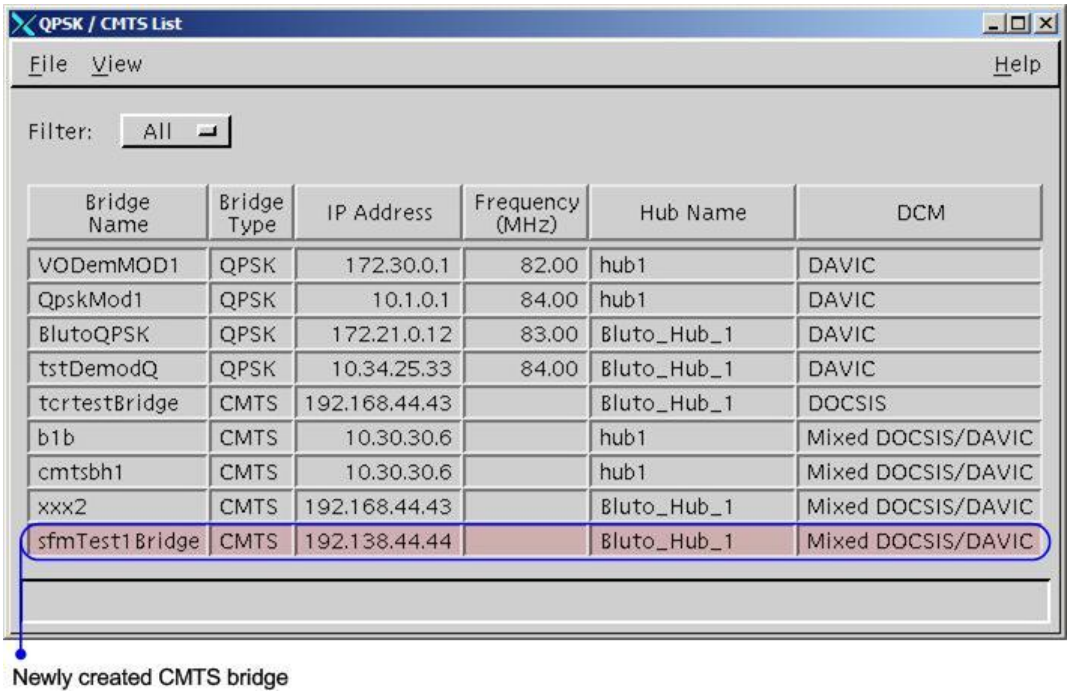
12 Click in the **SRM IP** field and enter the IP address of the Session Resource Manager (SRM).

Note: Refer to your network map to determine the IP address of the SRM.

13 If a vendor other than Cisco provides your conditional access system, click the **Disable EMM Generation** option to disable Cisco's PowerKEY EMMs.

Note: When disabling PowerKEY EMMs, DHCTs that have signed on and reported the ID for the CMTS bridge will not receive PowerKEY EMMs. In addition, new EMMs will not be generated for any DHCTs associated with the CMTS bridge.

14 Click **Save**. The Set Up CMTS Bridge window closes, and the CMTS bridge is listed in the Set Up CMTS window.



15 Do you need to set up another CMTS bridge for this CMTS?

- If **yes**, for each new bridge that you want to add to the DNCS, repeat steps 6 to 14.
- If **no**, you have successfully set up all the CMTS bridges for this CMTS chassis. From the File menu, click **Close** to close the Set Up CMTS window.

16 Do you want to set up another CMTS and its bridges?

- If **yes**, repeat steps 2 to 15 to set up another CMTS chassis and the CMTS bridges for the chassis.
- If **no**, select **File** and click **Close** to close the QPSK/CMTS List window.

CMTS Configuration Overview

Note: Cisco has tested ADSG with a Cisco CMTS; therefore, a Cisco CMTS is assumed throughout this document.

After the DNCS is configured with SFM, you will also need to configure ADSG on the CMTS.

Each CMTS in the system includes a single DSG agent. The DSG agent is configured to map all appropriate Cisco out-of-band IP flows onto the appropriate DOCSIS downstream channels based on the source and destination IP address in the defined classifiers. The DSG agent is configured to send this data to any MAC address that the operator deems appropriate.

