DOCSIS in a DBDS Environment

Please Read This Entire Guide

Important

Please read this entire guide. Give particular attention to all security and safety statements.

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 Laboratoris, 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

Chapter 2 Guidelines for Configuring the DBDS for DOCSIS

Disclaimer

Security Guidelines Disclaimer for Implementing DOCSIS in the DBDS

THE DBDS DOCSIS NETWORK SECURITY GUIDELINES ARE PROVIDED "AS IS, WHERE IS, WITH ALL FAULTS." THERE ARE NO WARRANTIES, WHETHER EXPRESS OR IMPLIED, WITH RESPECT TO THE GUIDELINES OR ANY OF THE INFORMATION PROVIDED THEREIN, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. CISCO DOES NOT WARRANT THAT THE FUNCTIONS DESCRIBED IN THE SECURITY GUIDELINES WILL MEET THE USER'S REQUIREMENTS OR THAT THE OPERATION OF ANY EQUIPMENT OR SOFTWARE PURSUANT TO THE SECURITY GUIDELINES SET FORTH WILL BE UNINTERRUPTED OR ERROR-FREE. CISCO MAKES NO WARRANTY OF NON-INFRINGEMENT, EXPRESS OR IMPLIED. THE USER OF THE SECURITY GUIDELINES ACKNOWLEDGES ITS RESPONSIBILITY TO USE ALL REASONABLE METHODS TO PROVE OUT AND THOROUGHLY TEST THE OPERATION OF THE DBDS DOCSIS SECURITY AND ALL OUTPUTS FROM THE DBDS PRIOR TO ITS USE IN THE USER'S OPERATIONS. IN NO EVENT SHALL CISCO BE LIABLE TO USER FOR LOSS OF PROFITS, INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, PUNITIVE OR EXEMPLARY DAMAGES ARISING OUT OF OR IN CONNECTION WITH THE USE OF THE SECURITY GUIDELINES OR ANY ACTS OR OMISSIONS ASSOCIATED THEREWITH, WHETHER SUCH CLAIM IS BASED ON BREACH OF WARRANTY, CONTRACT, TORT OR OTHER LEGAL THEORY AND REGARDLESS OF THE CAUSE OF SUCH LOSS OR DAMAGE OR WHETHER ANY OTHER REMEDY PROVIDED HEREIN FAILS.

About This Guide

Introduction

Cisco® has designed the Explorer® Digital Home Communication Terminal (DHCTs) 4200 Home Gateway to include the new Data-Over-Cable Service Interface Specifications (DOCSIS®) cable modem. With its integrated DOCSIS cable modem, the DHCT can serve as a gateway that can provide high-speed Internet access to a computer.

The cable modem interoperates with a CableLabs®-qualified DOCSIS 1.0 and 1.1 Cable Modem Termination System (CMTS). The modem provides broadband network operators with a cost-effective way to offer standards-based, high-speed data services to their subscribers. The Explorer 4200 Home Gateway supports DOCSIS 1.0.

Purpose

This application guide describes how you can set up DOCSIS in your Cisco digital cable network, also known as your Digital Broadband Delivery System (DBDS). This guide provides guidelines for provisioning DOCSIS and recommendations for updating the security of your DBDS network. You will learn about DOCSIS-capable DHCTs and their three modes of operation. In addition, you will learn about the network interfaces such as the CMTS, Dynamic Host Control Protocol (DHCP) server, QAM modulators, and QPSK modulators and demodulators that are used to support DOCSIS in a DBDS environment. Information is provided to help you set up the network interfaces within the DBDS so that the Digital Network Control System (DNCS) communicates with the DOCSIS-capable DHCTs.

Audience

This guide is written for DNCS operators, billing system operators, and IT system administrators. The operators or administrators must already be knowledgeable in general DBDS operation and functionality, CMTS, and DHCP server operation and functionality, as well as network addressing and subnetting schemes.

Scope

This guide covers the following topics:

- An introduction to DOCSIS in a DBDS environment and a brief description of the different DOCSIS operation modes
- Network guidelines for provisioning DOCSIS-capable DHCTs
- Security recommendations for the DBDS network in a DOCSIS environment
- Configuring Mixed DOCSIS/DAVIC on the DNCS
- Staging DOCSIS-capable DHCTs
- Setting Up a Home Network
- Frequently Asked Questions

System Requirements

To use a DOCSIS-capable Explorer 4200 Home Gateway, your DBDS must be operating with the following minimum software versions:

- System Release (SR) 3.0
- Cisco Resident Application (SARA) Client Release 1.41
- PowerTV Home Gateway Edition 1.0

Note: Sites using another vendor's resident application need to contact the vendor for their version of DOCSIS-compatible operating system and resident application.

Document Version

This is the second release of this guide.

Chapter 1
Introducing DOCSIS

Overview

Introduction

DOCSIS (Data-Over-Cable Service Interface Specifications) is a standard interface for cable modems that handle incoming and outgoing data signals between a cable service provider and a customer data terminal such as a personal computer (PC). Cisco includes DOCSIS functionality in the Explorer 4200 Home Gateway. The Home Gateway has an integrated cable modem that is compliant with DOCSIS 1.0 specifications. The cable modem provides a high-speed interactive communication path for applications running on external Customer Premise Equipment (CPE), such as PCs connected to the ports of the Home Gateway, as well as the DHCT CPE. The Home Gateway can use either a DOCSIS or DAVIC channel depending upon its communication mode.

Note: This document refers to the Explorer 4200 Home Gateway as a DOCSIS-capable DHCT.

This chapter introduces the communication modes that enable the DHCT to operate in a DOCSIS environment and provides a simplified network diagram of the communication modes. This chapter also describes the interfaces and communication paths that are required to support DOCSIS in a DBDS environment. A simplified diagram of the DBDS architecture that supports DOCSIS is also provided.

Required Hardware and Software

To introduce DOCSIS into the DBDS, cable service providers must install new hardware and software in their network. The following hardware and software are required to support DOCSIS:

- Cable Modem Termination System for DOCSIS 1.0 or higher
- Explorer 4200 Home Gateway
- System Release 3.0 or higher
- Cisco Resident Application (SARA) Client Release 1.41 or later (or similar)
- PowerTV Home Gateway Edition 1.0
- DHCP Server
- Trivial File Transfer Protocol (TFTP) Server
- Time Of Day (TOD) Server (optional)
- Domain Name System (DNS) Server (optional)

In This Chapter

This chapter contains the following topics.

Terminology

List of Terms

The following terms are used in the discussions throughout this guide. Please become familiar with these terms to help you better understand the concepts presented.

Term	Definition
Address Resolution Protocol (ARP)	Address Resolution Protocol is a TCP/IP protocol used to convert an IP address into a physical address, such as an Ethernet address. A host that needs to obtain a physical address can broadcast an ARP request onto the TCP/IP network. The host on the network that has the IP address in the request then replies with its physical hardware address.
A/V services	Analog or digital audio and video services.
Broadcast-only mode	A state in which a DHCT has not established an interactive communications path and only receives broadcast and conditional access (CA) data. Advanced services, such as digital broadcast, Interactive Program Guide (IPG), and Pay-Per-View (PPV), are available to the DHCT in this mode, but Impulse PPV (IPPV) polling and interactive data services do not function in broadcast–only mode.
Cable Modem Termination System (CMTS)	The Cable Modem Termination System is a piece of equipment in the headend that allows cable television operators to offer high-speed Internet access to home computers. The CMTS sends and receives digital cable modem signals on a cable network. The CMTS receives signals sent upstream from a user's cable modem, converts the signals into IP packets, and routes the signals to an Internet service provider for connection to the Internet. The CMTS also can send signals downstream to the user's cable modem. Cable modems cannot communicate directly with each other; they must communicate by channeling their signals through the CMTS.

Term	Definition
Conditional Access (CA) data	Conditional Access data consists of the system, software, and components necessary to provide for selective access or denial of specific services in a network. Establishes a means by which a cable service provider can collect subscriptions or other payments for services received. This data includes event Global Broadcast Authenticated Messages (GBAMs), time-of-day GBAMs, and Entitlement Management Messages (EMMs).
Core DHCT functionality	Core DHCT functionality includes the following functions: • Presentation of analog A/V services • Presentation of clear digital A/V services • Presentation of encrypted digital A/V services, either in subscription, IPPV or Reservation Pay-Per-View (RPPV) forms • Presentation of virtual channel services (VCS) • Presentation of Emergency Alert System (EAS) messages • Presentation of interactive services, including video-on-demand (VOD) • Reception and processing of System Information (SI), Service Application Manager (SAM), and IPG data • Reception and processing of IPPV polling messages
Customer Premise Equipment (CPE)	Customer premise equipment includes any communications equipment that is connected to the telecommunications network and resides on a customer's site.
DAVIC	Standard for broadcast and two-way interactive networking for digital transmission on broadband cable telecommunication systems developed by the Digital Audio Visual Council. See the specification in *Digital Broadband Delivery System: Out Of Band Transport – Mode B*, SCTE DVS 167 Revision 2, March 10, 2000.

Term	Definition
DAVIC-capable only	A DAVIC-capable only DHCT does not have a tuner to support DOCSIS. Cisco's DHCTs prior to the Explorer 4200 DHCT are DAVIC-only. For example, the Explorer 3100 DHCT is DAVIC-only.
DAVIC mode	A communication mode of the DHCT in which all communications (including DBDS broadcast and unicast data) use the DAVIC channel. The DOCSIS channel is not used.
DBDS broadcast data	Data that is broadcast by the DBDS to DHCTs. This data includes UNConfigIndication messages, UNDownload messages, UNPassthru messages, out-of-band conditional access (CA) messages, and out-of-band system information (SI).
Demilitarized Zone (DMZ)	A demilitarized zone is used by a company that wants to host its own Internet services without sacrificing unauthorized access to its private network. The DMZ is located between the Internet and an internal network's line of defense that is a combination of firewalls and bastion hosts. Typically, the DMZ contains devices accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers, and DNS servers.
DHCT Communication Mode (DCM)	The DHCT Communication Mode is the mode that the DHCT uses to communicate with other equipment in the DBDS or DOCSIS environment. The DHCT has three communication modes: • DAVIC • Mixed DOCSIS/DAVIC • DOCSIS
DHCT Customer Premise Equipment	The DHCT CPE is the operating system (OS) and application software components that provide core DHCT functionality. The DHCT CPE is internal to the DHCT.

Terminology, Continued

Term	Definition
Digital Broadband Delivery System (DBDS)	The entire network architecture of Cisco's digital system that ultimately provides signal to and from a subscriber's DHCT. The DBDS consists of five areas: sources, headend, transport network, hub, and access network.
Digital Home Communications Terminal (DHCT)	Cisco's digital set-top converter that is two-way capable for interactive services.
Digital Network Control System (DNCS)	The DNCS is a computer server that is used to monitor and control the DBDS network elements. Generally located at the DBDS headend, although it may be located elsewhere and remotely connected to the DBDS.
DOCSIS	Data-Over-Cable Service Interface Specifications that define interface standards for cable modems and supporting equipment. For more information on DOCSIS, refer to the following specifications: • *Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification* • *Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification* • *Data-Over-Cable Service Interface Specifications Operations Support System Interface Specification* For copies of these specifications, go to the CableLabs web site at the following address: http://www.cablelabs.com/
DOCSIS-capable	The ability to use a DOCSIS channel. For example, the Explorer 4200 DHCT is DOCSIS-capable.
DOCSIS or DSG mode	A DHCT communication mode in which all communications (DBDS broadcast data and unicast data) use the DOCSIS channel. The DAVIC channel is used, if available, as a redundant source of DBDS broadcast data.

Term	Definition
DOCSIS Media Access Control (MAC) domain	Same as MAC-sublayer domain. As defined in the *Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification*, SP-RFI-I06, the DOCSIS MAC-sublayer domain is a collection of upstream and downstream channels for which a single bandwidth allocation and management protocol operates. Within a single DOCSIS MAC-sublayer domain, each service ID (SID) assigned to a cable modem must be unique.
DOCSIS Set-top Gateway (DSG)	Functionality on the CMTS that encapsulates DBDS broadcast data into an Ethernet frame with a well-known Cisco MAC address before sending to the DHCT.
Domain Name System (DNS) Server	The Domain Name System (or Service) is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, you can easily remember them. However, the Internet is based on IP addresses. Whenever you enter a domain name, a DNS server must translate the name into the corresponding IP address.
DSG-capable	The ability in a CMTS to forward DBDS broadcast data through the DOCSIS channel.
Dynamic Host Control Protocol (DHCP)	Dynamic Host Control Protocol (DHCP) is a protocol that allows you to assign dynamic IP addresses to devices on a network. With dynamic addressing, a device can use a different IP address every time it connects to the network.
Element Management System (EMS)	The EMS is an application that runs on a separate workstation within the DBDS to monitor and manage system alarms that occur for hardware devices (network elements) in the DBDS.
Integrated Cable Modem (ICM)	The integrated cable modem (or ICM) is embedded in the Explorer 4200 DHCTs. These DHCTs can use a DOCSIS channel and can be used for high speed data service.

Term	Definition
Internet Control Message Protocol (ICMP)	ICMP is an extension to the Internet Protocol (IP) defined by RFC 792. ICMP supports packets containing error, control, and informational messages. The ping command, for example, uses ICMP to test an Internet connection.
Media Access Control (MAC) Address	The Media Access Control address is a hardware address that uniquely identifies each node of a network.
Mixed DOCSIS/DAVIC-capable	A feature of some models of the DHCT that allows reception of DAVIC out-of-band data while simultaneously using a DOCSIS channel for two-way communication. For example, the Explorer 4200 DHCT is Mixed DOCSIS/DAVIC-capable.
Mixed DOCSIS/DAVIC mode	A communication mode of the DHCT in which DBDS broadcast data is delivered over the DAVIC channel, and unicast data is delivered over the DOCSIS channel
Network Management System (NMS)	A network management system allows you to manage the following areas of your network: • Security: Ensuring that the network is protected from unauthorized users. • Performance: Eliminating bottlenecks in the network. • Reliability: Making sure the network is available to users and responding to hardware and software malfunctions.
Non-DBDS traffic	Any data communications service that does not require interaction with DBDS network elements, for example, PC access to Internet (High Speed Data Service).
Out-of-Band (OOB) Bridge	The OOB bridge refers to the QPSK or CMTS RF MAC domain.
PC CPE	A PC that is connected as CPE behind either a stand-alone cable modem or a DOCSIS-capable DHCT.

Term	Definition
Ping floods	A type of network security breach in which a network connected to the Internet is swamped with replies to ping requests. A smurf attacker sends ping requests to an Internet broadcast address. These are special addresses that broadcast all received messages to the hosts connected to the subnet. Each broadcast address can support multiple hosts, so a single ping request can be multiplied many times. The return address of the request itself is spoofed to be the address of the attacker's victim. All the hosts receiving the ping request reply to this victim's address instead of the real sender's address. A single attacker sending hundreds or thousands of these ping messages per second can flood the victim's network with ping replies and bring the entire network down.
Registered Cable Modem	A cable modem whose MAC address is located in the back-end server database. When the cable modem is registered, it is typically assigned a final Net 10 private IP address.
Service ID (SID)	A unique number assigned by the CMTS to each DOCSIS cable modem. The CMTS and cable modem use the SID for the purpose of upstream bandwidth allocation, ranging, upstream channel privacy, and class of service.
Smurf attacks	Security attacks that do not try to steal information, but attempt to disable a computer or network. For example, a smurf attack could attempt to disable a network with ping floods.
Spoofing	A technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer using a source IP address indicating that the message is coming from a trusted host. To engage in IP spoofing, a hacker must first use a variety of techniques to find an IP address of a trusted host and then modify the packet headers so that it appears that the packets are coming from that host.

Terminology, Continued

Term	Definition
Stand-alone Cable Modem (SCM)	The stand-alone cable modem is currently deployed by cable service providers and Internet service providers for high speed data service.
Subscribed PC CPE	PC CPE whose PC MAC address can be located in the Back-end Server Database. When in this subscribed state, the PC is assigned a public IP address.
Time Of Day (TOD) Server	The cable modem uses the TOD server to get the current date and time to accurately time-stamp its Simple Network Management Protocol (SNMP) messages and error log entries.
Trivial File Transfer Protocol (TFTP) Server	The cable modem uses the TFTP server to download its configuration file.
Unicast Data	Data that is addressed to a single destination. This includes, but is not limited to, unicast UNPassthru messages from the DNCS to the DHCT, and unicast data between an application running on the DHCT and a remote host.
Unregistered Cable Modem	A cable modem whose MAC address cannot be located in the back-end server database. A cable modem is unregistered only when the cable service provider offers self-provisioning for cable modems. In this case, the cable modem is assigned a temporary net 10 private IP address.
Unsubscribed PC CPE	A PC CPE whose PC MAC address cannot be located in the Back-end Server Database. In this case, the PC is assigned a temporary net 10 private IP address.
Upstream DBDS traffic	Data that flows from DHCTs to DBDS network elements to support interactive applications, such as, VOD or PPV services.
Virtual Private Network (VPN)	A secure network that is constructed by using public wires to connect nodes. For example, there are a number of systems that enable you to create networks using the Internet as the medium for transporting data. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network and that the data cannot be intercepted.

System Description

Introduction

This section describes the DBDS infrastructure in which DOCSIS-capable DHCTs operate. This section also provides descriptions of the various DHCT communication modes (DCMs) that are required to deploy DOCSIS-capable DHCTs in the DBDS. In addition, a diagram is provided that shows the layout of a network that can support the various communication modes.

Deploying DOCSIS-Capable DHCTs into the DBDS

There are two types of DOCSIS-capable DHCTs:

- One type is a Mixed DOCSIS/DAVIC-capable DHCT that has two out-of-band tuners and can receive both DAVIC and DOCSIS channels simultaneously.
- The other type is a DOCSIS-only DHCT that has one out-of-band tuner and can receive either a DAVIC or DOCSIS channel but not both simultaneously.

Some cable service operators deploying DOCSIS-capable DHCTs into existing systems may continue to operate their DAVIC QPSK out-of-band transmitters. Cisco's Mixed DOCSIS/DAVIC-capable DHCTs can receive the DAVIC out-of-band channel while simultaneously using a DOCSIS channel for interactive communications. In this case, the out-of-band data can take the "traditional" route over the DAVIC channel.

Other cable service providers may deploy DOCSIS-capable DHCTs into new hubs or new systems that may not have a DAVIC QPSK infrastructure. In this case, the system must transmit out-of-band data over the DOCSIS channel through a DSG-compliant CMTS.

A high-level description of each DHCT communication mode is provided in **DHCT Communication Modes**, next in this section.

DHCT Communication Modes

The following table describes each DHCT communication mode and the communication interfaces required for each mode in the DBDS.

Mode	Description
DAVIC	All downstream communications (including DBDS broadcast and unicast data) use the DAVIC out-of-band channel. Upstream communications use the DAVIC reverse channel. The DOCSIS channel is not used. The DNCS administers the IP address for the DHCT CPE. The DNCS continues to use DSM-CC UNConfig, UNSession, UNDownload, and UNPassthru messages for DHCTs operating in this mode.
Mixed DOCSIS/DAVIC	DBDS broadcast data communications use the downstream DAVIC out-of-band channel, and unicast communications use the DOCSIS bi-directional channel. One or more DHCP servers administer the IP address for the DHCT CPE. These servers are outside the DBDS span of control. The DNCS continues to use DSM-CC UNConfig, UNSession, UNDownload, and UNPassthru messages for DHCTs operating in this mode.
DOCSIS	All downstream communications (including DBDS broadcast and unicast data) use the DOCSIS channel through a DSG-compliant CMTS. The downstream DAVIC out-of-band channel may be used for DBDS broadcast data if the DOCSIS channel is impaired. One or more DHCP servers administer IP addresses for the DHCT CPE. These servers are outside the DBDS span of control. The DNCS continues to use DSM-CC UNConfig, UNSession, UNDownload, and UNPassthru messages for DHCTs operating in this mode.

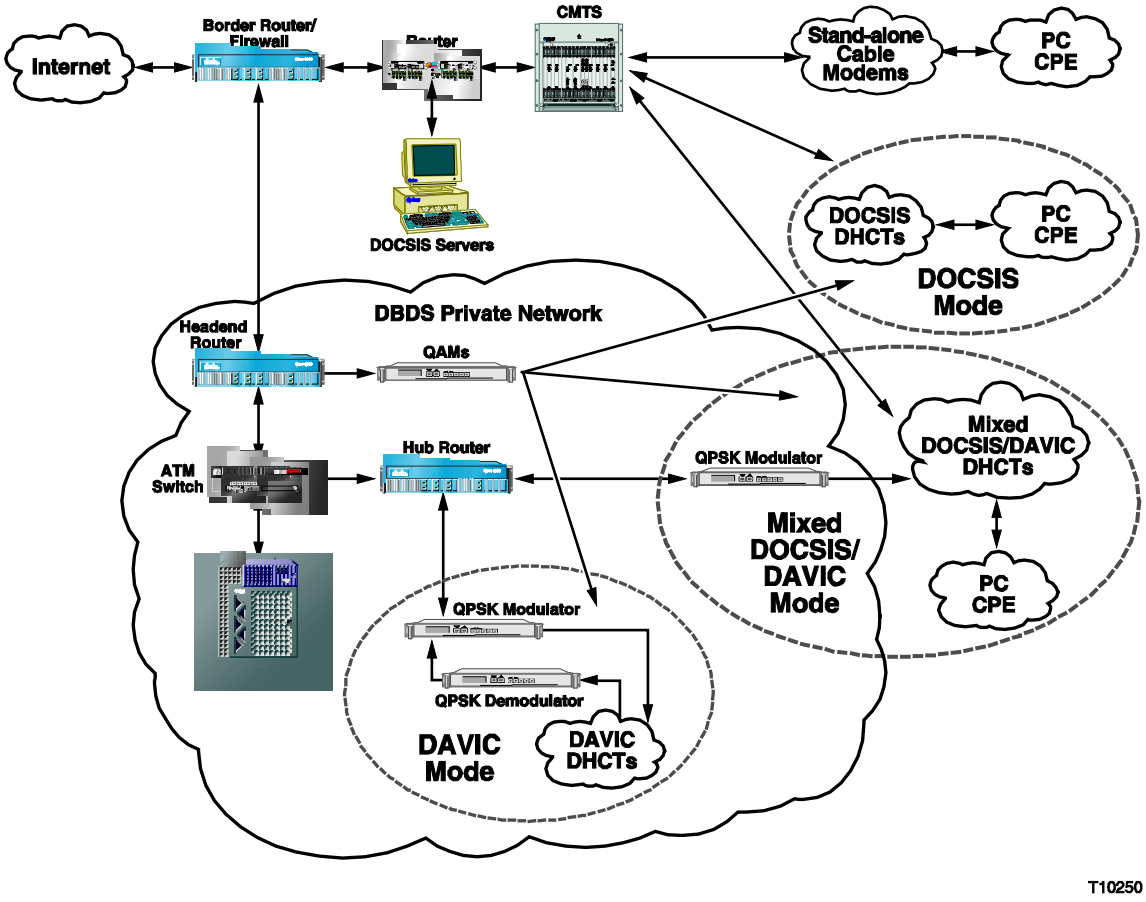
DOCSIS Settop Gateway (DSG)

For DHCTs operating in DOCSIS mode, DBDS broadcast data must be carried over the DOCSIS channel through a DSG-compliant CMTS. To accomplish this communication, DSG definitions are established on the CMTS to act as gateways for the DBDS broadcast data that must be delivered to the DHCTs in each of the DOCSIS MAC domains of the CMTS as specified in the *DOCSIS Set-top Gateway (DSG) Interface Specification*.