Note: The MAC address can be unicast or multicast (*Host Extensions for IP Multicasting, RFC 1112, August 1999*).

The CMTS is configured so that the downstream channel descriptor (DCD) message sent on each DSG channel that is carrying Cisco out-of-band flows contains necessary rules and classifiers. These rules and classifiers identify the availability and location (within that DSG channel) of the out-of-band flows for the Cisco DSG clients.

The DHCT does not have prior knowledge of the DSG tunnel address when it is searching for the appropriate DOCSIS downstream. Instead, the DHCT parses the DCD message and determines which, if any, Cisco DSG clients (client IDs) are listed in the DCD message. If the required client IDs are listed in the DCD message, the DHCT will remain on the DSG channel to receive the out-of-band data. If the required client IDs are not listed in the DCD message, the DHCT will continue searching for out-of-band data.

CMTS Global Configuration in a Non-Straddle Environment

A "non-straddle environment" is defined as a single DOCSIS RF downstream that covers the DHCT populations that are served by the same hub. The system operator should configure the following criteria in a non-straddle environment:

- DSG tunnels with their respective MAC address
- DSG classifiers that allow the CMTS to route traffic to the appropriate DSG tunnel
- Client lists that are used by the DHCT to pick rules that apply to it

CMTS Interface Configuration

Each interface on the CMTS device that receives multicast traffic must have several customized configurations. These configurations must specifically address the following two scenarios for configuring the CMTS:

- ***Non-Hub Straddling*** (on page 12)
- ***Hub Straddling (Regionalization)*** (on page 16)

The general IP multicast CMTS configurations include the following scenarios:

- Each interface that receives multicast traffic *must* be enabled with Protocol Independent Multicast (PIM).
- RF Interfaces that forward multicast traffic *must* be statically configured using the CMTS to join the Cisco out-of-band multicast groups defined on the DNCS.

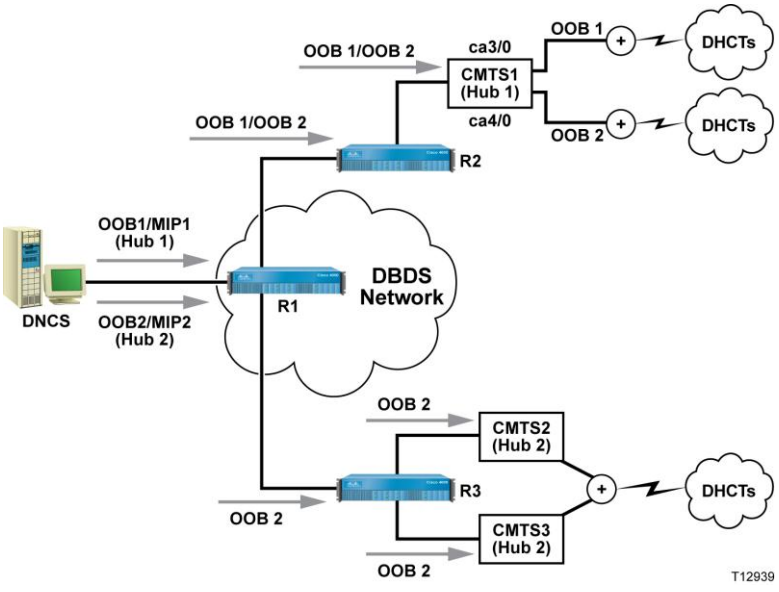
  Note: Some Internetwork Operating Systems (IOS), for example, Cisco, automatically include the "ip igmp static" command when the "cable downstream DSG Rule" is configured. If this occurs for your CMTS, configuring the "ip igmp static" command will *not* be necessary.
- DSG Rules should be configured on the downstreams to which they apply. This will result in a different DCD message sent from each downstream.
- The configuration of a DSG "Classifier" is required. The DSG Classifier enables the DSG agent to map the IP multicast address to the DSG tunnel. If ports are not included in the DSG classifier or if the DSG classifier is not included in the DCD message, the set-top will filter the Cisco DSG data based on existing, well-known port numbers.