Each CMTS DOCSIS MAC domain has a single definition for DBDS broadcast data. Each DSG definition takes IP packets matching its destination address and encapsulates them in an Ethernet frame, using a well-known Cisco MAC address. All DSG definitions use the same well-known Cisco MAC address; the DHCT filters on the well-known Cisco MAC address. By using this MAC address, DHCTs operating in DOCSIS mode can receive DBDS broadcast data without establishing an interactive communications path with the CMTS. Therefore, if the upstream plant is impaired, there is no impact on the DHCT's ability to receive DBDS broadcast data.

A Simplified Network View of the DHCT Communication Modes

The following diagram shows the layout of a network that can support DHCTs operating in the various communication modes.



System Requirements

Introduction

This section describes the network element requirements your DBDS must comply with to operate DOCSIS-capable DHCTs.

Network Element Requirements

The network elements in your DBDS must meet the following requirements to operate DOCSIS-capable DHCTs.

- The CMTS unit(s) used must adhere to the specifications detailed in the following publications:
  - *Data-Over-Cable Service Interface Specifications Radio Frequency Interface Specification*
  - *Data-Over-Cable Service Interface Specifications Cable Modem to Customer Premise Equipment Interface Specification*
  - *Data-Over-Cable Service Interface Specifications Operations Support System Interface Specification*
- The DHCP server(s) used must adhere to the specifications detailed in *Dynamic Host Control Protocol*, RFC-2131, March, 1997.
- DHCTs booting in DAVIC mode must receive an IP address from a private address pool managed by the DNCS.
- DHCTs booting in DOCSIS or Mixed DOCSIS/DAVIC mode must receive cable modem and DHCT CPE IP addresses from address pools managed by the DHCP server. The address pools managed by the DHCP server may be public or private.

If you are unsure of your system's ability to meet these requirements, contact your network administrator or Cisco Services to arrange for a network analysis.

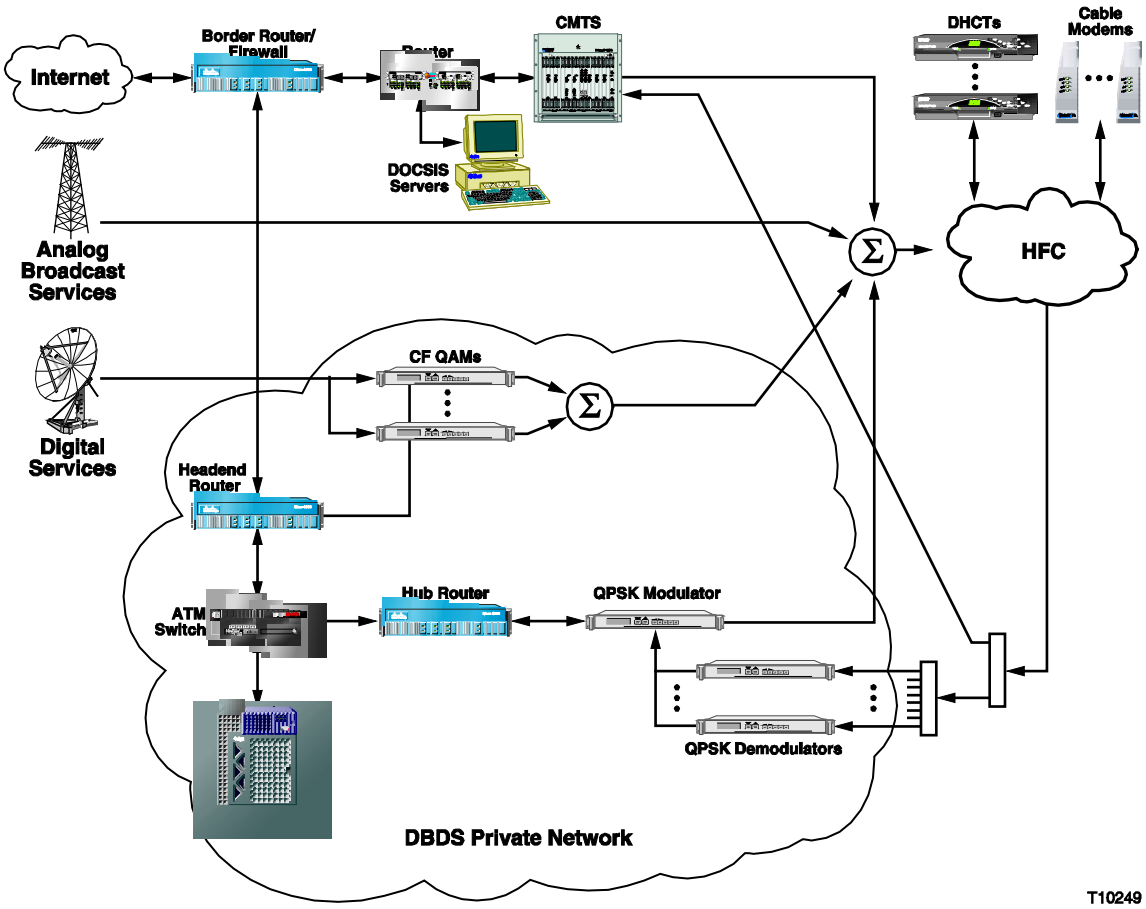
System Elements and Interfaces

Introduction

This section describes the system elements and interfaces that exist for a DBDS and shows a simplified diagram of the DBDS architecture that supports DOCSIS. This section also introduces the network elements, and DHCT and communication interfaces required for a DOCSIS environment. In addition, this section describes the DOCSIS Set-top Gateway(DSG), which forwards DBDS broadcast data to DHCTs operating in DOCSIS mode over the DOCSIS channel through a DSG-compliant CMTS.

A Simplified View of the System Architecture

The following diagram shows a simplified physical view of the system architecture and network interfaces required to implement DOCSIS in the DBDS.



Network Elements

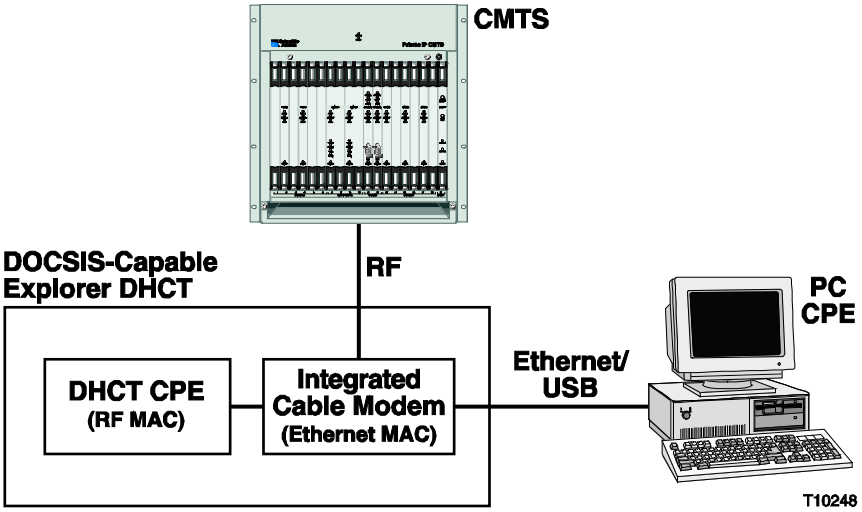
The following elements are required to support DOCSIS functionality in the DBDS.

- The downstream channels of the CMTS are combined with the QAM and DAVIC QPSK forward path signals, and the reverse path is split to feed any DAVIC QPSK demodulators in the hub and the CMTS.
- The border router/firewall between the CMTS and the Internet provides Internet/intranet routing, Network Address Translation (NAT), and filtering functionality, as required.
- The headend router between the CMTS and the DBDS private network provides the path for unicast data between the DNCS and the DHCTs operating in DOCSIS or Mixed DOCSIS/DAVIC mode.
- The downstream connections from the CMTS, QAMs, QPSK modulators, and upstream connections to the QPSK demodulators and CMTS are standard RF coax (F-type). The QAM, QPSK modulator, and QPSK demodulator each have one RF interface. (MQAMs have four RF interfaces.) The number of deployed CMTS devices is specific to the cable service operator and depends on implementation preferences. The number of downstream and upstream RF interfaces per CMTS or per CMTS blade is specific to the CMTS vendor.
- Control connections from the DBDS network to the QAMs/MQAMs and QPSK modulators are 10BaseT only for QAMs/MQAMS and 10/100 for QPSKs.
- The connection from the DNCS to the DBDS private network is ATM and/or Ethernet.
- The connections between the headend router and the CMTS, between the CMTS and border router, and between the CMTS and the DHCP server are vendor-specific. All these connections have the common trait of supporting IP traffic.

DHCT Interfaces

A DOCSIS-capable Explorer DHCT has an integrated cable modem and DHCT CPE. When a DHCT is initialized in DOCSIS or Mixed DOCSIS/DAVIC mode, the cable modem acts as a "front end" for communication to the DHCT. From the CMTS's perspective, the DHCT is the CPE "behind" the cable modem.

The following diagram shows a conceptual model of the interfaces in a DOCSIS-capable DHCT.



Communication Paths in the DOCSIS-Capable Explorer DHCT

Use of the communication paths differs with the DHCT's communication mode. A Mixed DOCSIS/DAVIC-capable Explorer DHCT uses three receivers to simultaneously receive analog and digital A/V services and DOCSIS and DAVIC downstream data.

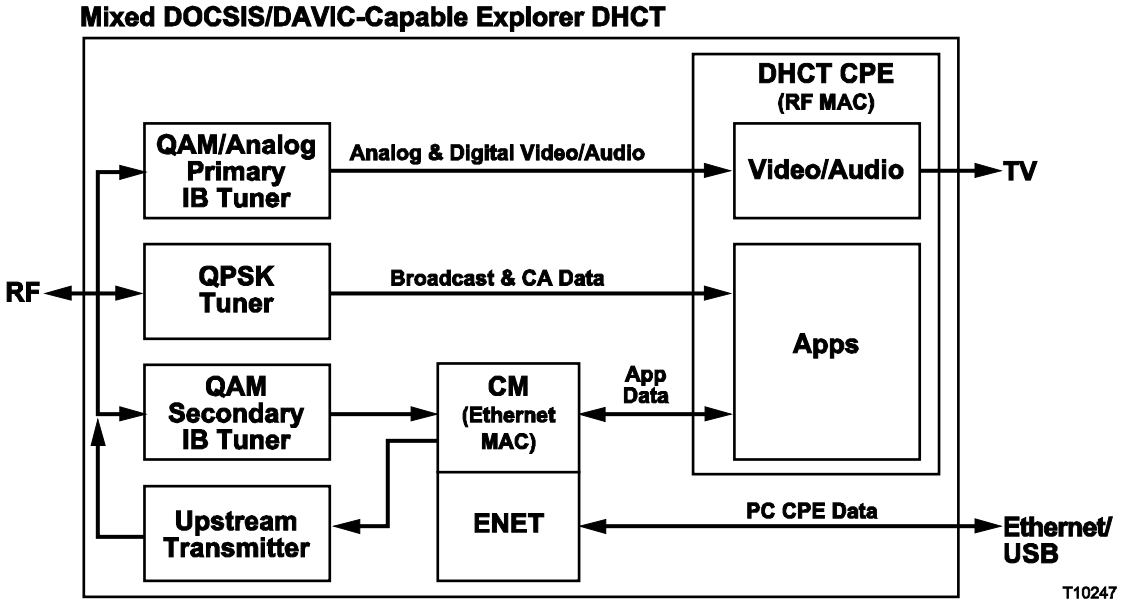
The DHCT has a QAM-16/QPSK transmitter to send data upstream. The three downstream receivers perform the following functions:

- The primary in-band receiver tunes to analog and digital A/V services.
- The secondary in-band receiver tunes to downstream DOCSIS high-speed data.
- The downstream DAVIC QPSK receiver tunes to out-of-band data when the DHCT is operating in DAVIC or Mixed DOCSIS/DAVIC mode.

The upstream transmitter sends data either to the DAVIC QPSK demodulator in DAVIC mode or to the DOCSIS CMTS in either a Mixed DOCSIS/DAVIC or DOCSIS mode.

Note: A DOCSIS-capable DHCT has two MAC addresses. The DOCSIS-cable modem MAC address is often called the Ethernet MAC address. The DHCT CPE MAC address is often called the RF MAC address.

The following diagram shows the various communication paths within a Mixed DOCSIS/DAVIC-capable DHCT that is operating in Mixed DOCSIS/DAVIC mode.



DHCT Initialization

Introduction

This section describes how DOCSIS-capable DHCTs operating in Mixed DOCSIS/DAVIC mode obtain the IP addresses for their cable modems and DHCT CPEs during initialization. This section also addresses how these DHCTs communicate their DHCT CPE IP address to the DNCS.

Obtain and Communicate IP Addresses

When the DOCSIS-capable DHCT boots in DOCSIS or Mixed DOCSIS/DAVIC mode, the DHCP server assigns an IP address to the cable modem element and the DHCT CPE.

After obtaining the IP addresses, the DHCT communicates the DHCT CPE IP address to the DNCS using DNCS UNConfig messages. The DNCS must send an acknowledgement of receiving the IP address to the DHCT. Otherwise, the DHCT continues to attempt to communicate the IP address to the DNCS until it receives an acknowledgement.

The following table shows the communication exchange when IP addresses are delivered to DHCTs in DAVIC and DOCSIS or Mixed DOCSIS/DAVIC mode:

Message	DAVIC Mode	DOCSIS or Mixed DOCSIS/DAVIC Mode
UNConfigRequest	The UNConfigRequest message is sent from the DHCT to the DNCS to request an IP address.	The UNConfigRequest message is sent from the DHCT to the DNCS to report its IP address that was assigned by the DHCP server.
UNConfigConfirm	The UNConfigConfirm message is sent from the DNCS to the DHCT to deliver an IP address.	The UNConfigConfirm message is sent from the DNCS to the DHCT to acknowledge receipt of the UNConfigRequest message.

The DHCT communicates its IP address to the DNCS when the DHCT initializes (or boots) and when the IP address changes.

The DNCS distinguishes between DAVIC DHCTs that obtain their IP addresses from the DNCS, and DOCSIS DHCTs that obtain their IP addresses from other servers. This distinction is embedded in the UNConfigRequest message sent from the DHCT to the DNCS. The DOCSIS DHCT includes its IP address in the message, whereas the DAVIC DHCT does not.

PC applications receive IP data through the DOCSIS channel as soon as cable modem registration is complete. Advanced DHCT services, such as VOD, that require registration with the DNCS become available only after the DHCT receives the UNConfigConfirm message from the DNCS.

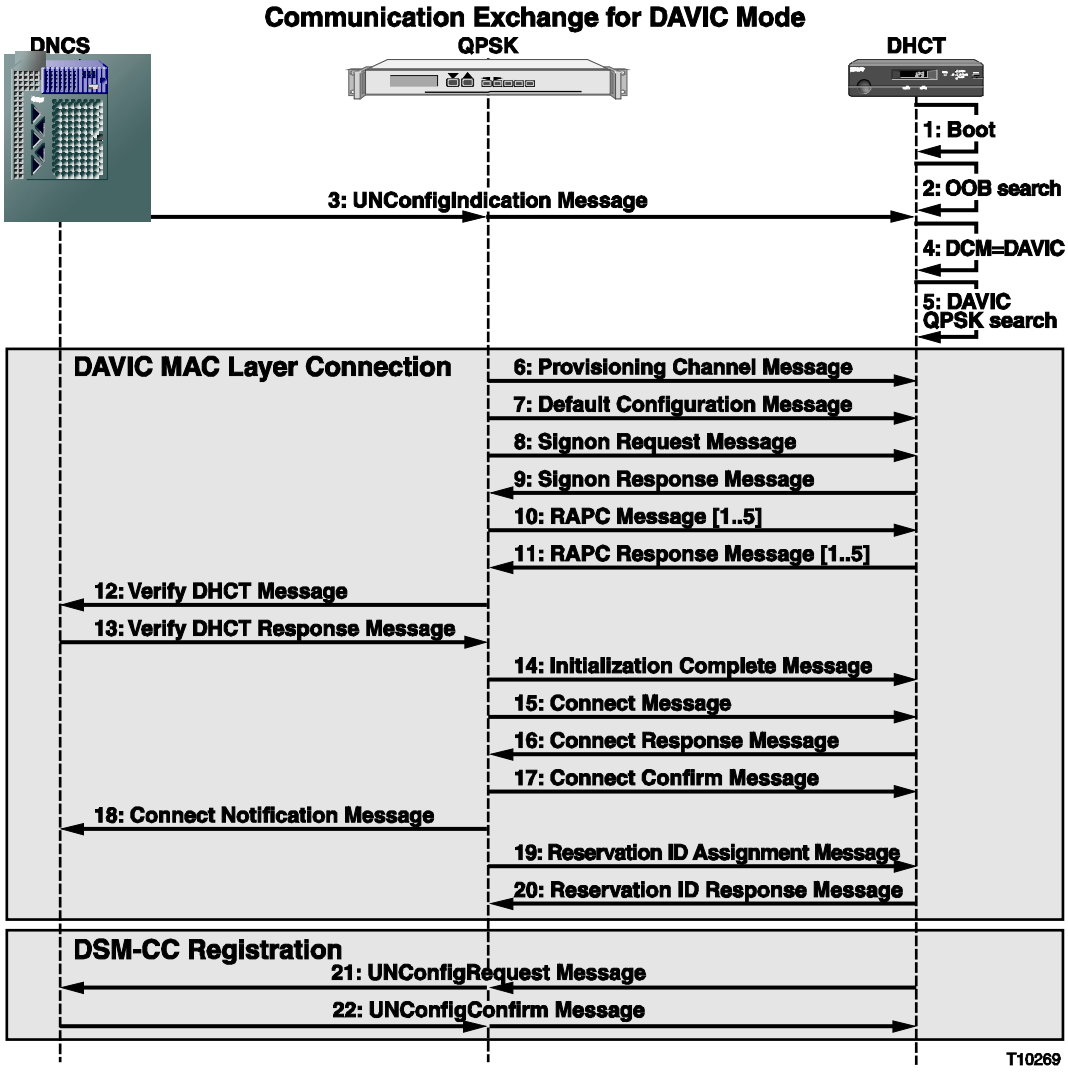
Communication Exchange

The following three illustrations show the communication exchange among the network components for the three communication modes:

- DAVIC
- Mixed DOCSIS/DAVIC
- DOCSIS

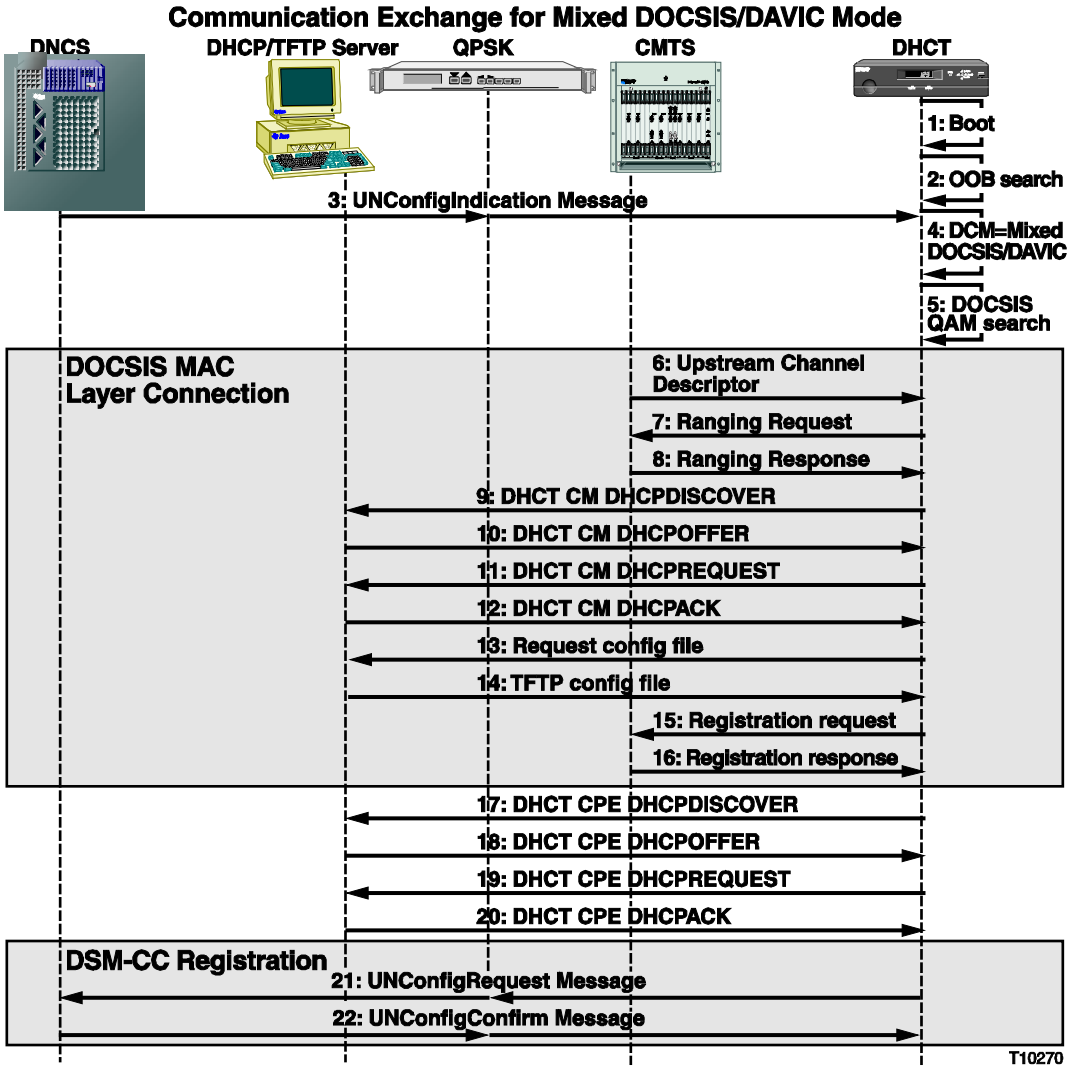
Communication Exchange for DAVIC Mode

The following illustration shows the communication exchange between the DHCT and the DNCS in DAVIC mode.