Non-Hub Straddling

Non-hub straddling includes the configuration of the CMTS when the CMTS' downstream message traffic is entirely contained within a single hub. When the CMTS message traffic is isolated in this manner, the resulting message traffic is defined as "non-hub straddling" (from a client set-top perspective). When the set-top tunes to receive downstream message traffic, it receives messages that were generated only for the given hub in which the set-top resides. The scenarios in ***Example: Non-Hub Straddling*** (on page 13) address a CMTS in which message traffic is categorized as non-hub straddling.

Notes:

- In the following examples, the first usable IP address is configured as the gateway IP address.
- It is strongly recommended that the service provider prevent DBDS multicast traffic from flowing to the home network by applying MIB filters to stand-alone cable modems. These filters are defined in the *DOCSIS Cable Device MIB Cable Device Management Information Base for DOCSIS compliant Cable Modems and Cable Modem Termination Systems, RFC 2669, August 1999*.
- The following scenarios are only examples. To acquire a more up-to-date sample, refer to your current CMTS configuration.
- The line numbers to the left of the example CMTS configuration scenarios are for illustrative and explanatory purposes only. They are not indicative of actual CMTS device listings.



Example: Non-Hub Straddling

The following list describes various command lines within the example:

- Lines 2-3 define the client list.
- Lines 4-5 define the DSG tunnels.
- Lines 6-7 define the destination IP address and port (classifiers).
- Line 9 defines the interface name.
- Line 10 defines the interface IP address.
- Lines 11, 18, 27, and 52 enable the Protocol Independent Multicast (PIM).
- Lines 30 and 55 statically configure IGMP on the RF interface that forwards IP multicast traffic.
- Lines 31 and 56 enable DCD.
- Lines 32 and 57 specify Rule 1 priority, clients, and tunnel for this downstream interface.
- Line 33 and 58 specify Rule 1 classifiers for this downstream interface.

```
1   ip multicast-routing
2   cable dsg client-list 1 id-index 1 mac-addr 0001.a6d0.0b1e
3   cable dsg client-list 1 id-index 2 ca-system-id E00
4   cable dsg tunnel 1 mac-addr 0100.5e40.0104
5   cable dsg tunnel 2 mac-addr 0100. 5e40.0105
6   cable dsg cfr 1 dest-ip 239.192.1.4 tunnel 1 dest-port 2000 13821 priority 0
    src-ip 10.253.0.1
7   cable dsg cfr 2 dest-ip 239.192.1.5 tunnel 2 dest-port 2000 13821 priority 0
    src-ip 10.253.0.1
8   !
9   interface FastEthernet0/0
10  ip address 10.200.16.1 255.255.255.0
11  ip pim sparse-dense-mode
12  ip mroute-cache
13  duplex full
14  no keepalive
15  !
16  interface FastEthernet1/0
17  ip address 10.100.16.205 255.255.192.0
18  ip pim sparse-dense-mode
```

```
19  ip mroute-cache
20  duplex full
21  no keepalive
22  !
23  interface Cable3/0
24  ip address 10.32.40.1 255.255.248.0 secondary
25  ip address 10.0.40.1 255.255.248.0
26  ip helper-address 10.100.16.13
27  ip pim sparse-dense-mode
28  cable dhcp-giaddr policy
29  ip dhcp relay information option
30  ip igmp static-group 239.192.1.4
31  cable downstream dsg dcd-enable
32  cable downstream dsg rule 1 priority 1 clients 1 tunnel 1
33  cable downstream dsg rule 1 classifiers 1
34  ip mroute-cache
35  cable insertion-interval 500
36  cable downstream annex B
37  cable downstream modulation 64qam
38  cable downstream interleave-depth 32
39  cable downstream frequency 723000000
40  cable downstream channel-id 0
41  cable upstream 0 frequency 30000000
42  cable upstream 0 power-level 2
43  cable upstream 0 channel-width 200000
44  cable upstream 0 minislot-size 64
45  cable upstream 0 modulation-profile 6
46  no cable upstream 0 shutdown
47  !
48  interface Cable4/0
49  ip address 10.20.48.1 255.255.248.0 secondary
50  ip address 10.40.48.1 255.255.248.0
51  ip helper-address 10.100.16.13
52  ip pim sparse-dense-mode
53  cable dhcp-giaddr policy
```

```
54  ip dhcp relay information option
55  ip igmp static-group 239.192.1.5
56  cable downstream dsg dcd-enable
57  cable downstream dsg rule 1 priority 1 clients 1 tunnel 2
58  cable downstream dsg rule 1 classifiers 2
59  ip mroute-cache
60  cable insertion-interval 500
61  cable insertion-interval 500
62  cable downstream annex B
63  cable downstream modulation 64qam
64  cable downstream interleave-depth 32
65  cable downstream frequency 729000000
66  cable downstream channel-id 0
67  cable upstream 0 frequency 10000000
```