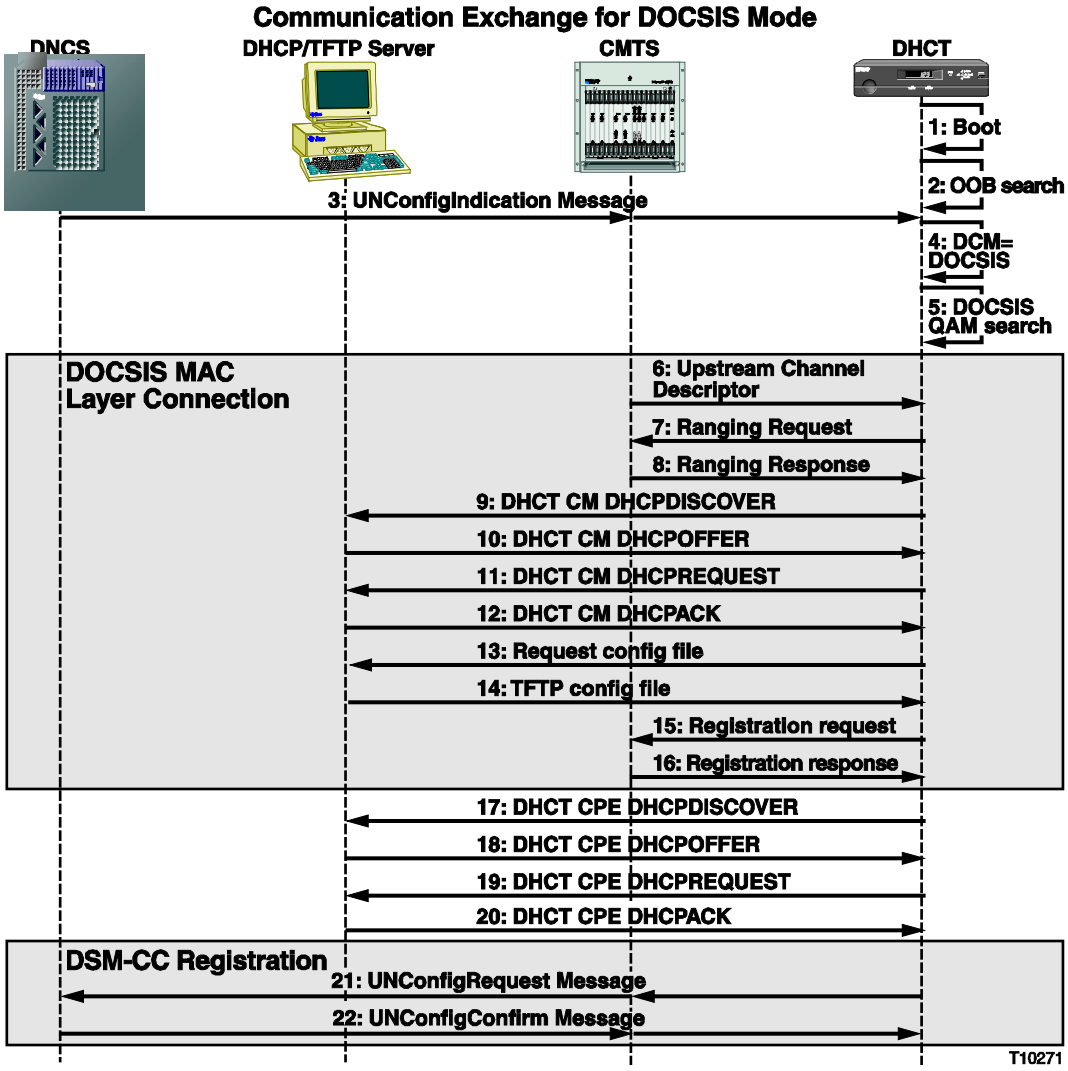
Communication Exchange for Mixed DOCSIS/DAVIC Mode

The following illustration shows the communication exchange between the DHCT and DNCS in Mixed DOCSIS/DAVIC mode.



Communication Exchange for DOCSIS Mode

The following illustration shows the communication exchange between the DHCT and the DNCS in DOCSIS mode.



DHCT Communication Modes

Introduction

This section describes the DHCT Communication Modes (DCMs) used by DOCSIS-capable DHCTs within a DBDS environment.

The DOCSIS-capable DHCT is instructed to use a specific DHCT communication mode through a DCM setting. The DNCS operator defines the communication mode on the DNCS. The DNCS embeds the mode in the UNConfigIndication message. This small message is periodically broadcasted on the downstream DAVIC out-of-band QPSK signals and on the CMTS downstream channels through DSG definitions.

The DCM indicates which DHCT Communication Mode is to be used:

- DAVIC
- Mixed DOCSIS/DAVIC
- DOCSIS

The DCM is ignored by DHCTs that are not DOCSIS-capable.

The DCM is common to all DHCTs within the span of control of a single downstream DAVIC out-of-band QPSK transmitter or a single DSG definition on a CMTS. DCMs are not customized for individual DHCTs. All DOCSIS-capable DHCTs within the span of control of a QPSK or CMTS DOCSIS MAC domain receive the same DCM. The QPSK or CMTS DOCSIS MAC domain is the smallest level of granularity by which DCMs can be defined. DCMs cannot be defined for individual DHCTs. In a network in which the DAVIC and DOCSIS systems are overlaid, the DCM through each path must be consistent as seen by a receiving DHCT.

After initialization, the operator can change the mode of a DHCT from the DNCS by changing the DCM on the QPSK or CMTS and sending a DCM Updated message. When the DHCT receives a DCM Updated message, the DHCT attempts to establish an interactive data communications path per the DCM setting in the next UNConfigIndication message it receives if the communication mode is different from the current setting in the DHCT.

Unless the DHCT has received a DCM Updated message, the DHCT will ignore any change in the communication mode after it has successfully established an interactive communications connection.

Only DOCSIS-capable DHCTs can process the DCM setting that the DNCS operator defines on the DNCS. DAVIC-only DHCTs ignore the setting and continue to operate in DAVIC mode.

Receiving Communication Mode Upon Initialization

When a DHCT reboots, it attempts to establish an interactive connection using the DCM and other parameters it used for its last successful connection. This reboot process minimizes boot time by not requiring the DHCT to wait for a UNConfigIndication message. Also, the expectation is that the vast majority of the time when a DHCT reboots, it is in the same physical location. However, if the DHCT establishes an interactive connection prior to receiving the first UNConfigIndication and then discovers that the DCM in the UNConfigIndication is different from that into which it booted, it must enter into that mode.

DAVIC Mode Operation

DOCSIS-capable DHCTs that receive a DAVIC DCM setting in the UNConfigIndication message attempt to establish an interactive communications path over the DAVIC channel. DBDS broadcast data traffic is received over the DAVIC channel in this mode. DOCSIS-capable DHCTs in this mode do not attempt to establish an interactive communications path over the DOCSIS channel.

Mixed DOCSIS/DAVIC Mode Operation

Mixed DOCSIS/DAVIC-capable DHCTs that receive a Mixed DOCSIS/DAVIC DCM setting in the UNConfigIndication message attempt to establish an interactive communications path over the DOCSIS channel only. DBDS broadcast data traffic is received over the DAVIC channel in this mode. DOCSIS-capable DHCTs in this scenario do not attempt to establish an interactive communications path over the DAVIC channel.

DOCSIS Mode Operation

DOCSIS-capable DHCTs that receive a DOCSIS DCM setting in the UNConfigIndication message attempt to establish an interactive communications path over the DOCSIS channel. A DOCSIS-capable DHCT receives DBDS broadcast data over the DOCSIS channel. However, for the DOCSIS-capable DHCT to receive DBDS broadcast data over the DOCSIS channel, a DSG-compliant CMTS must send the data. DOCSIS-capable DHCTs in this mode do not attempt to establish an interactive communications path over the DAVIC channel.

DHCT Response to System Interruptions

Introduction

This section describes how system interruptions affect a DOCSIS-capable DHCT. For each of the three DHCT Communication Modes, interruption of critical downstream and upstream communication is considered.

Important: After the DHCT establishes an interactive connection, it ignores any mode changes that are in DCM messages. The DHCT will act on changes in the DCM message only if it receives a DCM Updated message.

How a DHCT Operating in DAVIC Mode Responds to the Loss of the DAVIC Channel

This section describes how a DHCT operating in DAVIC mode responds when it loses the DAVIC channel.

Loss of the DAVIC Channel

A DHCT operating in DAVIC mode responds to the loss of the downstream DAVIC out-of-band QPSK signal in the following ways:

- After a timeout period, the DHCT attempts to find DBDS broadcast data on another downstream DAVIC out-of-band channel by scanning the DAVIC QPSK spectrum.
- The DHCT maintains audiovisual services, and does not disrupt these services when the downstream DAVIC out-of-band QPSK signal is recovered and the interactive connection is restored.

If a DHCT that boots in DAVIC mode loses the DAVIC forward channel, then all broadcast and unicast communications with the DHCT are interrupted. However, analog, clear digital, and subscription services continue to function. For example, all purchased IPPV events already in progress will continue without interruption. Any new IPPV event purchases can only succeed if the appropriate GBAMs were cached by the DHCT prior to the interruption of the DAVIC channel. VOD events that are already in progress will continue without interruption only if the interactive session timeout value is longer than the DAVIC channel interruption. The ability to fast-forward, pause, and rewind (trick modes) will be lost during the loss of the interactive channel.

While the DAVIC channel is unavailable, RPPV event purchases, interactive applications (Web browsing, e-mail, and so forth), new VOD event purchases, out-of-band System Information (SI) updates, Service Application Manager (SAM) updates, and out-of-band IPG updates will not function.

How a DHCT Operating in Mixed DOCSIS/DAVIC Mode Responds to the Loss of the DOCSIS or DAVIC Channel

This section describes how a DHCT operating in Mixed DOCSIS/DAVIC mode responds when it loses its DOCSIS or DAVIC channels.

Loss of the DOCSIS Channel

A DHCT operating in Mixed DOCSIS/DAVIC mode responds to the loss of the downstream DOCSIS signal in the following ways:

- The DHCT monitors its last-good downstream DOCSIS frequency until expiration of internal timeouts. It then scans the entire DOCSIS spectrum to locate and use a DOCSIS signal with which it can establish an interactive connection.
- The DHCT continues to receive DBDS broadcast data over the downstream DAVIC out-of-band QPSK channel.
- The DHCT does not attempt to establish an interactive DAVIC connection.
- The DHCT maintains audiovisual services and does not disrupt these services when the downstream DOCSIS signal is recovered and an interactive connection is restored.

Because the loss of the DOCSIS channel in Mixed DOCSIS/DAVIC mode represents a loss of interactive communications only, the DHCT can still provide analog, clear digital, and subscription digital services, IPPV, RPPV, OOB SI updates, SAM updates and IPG updates. Purchased VOD events in progress continue uninterrupted only if the interactive session timeout value is longer than the DOCSIS channel interruption. However, the subscriber cannot fast-forward, pause, or rewind the program while the interactive communication is lost. Interactive applications and new VOD event purchases will also not function.

Loss of the DAVIC Channel

A DHCT operating in Mixed DOCSIS/DAVIC mode responds to the loss of the downstream DAVIC out-of-band QPSK signal in the following ways:

- After a timeout period, the DHCT attempts to find DBDS broadcast data on another downstream DAVIC out-of-band channel by scanning the DAVIC QPSK spectrum.
- The DHCT maintains audiovisual services, and does not disrupt these services when the downstream DAVIC out-of-band QPSK signal is recovered.

The loss of the DAVIC channel in Mixed DOCSIS/DAVIC mode means that DHCT broadcast and CA data is unavailable to the DHCT, unless the DHCT can receive it over DOCSIS. The interactive data connection over the DOCSIS channel remains intact. Whether the DHCT has DBDS broadcast data or not, analog, clear digital, and subscription digital services will continue to function, and purchased IPPV and VOD events that are already in progress will continue uninterrupted.

If the DHCT does not have any DBDS broadcast data, new IPPV event purchases will only succeed if the appropriate GBAMs were cached by the DHCT prior to the DAVIC channel interruption. RPPV events, OOB SI updates, SAM updates and IPG updates will not function. Interactive applications including new VOD event purchases may or may not work, depending upon their use of broadcast data.

How a DHCT Operating in DOCSIS Mode Responds to the Loss of the DOCSIS Channel

This section describes how a DHCT operating in DOCSIS mode responds when it loses its DOCSIS channels.

Loss of the DOCSIS Channel

A DHCT operating in DOCSIS mode responds to the loss of the downstream DOCSIS signal in the following ways:

- The DHCT monitors its last-good downstream DOCSIS frequency until expiration of internal timeouts. It then scans the entire DOCSIS spectrum to locate and use a DSG-enabled DOCSIS signal with which it can establish an interactive connection.
- If DBDS broadcast data is unavailable on any DOCSIS channel, the DHCT scans for a downstream DAVIC out-of-band QPSK signal and uses this, if present, to receive DBDS broadcast data while the DBDS broadcast data over DOCSIS is unavailable.
- The DHCT does not attempt to establish an interactive DAVIC connection.
- The DHCT maintains audiovisual services and does not disrupt these services as the downstream DOCSIS signal is recovered and an interactive connection is restored.

Analog, clear digital, and subscription digital services will continue to function, and purchased IPPV events in progress will continue uninterrupted. The purchased VOD events in progress will continue uninterrupted if the interactive session timeout value is longer than the DOCSIS channel interruption. However, the subscriber cannot fast-forward, pause, or rewind the program while the interactive communication is lost.