Hub Straddling (Regionalization)

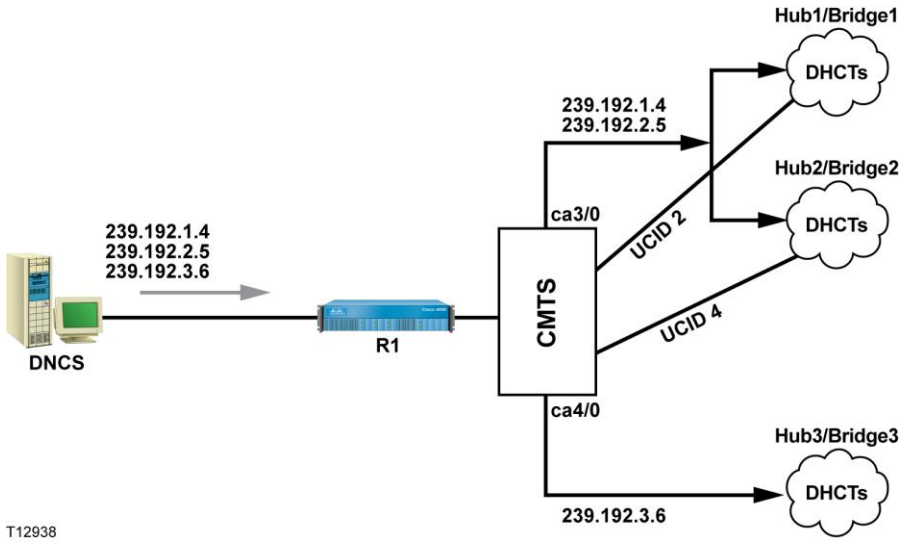
This section describes the second CMTS configuration option in which the downstream message traffic from the CMTS is not entirely contained within a single hub. When CMTS message traffic is not isolated to a single hub, the resulting message traffic is defined as "hub straddling" (from a client set-top perspective). When the set-top tunes to receive downstream message traffic, it can potentially receive messages that were generated for more than the single given hub in which the set-top box resides.

Go to ***Example: Hub Straddling*** (on page 17) to see an example that addresses a CMTS in which message traffic is categorized as hub straddling. In this case, the DCD rules define the hub data in which the set-top will use.

The DCD data is described as follows. As mentioned in the ***DNCS Overview*** (on page 4), a set of DSG data in an SFM environment comprises all out-of-band data (BFS, CA, PT, SI, and UNCI message types). This out-of-band data utilizes the same multicast IP address. Each set of DSG data on a given DSG channel is associated with a unique upstream channel ID or a set of upstream channel IDs. The CMTS device is configured such that the DCD rules associated with a set of DSG data is marked with the UCIDs of the associated upstream channels. When a DOCSIS two-way connection is achieved, the set-top selects the correct DCD rules to use and, consequently, receives the correct set of DSG data. To help clarify this concept, see ***Example: Hub Straddling*** (on page 17).

Notes:

- Set-tops that reside in a hub must have their upstream channels connected to the same upstream ports.
- The UCID range always starts with one (1) even though the labeling of the physical upstream cable interface on some CMTS vendors starts with zero (0). In other words, for set-tops connected to "US0," their corresponding UCID is one (1).



Example: Hub Straddling

The following list describes various command lines within the example:

- Lines 2-3 define the client list.
- Lines 5-7 define the DSG tunnels.
- Lines 9-11 define the destination IP address and port (classifiers).
- Lines 15, 22, 31, and 61 enable the Protocol Independent Multicast (PIM).
- Lines 34, 35, 64, and 65 statically configure IGMP on the RF interface that forwards IP multicast traffic.
- Lines 36 and 65 enable DCD.
- Lines 37 to 39 define the DSG rule with priority, clients, tunnel, UCID, and classifiers for hub #1.
- Lines 40 to 42 define the DSG rule with priority, clients, tunnel, UCID, and classifiers for hub #2.
- Lines 66 and 67 define the DSG rule with priority, clients, tunnel, UCID, and classifiers for hub #3.

```
1   ip multicast-routing
2   cable dsg client-list 1 id-index 1 mac-addr 0001.a6d0.0b1e
3   cable dsg client-list 1 id-index 2 ca-system-id E00
4   !
5   cable dsg tunnel 1 mac-addr 0100.5e40.0104
6   cable dsg tunnel 2 mac-addr 0100.5e40.0205
7   cable dsg tunnel 3 mac-addr 0100.5e40.0306
8   !
9   cable dsg cfr 1 dest-ip 239.192.1.4 tunnel 1 dest-port 2000  13821 priority 0
    src-ip 10.253.0.1
10  cable dsg cfr 2 dest-ip 239.192.2.5 tunnel 2 dest-port 2000  13821 priority 0
    src-ip 10.253.0.1
11  cable dsg cfr 3 dest-ip 239.192.3.6 tunnel 3 dest-port 2000  13821 priority 0
    src-ip 10.253.0.1
12  !
13  interface FastEthernet0/0
14  ip address 10.200.16.1 255.255.255.0
15  ip pim sparse-dense-mode
16  ip mroute-cache
17  duplex full
```

```
18  no keepalive
19  !
20  interface FastEthernet1/0
21  ip address 10.100.16.205 255.255.192.0
22  ip pim sparse-dense-mode
23  ip mroute-cache
24  duplex full
25  no keepalive
26  !
27  interface Cable3/0                          (STRADDLE CONFIGURED
                                                 ON THIS DOWNSTREAM)
28  ip address 10.32.40.1 255.255.248.0 secondary
29  ip address 10.0.40.1 255.255.248.0
30  ip helper-address 10.100.16.13
31  ip pim sparse-dense-mode
32  cable dhcp-giaddr policy
33  ip dhcp relay information option
34  ip igmp static-group 239.192.1.4
35  ip igmp static-group 239.192.2.5
36  cable downstream dsg dcd-enable
37  cable downstream dsg rule 1 priority 1 clients 1 tunnel 1
38  cable downstream dsg rule 1 ucid 2
39  cable downstream dsg rule 1 classifiers 1
40  cable downstream dsg rule 2 priority 1 clients 1 tunnel  2
41  cable downstream dsg rule 2 ucid 4
42  cable downstream dsg rule 2 classifiers 2
43  ip mroute-cache
44  cable insertion-interval 500
45  cable downstream annex B
46  cable downstream modulation 64qam
47  cable downstream interleave-depth 32
48  cable downstream frequency 723000000
49  cable downstream channel-id 0
50  cable upstream 0 frequency 30000000
51  cable upstream 0 power-level 2
```

```
52  cable upstream 0 channel-width 200000
53  cable upstream 0 minislot-size 64
54  cable upstream 0 modulation-profile 6
55  no cable upstream 0 shutdown
56  !
57  interface Cable4/0                          (NO STRADDLE CONFIGURED
                                                ON THIS DOWNSTREAM)
58  ip address 10.20.48.1 255.255.248.0 secondary
59  ip address 10.40.48.1 255.255.248.0
60  ip helper-address 10.100.16.13
61  ip pim sparse-dense-mode
62  cable dhcp-giaddr policy
63  ip dhcp relay information option
64  ip igmp static-group 239.192.3.6
65  cable downstream dsg dcd-enable
66  cable downstream dsg rule 1 priority 1 clients 1 tunnel 3
67  cable downstream dsg rule 1 classifiers 3
68  ip mroute-cache
69  cable insertion-interval 500
70  cable insertion-interval 500
71  cable downstream annex B
72  cable downstream modulation 64qam
73  cable downstream interleave-depth 32
74  cable downstream frequency 729000000
75  cable downstream channel-id 0
```

ADSG DHCT Initialization

Introduction

The DHCT does not have prior knowledge of the DSG tunnel address as it searches for the appropriate DOCSIS downstream channel. For this reason, the DCD message is used to retrieve parameters that can identify the location of the DSG tunnels.