If the DHCT does not receive DBDS broadcast data, new IPPV event purchases will only succeed if the appropriate GBAMs were cached by the DHCT prior to the DOCSIS channel interruption. RPPV events, OOB SI updates, SAM updates and IPG updates will not function without DBDS broadcast data. Interactive applications and new VOD event purchases will not function.

Loss of DBDS Broadcast Data On a DOCSIS Channel

A DHCT operating in DOCSIS mode responds to the loss of DBDS broadcast data in the following ways:

- The DHCT maintains its interactive DOCSIS connection without interruption.
- The DHCT scans for a downstream DAVIC out-of-band QPSK signal, and uses the DAVIC channel if present to receive DBDS broadcast data.
- The DHCT does not attempt to scan the DOCSIS frequency band for a different DSG-enabled signal.
- The DHCT does not attempt to establish an interactive DAVIC connection.
- The DHCT maintains audiovisual services and does not disrupt these services as DBDS broadcast data is recovered and an interactive connection is restored.

Loss of DBDS Broadcast Data While the DHCT Boots

A DHCT responds to the loss of DBDS broadcast data while booting in the following ways:

- While booting, if a DHCT finds DBDS broadcast data on a DAVIC QPSK signal but not on any DOCSIS channel, and the DCM message indicates that the DOCSIS mode is to be used, the DHCT will establish an interactive DOCSIS connection. The DHCT will operate in Mixed DOCSIS/DAVIC Mode until it is rebooted.
- While booting, if the DHCT cannot find DBDS broadcast data on a DOCSIS signal or on a DAVIC QPSK signal, it will not establish any interactive connection. The DHCT will continue to search for DBDS broadcast data on either the DAVIC or DOCSIS channel until it is found. IP data-forwarding services for interactive DHCT applications and for external CPE will be unavailable until DBDS broadcast data is again available.

Chapter 2
Guidelines for Configuring the DBDS for DOCSIS

Overview

Introduction

DOCSIS-capable DHCTs include a DHCT CPE and an integrated cable modem, which provides high speed data service. With this design, it is extremely important that the network administrator carefully plan and manage the distribution of IP addresses to the end-user devices. Careful planning can prevent conflicts of IP addresses with existing DAVIC DHCTs or the DBDS network.

This chapter provides guidelines to help you assign IP addresses for your DHCP server, CMTS, and end-user devices, such as stand-alone cable modems, integrated cable modems, DHCT CPE, and PC CPE. In addition, this chapter provides guidelines to help you configure the CMTS and provision servers on a DBDS network that supports DOCSIS. The cable service provider is responsible for managing IP addresses, the DOCSIS servers, and the CMTS.

At the end of this chapter, we provide a checklist of the tasks you need to do for the different system components to enable Mixed DOCSIS/DAVIC or DOCSIS in the DBDS.

In This Chapter

This chapter contains the following topics.

Assumptions

Introduction

This section lists the assumptions that Cisco has made about your system so that we can provide these guidelines for provisioning DOCSIS onto the DBDS.

The IP addresses used in this document are only examples. Cable service providers should determine their own IP addressing scheme. The IP subnet mask(s) that the cable service provider chooses determines the number of end-user devices that can be connected per CMTS DOCSIS MAC domain. Therefore the cable service provider's IP address blocks might be different from those used in these guidelines.

What Did We Assume?

We have made the following assumptions about your system:

- 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).
- The entire 10 network is dedicated to end-user devices.
- The cable service provider will not use any subnets from the private 10 network IP addresses that are currently being used by existing DHCTs and DBDS network elements in order to avoid any IP address conflict.
- The cable service providers will assign one subnet block to the integrated cable modem and another subnet block to the stand-alone cable modem.

  Note: Although stand-alone cable modems and integrated cable modems could share the same subnet block, Cisco recommends that they use a different subnet block for security purposes.
- This chapter assumes that each CMTS DOCSIS MAC domain can support a maximum of 2000 stand-alone cable modems or integrated cable modems. (The DOCSIS SID number places an absolute limit of 8191 cable modems per DOCSIS MAC domain).
- The cable service provider does not track the PC connected behind the cable modem. Therefore, an unsubscribed PC category is not required.
- The DHCP servers must implement the specifications in *Dynamic Host Control Protocol*, RFC-2131, March 1997.
- Interface bundling, which allows multiple cable interfaces to share a single IP subnet, is not enabled on the CMTS.
- The cable service provider does not allow for self-provisioning of integrated cable modems. MAC addresses for integrated cable modems are pre-provisioned in a database. Therefore, an unregistered integrated cable modem category is not required.
- The cable service provider does allow self-provisioning for stand-alone cable modems, and no cable modem MAC address is pre-provisioned in the database. Therefore, an unregistered stand-alone cable modem category is required. In the self-provisioning model, the subscriber buys his or her own cable modem, connects to the cable service provider's network, and uses the cable service provider's user interface to provide all of the required information.

IP Address Assignment

Introduction

This section provides guidelines for assigning IP addresses using a carefully-planned IP addressing scheme and the private IP address space.

IP Addressing Scheme

Because the overall network architecture for each cable service provider can differ, this chapter describes a simplified view of assigning IP addresses. The cable service provider must take full control and responsibility of their IP addressing scheme. Cisco strongly recommends that each cable service provider carefully plan their IP addressing scheme to allow for any future service growth (such as Cable Telephony and others). The cable service provider can further divide the IP addresses into hierarchical subnets. Contact Cisco Services for assistance.

IP network number assignment is guided by classifying each IP host as one of the following categories:

- Unregistered stand-alone cable modems
- Registered stand-alone cable modems
- Registered integrated cable modems
- DHCT CPE
- Subscribed PC CPE

Each of the categories above is in the private 10 network space except the subscribed PC CPE category, which is assigned a public cable service provider/Internet service provider IP address.

Private IP Address Space

The private IP address space is used for assigning IP addresses to the stand-alone cable modems, integrated cable modems, and the DHCT CPE.

The private address space will be 10.0.0.0 to 10.255.255.255, which provides 16,777,216 IP addresses. Cisco recommends that the cable service provider use a hierarchical addressing plan whenever possible. A hierarchical addressing plan allows the cable service providers to efficiently allocate addresses and summarize their routes in their router equipment. Using this plan also reduces the number of routing table entries in the routers.

Continued on next page

To use such a plan and to allow for network and subscriber growth within a region, we recommend that you partition the 10 network into four different large subnets with a 10-bit subnet mask (also known as the /10 prefix) as shown in the following examples:

- Subnet 1: 10.0.0.0 – 10.63.255.255
- Subnet 2: 10.64.0.0 - 10.127.255.255
- Subnet 3: 10.128.0.0 – 10.191.255.255
- Subnet 4: 10.192.0.0 – 10.255.255.255

Note: The 10-bit subnet mask is equivalent to 255.192.0.0 net mask.

Subnet 1 (10.0.0.0/10) can be further subdivided into two subnets each with a /11 prefix to support integrated cable modems and DHCT CPEs:

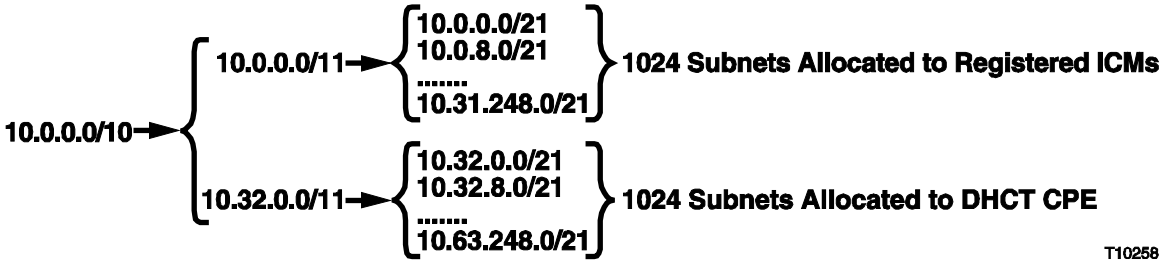
- 10.0.0.0/11
- 10.32.0.0/11

Assuming that each CMTS DOCSIS MAC domain can support a maximum of 2000 integrated cable modems, you can partition the first subnet 10.0.0.0 /11 even further to provide 1024 subnets with a /21 prefix. Assuming four blades or RF interfaces per CMTS, this configuration can support 256 CMTS's (1024 divided by 4). If each CMTS DOCSIS MAC domain is assigned a subnet with a /21 prefix, this subnet can support 2046 cable modems per CMTS DOCSIS MAC domain and can support 2046 IP addresses.

Note: The equivalent mask for the /11 prefix is 255.224.0.0. The equivalent mask for the /21 prefix is 255.255.248.0.

The first subnet 10.0.0.0/11 can be partitioned into 1024 subnets with /21 prefix and can be assigned to the registered integrated cable modems. The second subnet 10.32.0.0/11 can be partitioned into 1024 subnets with /21 prefix and can be allocated to the DHCT CPE.

The following diagram provides an example of how you can partition Subnet 1 (10.0.0.0/10) to support integrated cable modems and DHCT CPEs:



Subnet 2 (10.64.0.0/10) can be further subdivided into two subnets each with a /11 prefix to support registered and unregistered stand-alone cable modems:

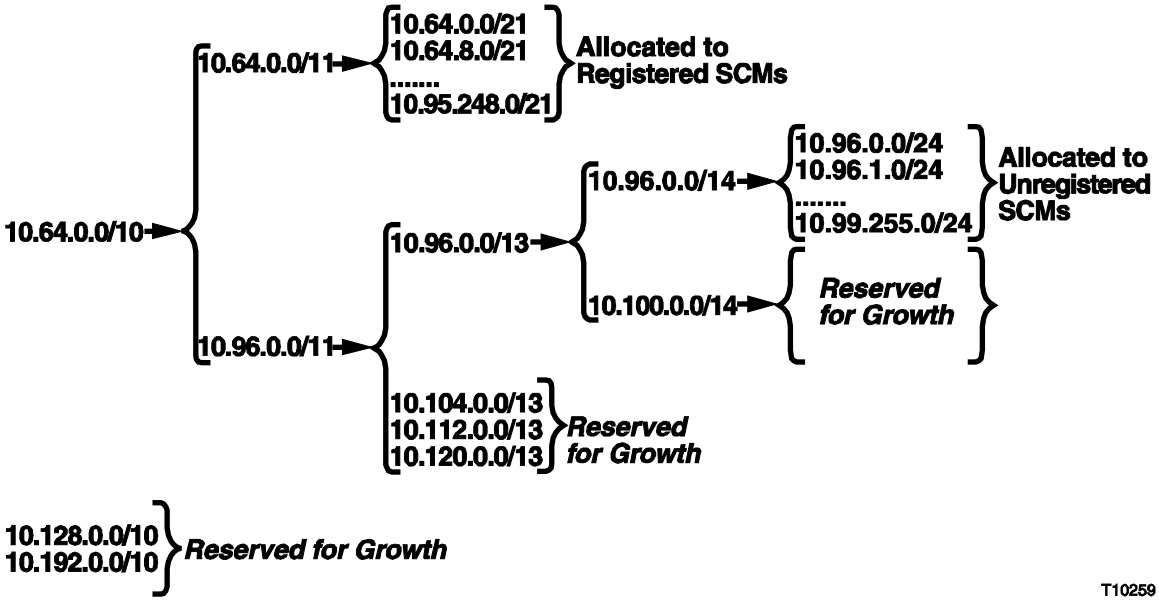
- 10.64.0.0/11
- 10.96.0.0/11

The first subnet, 10.64.0.0/11, can be partitioned into 1024 subnets with a /21 prefix. You can assign addresses from these subnets to registered stand-alone cable modems.

Because the unregistered stand-alone cable modem is a temporary state, a subnet with a /24 prefix per CMTS DOCSIS MAC domain would typically be sufficient to support stand-alone cable modems during registration. Therefore, the second subnet, 10.96.0.0/11, can be partitioned into 1024 subnets with the /24 prefix. You can assign addresses from these subnets to unregistered stand-alone cable modems. The majority of subnet 10.96.0.0/11 can then be reserved for growth.