DHCTs can also receive DSG data without establishing an interactive communications path with the CMTS. This allows the DBDS to support ADSG DHCTs in a one-way operating environment.

Out-of-Band Flow and the DOCSIS Downstream

As part of its initialization, the DHCT searches the DOCSIS spectrum until it locates a downstream channel that is carrying a DCD message. The DHCT parses the DCD message and determines which, if any, client IDs are listed in the DCD message. The DHCT requires that the Cisco client ID (for example, mac-addr 0001.a6d0.0b1e) be listed in the DCD for it to remain on the DSG channel and discover the DSG tunnel addresses for receiving out-of-band data. If the required Cisco client ID is not listed in the DCD, the DHCT will continue its out-of-band data search. Once the DHCT locates a valid DSG channel, it remains on that channel and continuously receives out-of-band data (for example, DSG data). The DHCT then attempts to register with the CMTS.

If the DHCT supports PowerKEY conditional access (CA), the DHCT uses the CA ID to receive CA data (for example, ca-system-id E00). In order to ensure proper orientation of the Cisco DHCTs that support PowerKEY CA, rules contain both clients IDs (for example, mac-addr 0030001.a6d0.0b1e and ca-system-id E00), which must be configured on the CMTS.

If a straddle area exists (for example, UCID-based rules), the DHCT accomplishes the following tasks:

- Parses the DCD message
- Achieves a DOCSIS two-way connection
- Selects the correct rules to use based on its assigned UCID during DOCSIS registration

Loss of the DSG Data on a DSG Channel

When a DHCT is operating in ADSG mode, the initialization sequence differs from the sequence used with a standard DOCSIS cable modem. In the ADSG mode, the DHCT responds differently to the following values and conditions:

- Timeouts
- Error conditions

In ADSG, the DHCT uses the configurable timer values as specified in the DCD message. When the out-of-band data is no longer present on the downstream channel, the DHCT monitors the current downstream DOCSIS frequency until the combined value of Tdsg2 and Tdsg4 is reached. The DHCT then scans the entire DOCSIS spectrum until it finds a DOCSIS signal that is carrying DSG data.

Loss of the DOCSIS Upstream Channel

When a DHCT is operating in ADSG mode and loses its DOCSIS upstream channel, the DHCT starts the Tdsg3 timer and remains tuned to the DOCSIS downstream channel that contains out-of-band data. The DHCT continues to receive DSG data on the downstream channel regardless of two-way capabilities. When the Tdsg3 timer expires, the DHCT tries to reacquire the upstream channel and establish two-way connectivity. If the DBDS broadcast data becomes unavailable on the DOCSIS downstream channel, the DHCT resumes downstream scan after a Tdsg2 +Tdsg4 timeout.

Server Configurations

Introduction

This section provides guidelines for configuring the server components for a DBDS network using DOCSIS:

- Mandatory DOCSIS 1.0 servers
  - Dynamic host configuration protocol (DHCP) server
  - Trivial file transfer protocol (TFTP) server
- Optional servers
  - Time of day (TOD) server
  - Domain naming system (DNS) server

Mandatory DOCSIS 1.0 Servers

This section describes the DHCP and TFTP server configurations are required to operate DOCSIS on the DBDS. To configure a DBDS network in a DSG environment, you must configure the following servers:

- DHCP server
- TFTP server

For the purpose of this example, Cisco assumes that the service providers have already deployed the servers identified in this section for their high-speed data service. The service providers are responsible for deploying and configuring their servers.

DHCP Server

Unique scope must be configured on the DHCP server for the eCM and the eSTB.

During manufacturing, DHCTs are configured with both an RF MAC address and an Ethernet MAC address. The DOCSIS cable modem uses the Ethernet MAC address and the DHCT CPE uses the RF MAC address. System administrators should be aware of these MAC addresses if they will be provisioned on the DHCP server.

The DHCT server is a required server that provides IP addresses for the embedded cable modem (eCM) and the embedded set-top box (eSTB). The following table allows the operator to appropriately configure their DHCP servers to recognize DHCP messages that originate from the eCM and the eSTB.

Note: You can use the same DHCP server that is used for your existing stand-alone cable modems.

Opt. #	Subopt	Description	Data Source for eCM	Data Source for eSTB
0	—	Pad option data	X	X
43	—	Vendor specific information in sub-options	X	X
	1	Client requested server sub-options list (n=0)	Hardcoded: null string	Hardcoded:null string
	2	STB or ECM	Hardcoded: "ECM"	Hardcoded:"ECM"
	3	Colon delimited list of embedded eSAFE devices (e.g., ECM:ESTB)	Hardcoded: "ECM ESTB"	Hardcoded:"ECM:ESTB"
	4	Device serial number also in MIB object docsDevSerialNumber (e.g.,SABHRCHRN)	NVM:kNvm_DeviceSerialNumber	NVM:kNvm_DeviceSerialNumber
	5	Hardware version number from <Hardware version> field also in MIB object sysDescr (e.g., 0000000A)	NVM:kNvm_HWConfigNumber	NVM:kNvm_HWConfigNumber
	6	Software version number from <Software version> field also in MIB object sysDescr (e.g., 6.10.0.9)	Hardcoded	Unified image version number (component 0)

Opt. #	Subopt	Description	Data Source for eCM	Data Source for eSTB
	7	Boot ROM version number from <Boot ROM version> field also in MIB object sysDesc (e.g., 81F4009E)	Bootloader: kBldr_SiVersion	Bootloader:kBldr_SiVersion
	8	6-octet OUI as Vendor Identifier (e.g., 000002DE)	NVM:kNvm_OUI	NVM:kNvm_OUI
	9	Device model number from <Model number> field also in MIB object sysDescr (e.g., 0000206C)	NVM:kNvm_HWModelNumber	NVM:kNvm_HWModelNumber
	10	Vendor name from <Vendor name> field also in MIB object sysDescr	Hardcoded	Hardcoded
	11	Set-top capability using the encoding format per OpenCable CFR specification. Since there is no standard or required capability identification, the vendor must provide documentation on the supported capability	reserved	Hardcoded : "0500"
	15	Conditional Access System vendor-specific device identification, which is the eSTB RF MAC address as a displayable string w/o colons or dashes (e.g. '0002DE0ABEF0')	reserved	Bootloader: kBldr_RFMACAddress
50	—	Client requested IP address	X	X
51	—	Client IP address lease time in seconds	X	X
53	—	DHCP message type	X	X
54	—	DHCP server identifier IP address	eCM requested server id IP @ request	eCM requested server id IP @ request

Opt. #	Subopt	Description	Data Source for eCM	Data Source for eSTB
55	—	Client requested Server options list (e.g., 1 3 6 7 15 23 43 50 51 54)	code 1: subnetMask code 2: timerOffset code 3: routersOnSubnet code 4: timeServer code 7: logServer	code 1: subnetMask code 2: timerOffset code 3: routersOnSubnet code 4: timeServer code 7: logServer
60	—	Vendor Class identifier (e.g., DSG1.0)	Hardcoded: "docsis1.0"	Hardcoded:"DSG1.0"
61	—	Client-identifier, 1-byte hardware type plus 6-byte MAC address	Ethernet h/w type(i.e. 1) and eCM MAC address	Ethernet h/w type(i.e. 1) and eSTB MAC address
255	—	End of option data	X	X

TFTP Server

The same TFTP server that you currently use for stand-alone cable modems can also be used for integrated cable modems. However, the integrated cable modems may require a different set of SNMP filters than the stand-alone cable modem.

Optional Servers

In addition to the servers required for the DBDS network that is using DOCSIS, you may also configure your TOD and DNS servers, if used.

TOD Server

The TOD server provides a timestamp for logged DOCSIS events. The service provider may use the same TOD server for both their integrated cable modems and their stand-alone cable modems. However, a TOD server is not required for integrated cable modems. The DHCT CPE does not use a TOD server.

DNS Server

The DNS server resolves names to IP addresses. It is not required for DHCT CPE.

3

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

Access your company's extranet site to view or order additional technical publications. For accessing instructions, contact the representative who handles your account. Check your extranet site often as the information is updated frequently.

Index

Cisco Systems, Inc.
5030 Sugarloaf Parkway, Box 465447
Lawrenceville, GA 30042

678 277-1120
800 722-2009
www.cisco.com

June 2012 Printed in USA

Part Number 4004619 Rev D