The following diagram provides an example of how you can partition Subnet 2 (10.64.0.10) to support registered and unregistered stand-alone cable modems.

Note: In summary, Subnet 1 (10.0.0.0/10) and part of Subnet 2 (10.64.0.0/10) are used first. The other two Subnets (3 and 4), in addition to some residual IP addresses from Subnet 2, are left for growth.



Assigning Network Blocks to a CMTS Cable Interface Card

The following table illustrates how you can assign each CMTS cable interface card to a network block or subnet for each end-user category (registered integrated cable modems, registered stand-alone cable modems, DHCT CPE, and unregistered stand-alone cable modems).

CMTS Cable Interface Card	End User Category	Subnet Size per CMTS Cable Interface	Sample Subnet
1	Registered ICM	/21 prefix	10.0.0.0
	Registered SCM	/21 prefix	10.64.0.0
	DHCT CPE	/21 prefix	10.32.0.0
	Unregistered SCM	/24 prefix	10.96.0.0
2	Registered ICM	/21 prefix	10.0.8.0
	Registered SCM	/21 prefix	10.64.8.0
	DHCT CPE	/21 prefix	10.32.8.0
	Unregistered SCM	/24 prefix	10.96.1.0
3	Registered ICM	/21 prefix	10.0.16.0
	Registered SCM	/21 prefix	10.64.16.0
	DHCT CPE	/21 prefix	10.32.16.0
	Unregistered SCM	/24 prefix	10.96.2.0
4	Registered ICM	/21 prefix	10.0.24.0
	Registered SCM	/21 prefix	10.64.24.0
	DHCT CPE	/21 prefix	10.32.24.0
	Unregistered SCM	/24 prefix	10.96.3.0

CMTS Configuration

Introduction

This section provides guidelines for configuring the CMTS to work with DHCTs in Mixed DOCSIS/DAVIC mode or DOCSIS mode.

Interface Configuration

Either the first (.1) or last usable IP address (.254) from each network block is typically configured as the gateway IP address for the end-user devices on each cable interface card of a CMTS. In this example, the first usable IP address is configured as the gateway IP address. When deploying the DOCSIS-capable DHCTs the cable service operator should continue to configure their CMTS as they do today, with the following modifications:

- Implement any desired DSG definitions.
- Add a new Gateway IP address (from the DHCT CPE subnet) for the DHCT CPE at each CMTS RF interface.
- Add a route pointing to the DNCS so that any packet from the DHCT CPE destined to the DNCS is routed appropriately.

Global Configuration for the DOCSIS Set-top Gateway

As specified in *DOCSIS Set-top Gateway (DSG) Interface Specification*, the DSG is intended to provide DOCSIS channel transport for out-of-band messaging that is traditionally carried on dedicated channels. DSG definitions are established on the CMTS to act as gateways for the DHCT broadcast, CA, OOB SI, and Passthru flows that must be delivered to the DHCTs in each of the MAC domains of the CMTS.

The system operator chooses the DSG IP address from the DHCT CPE subnet on each CMTS cable interface card that is needed to support DHCT CPEs. The examples in this section use the second usable IP address (.2) from the DHCT CPE's subnet.

The DNCS delivers the out-of-band data flows to each DSG IP address (taken from the DHCT CPE subnet). The DSG definition defined on the CMTS then takes IP packets destined for the DSG IP address and encapsulates them in an Ethernet frame, using a well-known Cisco MAC address (00:01:A6:D0:0B:1E).

DHCTs operating in DOCSIS mode can receive DBDS broadcast data without establishing an interactive communications path with the CMTS. In this scenario, the DBDS supports DOCSIS DHCTs in a one-way operating environment (for example, a reverse-path-impaired condition).

The example below shows a partial configuration of a CMTS DOCSIS MAC domain.

Note: Stand-alone cable modem subnets are omitted from the configuration example.

Interface Cable3/0	
ip address 10.0.0.1 255.255.248.0	(*Registered ICM*)
ip address 10.32.0.1 255.255.248.0 secondary	(*DHCT CPE*)
ip address (Internet service provider public address) secondary	(*Subscribed PC*)
cable dhcp-giaddr primary (*or policy)*	*(Gateway IP address)*
ip dhcp relay information option	(*The CMTS inserts the DHCP relay agent information in forwarded DHCP messages to the DHCP server*.)
cable helper-address (192.168.24.23)	(*DHCP server IP address*)
!	
!	
arp 10.32.0.2 0001.a6d0.0b1e ARPA	(*DSG Definition*)

DNCS and Server Configurations

Introduction

This section provides guidelines for configuring the following DNCS and Server components for a DBDS network using DOCSIS:

- DNCS
- Mandatory DOCSIS 1.0 Servers
  - DHCP Server
  - TFTP Server
- Optional Servers
  - TOD Server
  - DNS Server

DNCS

The DNCS currently transmits the DBDS broadcast data. DHCTs operating in DOCSIS systems still need these flows; however, they may not be able to rely on QPSK modulators to deliver the flows. DSG-compliant CMTS routing and ARP settings have been devised to mimic the QPSK behavior. One DSG is defined for all flows. Therefore, every CMTS out-of-band (OOB) bridge requires one DSG definition. The cable service providers can select any IP address from that subnet range, but we recommend that they choose it from the upper end or the lower end of the range to avoid splitting scopes at the DHCP server.

The DNCS provides a user interface for defining a CMTS OOB bridge. When defining a CMTS OOB bridge, the operator should provide the following information:

- a name for the bridge
- a hub to associate with the bridge
- the name and IP address of the CMTS hosting the bridge
- a DSG IP address
- a DHCT communication mode

Routes pointing to the DHCT CPE subnets must be added in the DNCS and on any other router(s) located between the DNCS and the CMTS.

The DNCS provides the operator with tools to select the DCM for individual out-of-band bridges, including QPSK modulators. Refer to Chapter 1 for a description of the different modes.

Mandatory DOCSIS1.0 Servers

This section describes the DHCP and TFTP server configurations that are mandatory to operate DOCSIS in the DBDS. These servers must be configured for a DBDS network in a DOCSIS environment.

For the purpose of this example, Cisco assumes that the cable service providers have already deployed the servers identified in this section for their high-speed data service. The cable service providers are responsible for deploying and configuring their servers. The DHCP servers must be able to differentiate between a DHCT CPE DISCOVER message and a PC CPE DISCOVER message as discussed in this section.

DHCP Server

The DHCP server is required and provides IP addresses for stand-alone cable modems, integrated cable modems, DHCT CPE, and PC CPE. You can use the same DHCP server that is used for your existing stand-alone cable modems.

As stated earlier, the end-user devices, except PC CPE, should use the private network 10 space. Different scopes must be configured on the DHCP server. The network operator must make sure that the defined scope for the DHCT CPE excludes both the DHCT CPE gateway IP address configured on the CMTS RF interface and the DSG IP address to prevent address conflict.

The following example illustrates some of the possible scopes that can be configured on the DHCP server:

- Registered ICM 10.0.0.2 – 10.0.7.254
- DHCT CPE 10.32.0.3 – 10.32.7.254 (10.32.0.2 is not included here because it is reserved for the DSG definition.)
- Registered SCM 10.64.0.2 – 10.64.7.254
- Unregistered SCM 10.96.0.2 – 10.96.0.254
- Subscribed PC Internet service provider public address range

Important: At manufacture, 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. Network administrators should be aware of these MAC addresses if they will be provisioned on the DHCP server.

To allow a DHCP server to recognize DHCP DISCOVER messages coming from a Cisco DHCT, the integrated cable modem of the DHCT sends the DHCPDISCOVER message option 60 set to docsis1.0 and option 43 with option code 5 set to sciatl:cm:4200. The DHCT CPE sends in the DHCPDISCOVER message option 60, and option 43 with option code 5 both set to sciatl:dhct:model#. The model# field should not be used as a key in the server since this will vary per DHCT model. The intent is to use that field for troubleshooting purposes only.

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 configuration file than the stand-alone cable modems for the following two reasons:

- When setting the Max CPE parameter in the integrated cable modem configuration file, the operator must reserve 1 CPE slot to support traffic to the DHCT CPE. For example, in order to allow 1 PC, that parameter needs to be set to 2. Therefore the Max CPE for integrated cable modem must always be set to n+1, where n represents the number of allowed PCs. (An integrated cable modem using a configuration file with a Max CPE field that is blank or that contains the value 0 or 1 will support no external (PC) CPEs.)
- The integrated cable modem 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 using DOCSIS, you must also configure your Time of Day (TOD) and Domain Name Service (DNS) servers, if used.

TOD Server

The TOD server provides a timestamp for logged DOCSIS events. The cable 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. A DNS server is not required for DHCT CPE, but may be required for PC CPE that has a need for Internet access. Only the PC CPE has direct Internet access.

Enable Mixed DOCSIS/DAVIC in the DBDS

Introduction

This section provides a summary of what you must do to the various system components to enable Mixed DOCSIS/DAVIC in the DBDS.

Enabling Mixed DOCSIS/DAVIC in the DBDS

To enable Mixed DOCSIS/DAVIC in the DBDS, you must do the following on the DNCS, DHCP server, TFTP server, CMTS, and other routers:

DNCS

- Define the QPSK bridges.

  Note: When operating in a Mixed DOCSIS/DAVIC mode, you do not have to define a CMTS bridge.

- Add proper IP routes to reach the DHCT subnets.

CMTS

- Add proper IP routes to reach the DNCS and DOCSIS servers.
- Configure the RF interface with the following IP addresses:
  - Gateway IP address from the integrated cable modem IP address pool
  - Gateway IP address from the DHCT CPE IP address pool
  - Gateway IP address from the PC IP address pool (if offering high-speed data service)

DHCP Server

You can use the same DHCP server that you use for your existing stand-alone cable modems with the following modifications:

- Define the scopes for the integrated cable modem, DHCT CPE, and PC CPE subnets.
- Define the router gateway (in each policy) to match the respective subnet as defined in the CMTS RF interface.
- For proper routing, ensure that no IP addresses overlap between the following devices:
  - Existing DAVIC DHCT and new Mixed DOCSIS/DAVIC DHCTs
  - Existing stand-alone cable modems and the newly deployed integrated cable modems in the DOCSIS-capable DHCT
- Add proper IP routes to reach the integrated cable modem, DHCT CPE, and PC CPE subnets.
- Add proper IP routes to reach the CMTS.

- Configure the DHCP server to recognize DHCP DISCOVER messages coming from the DHCT CPE. The server may use either a DHCT CPE MAC address, option 60, or option 43 with option code 5, as discussed earlier in this chapter.
- Provision the directory-path name and location of the configuration file for the integrated cable modem.

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 configuration file than the stand-alone cable modems for reasons discussed in **DNCS and Server Configurations**, earlier in this chapter.

Other Routers

You must properly configure any router located between the DNCS and the CMTS to allow two-way communication between the DNCS and the DHCT CPEs.

Enable DOCSIS in the DBDS

Introduction

This section provides a summary of what you must do to the various system components to enable DOCSIS in the DBDS.

Enabling DOCSIS in the DBDS

To enable DOCSIS in the DBDS, you must do the following on the DNCS, DHCP server, TFTP server, CMTS, and other routers:

DNCS

- Define the CMTS bridges.
- Add proper IP routes to reach the DHCT subnets.

CMTS

- Configure the DSG definitions.
- Add proper IP routes to reach the DNCS and DOCSIS servers.
- Configure the RF interface with the following IP addresses:
  - Gateway IP address from the integrated cable modem IP address pool
  - Gateway IP address from the DHCT CPE IP address pool
  - Gateway IP address from the PC CPE IP address pool (if offering high-speed data service)

DHCP Server

You can use the same DHCP server that you use for your existing stand-alone cable modems with the following modifications:

- Define the scopes for the integrated cable modem, DHCT CPE and PC CPE subnets.
- Define the router gateway (in each policy) to match the respective subnet as defined in the CMTS RF interface.
- For proper routing, ensure that no IP addresses overlap between the following devices:
  - Existing DAVIC, Mixed DOCSIS/DAVIC DHCTs and newly deployed DOCSIS DHCTs
  - Existing stand-alone cable modems and the newly deployed integrated cable modems in the DOCSIS-capable DHCTs
- Ensure that the DHCT CPE scopes do not include the DSG IP addresses defined on the DNCS and the CMTS.
- Add proper IP routes to reach the integrated cable modem, DHCT CPE, and PC CPE subnets.

- Add proper IP routes to reach the CMTS.
- Configure the DHCP server to recognize DHCP DISCOVER messages coming from the DHCT CPE. The server may use either a DHCT CPE MAC address, option 60, or option 43 with option code 5, as discussed earlier in this chapter.
- Provision the directory-path name and location of the configuration file for the integrated cable modem.

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 configuration file than the stand-alone cable modems for the reasons discussed in **DNCS and Server Configurations**, earlier in this chapter.

Other Routers

You must properly configure any router located between the DNCS and the CMTS to allow two-way communication between the DNCS and the DHCT CPEs.

Chapter 3
Security Recommendations for the DBDS Network in a DOCSIS Environment

Overview

Introduction

Before deploying DOCSIS-capable DHCTs, we recommend that your network administrators update their existing security policies to help protect the DBDS private network from unauthorized external access (for example, from the Internet) and from unauthorized internal access (for example, any non-DHCT CPE element). By denying all foreign access to the DBDS private network, you can reduce the risk of intrusion, denial of service and theft of data attacks on the DNCS, EMS, App Servers, QAM Modulators, QPSKs, and DHCTs.

To help guard against a computer security breach, you must understand the basics of system security, establish policies and procedures to protect your network, and implement such policies and procedures.

This chapter assumes that you already have some network security measures in place, and does not provide detailed information on network security. This chapter provides guidelines that your network administrators may consider incorporating into their existing security policies. Following the security recommendations included in this chapter does not guarantee complete shielding of the DBDS network from security threats and attacks. No system that is connected to a network can ever be completely protected from security threats and attacks.

Disclaimer

Before using the security guidelines provided in this chapter, read the **DBDS DOCSIS Security Guidelines Disclaimer** in the **Disclaimer** section, earlier in this application guide.

Audience

This chapter is intended for experienced network administrators who manage network configurations and security.

In This Chapter

This chapter contains the following topics.

Recommendations on IP Address Assignment

Introduction

This section provides recommendations for assigning IP addresses to end-user devices. This section also describes the data paths that must be made secure in the DBDS.

IP Addresses for Servers

Depending on your network architecture, you can assign either private or public addresses to your servers. The interface that terminates end-user traffic may use a public IP address. Any interfaces connected to a LAN dedicated to inter-server traffic and administrative traffic may use private IP addresses.

If the cable service provider uses an external Internet Service Provider for high speed data (HSD) service, then the proxy server needs to communicate with the Internet service provider server for user authentication purposes. If the cable service provider is the Internet service provider, then no such server communication is required.

The DHCP server scopes are provisioned with IP address blocks from the private network space plus any Internet service provider public IP addresses. If the cable service provider is also the Internet service provider, the DHCP server scopes are provisioned with the cable service provider's public IP address block.

IP Addresses for End-User Equipment

For security reasons, Cisco strongly recommends that IP addresses for DHCT CPE be assigned from subnets that are separate (distinct) from those used for other end-user devices IP addresses. In other words, no single subnet should be used to assign IP addresses for DHCT CPE and any other type of device at the same time. It is recommended that the cable service provider segregate IP addresses for stand-alone cable modems from IP addresses for integrated cable modems. For examples of IP addresses for end-user equipment, refer to **Assigning Network Blocks to a CMTS Cable Interface Card** in Chapter 2 of this guide.

Note: Chapter 2 assumes that no unsubscribed PC CPE category exists, but this chapter considers this category from a security standpoint.

Security Recommendations

Cisco recommends that you follow these security recommendations when assigning IP addresses to the end-user devices in a DOCSIS network.

Because several of the security recommendations relate to each other, we assigned numbers to each recommendation for ease of reference. The recommendations are numbered in increments of 10 to allow for growth as new recommendations are added.

This section describes security recommendations 10 through 30 for assigning IP addresses. Recommendations 40 through 410 for securing the data paths in the DBDS are provided later in this chapter.

 # 10

Assign a *distinct* private IP address range to each end-user device type: unregistered stand-alone cable modem, registered stand-alone cable modem, registered integrated cable modem, DHCT CPE, and unsubscribed PC CPE.

 # 20

Assign DHCT CPE IP addresses from a subnet of the private 10.0 network. This subnet should be separate from the subnets from which you assign IP addresses for all other end-user devices.

 # 30

Plan an IP address scheme to avoid IP address conflicts between the newly deployed DOCSIS-capable DHCTs (integrated cable modem and DHCT CPE) and any network element or devices on the cable service provider's network.

Types of Security Attacks

Introduction

Security attacks can be classified into three main categories: intrusion, denial of service, and theft of data. If you follow the recommendations covered in this chapter and implement them correctly, you can reduce security risks on the DBDS network. However, this does not guarantee complete shielding of your DBDS network from security threats and attacks. Review these guidelines on a regular basis; incorporate the recommendations into your network security policies to make sure they are successfully supporting the security needs. This section describes the different categories of security attacks.

Intrusion

An intrusion on the DBDS may include any of the following events:

- An unauthorized party takes control of the DNCS, App Server, or DHCT functions.
- "Rogue" applications are run on the DNCS, App Server, or DHCT.
- An unauthorized party connects to the DNCS, App Server, or DHCT through telnet, FTP, TFTP, NFS, HTTP, or other non-secure services.

Denial of Service

Denial of service may include any of the following events:

- Flooding the DNCS, App Server, QAMs, QPSKs, or DHCT CPUs with data.
- Data corruption on the DNCS, App Server, QAMs, QPSKs or DHCTs.
- Spoofing (the process where one device makes itself look like another device to get past security measures) the DNCS or other servers.

Theft of Data From the DBDS

The following types of data on the DBDS are the most likely targets for theft:

- SNMP data on the DNCS, App Server, or DHCT
- CA data
- Configuration (database) data on the DNCS

Data Paths and Traffic Flows

Introduction

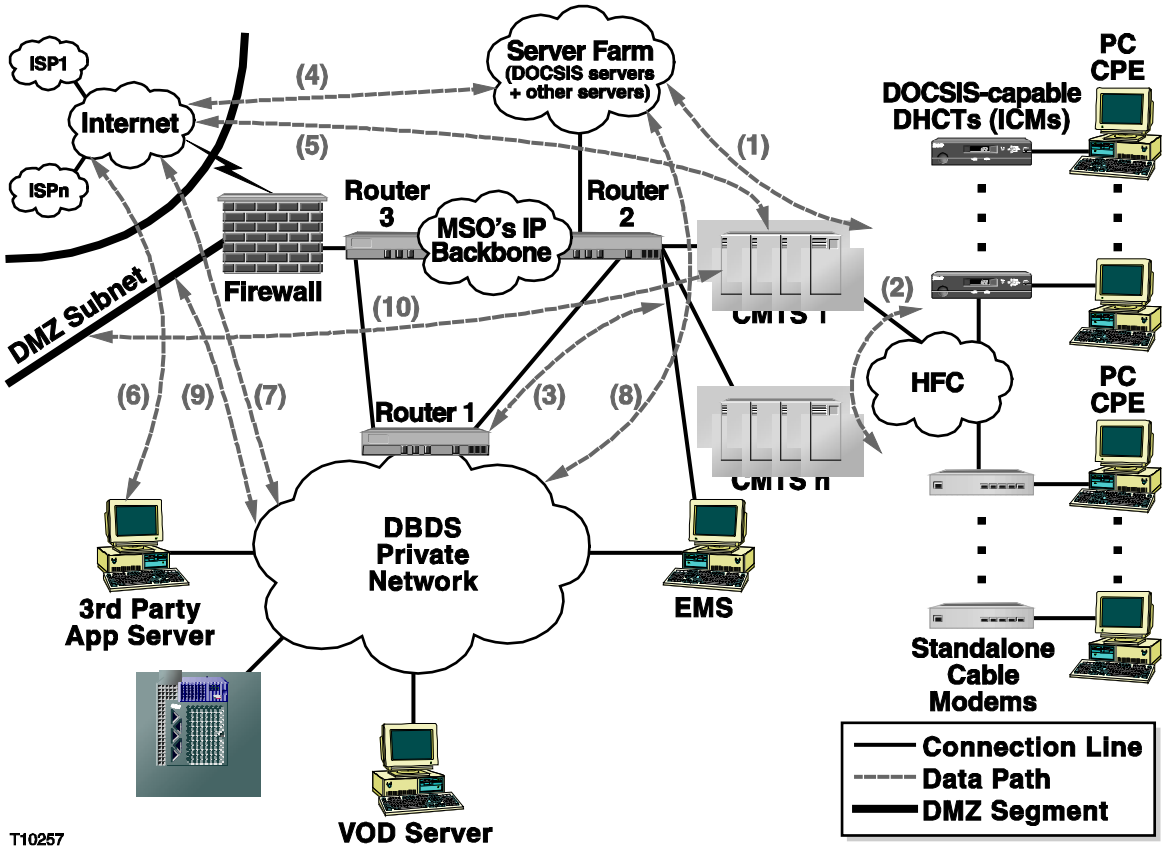
One of the first steps in network security is to secure the data paths into, out of, and within your network. There are nine network data paths requiring security considerations. This section describes the data paths and traffic flows in the DBDS that must be made secure and provides a diagram that shows the different data paths and traffic flows. The recommendations that cover each flow are addressed in **DBDS Network Security**, next in this chapter.

The following data paths must be made secure on the DBDS:

- Path 1: Registration between integrated cable modems, DHCT CPE, PC CPE, stand-alone cable modems, and the DOCSIS servers.
- Path 2: Communication among end-user devices (cable modem, DHCT CPE, PC CPE) within the same region.
- Path 3: Communication between the DBDS servers (application servers, DNCS, VOD servers) and the end-user devices.
- Path 4: Communication between the cable service provider's server farm and Internet service provider registration servers to authenticate and authorize end users. This path may not exist if the cable service provider is also the Internet service provider providing HSD service to the end users.
- Path 5: Communication between end-user devices and the Internet.
- Path 6: Communication between application servers and the Internet. This communication exists today, but the physical connectivity depends on the server.
- Path 7: Communication between any DBDS network element and the Internet.
- Path 8: Communication between any DBDS network element and the server farm.
- Path 9: Communication between any DBDS network element and the DMZ network.
- Path 10: Communication between end-user devices and the DMZ network.

High-Level View of Data Paths and Traffic Flows in the DBDS Network

The following diagram shows a high-level view of the data paths and traffic flows in a DBDS network.



Secure Data Paths

The following table covers all the data paths and identifies which corresponding bi-directional traffic flows should be allowed or denied according to Cisco's recommendations. Because this chapter focuses on the DBDS and DHCT security risk management, any traffic that does not pertain to the DBDS or the DHCT is outside the scope of this application guide and will be left to the cable service provider's implementation.

Data Path	Flow	Description	Allowed or Denied
1	1.1	Registered integrated cable modem - DOCSIS Server	Allowed
	1.2	DHCT CPE - DHCP Server	Allowed
	1.3	Unsubscribed PC CPE – DOCSIS Server	Allowed
	1.4	Subscribed PC CPE– DOCSIS Server	Cable Service Provider's Implementation
	1.5	Registered integrated cable modem – non-DOCSIS Server	Denied
	1.6	DHCT CPE – non-DOCSIS Server	Cable Service Provider's Implementation
	1.7	Unsubscribed PC CPE – non-DOCSIS Server	Cable Service Provider's Implementation
	1.8	Subscribed PC CPE– non-DOCSIS Server	Cable Service Provider's Implementation

Data Path	Flow	Description	Allowed or Denied
2	2.1	Registered integrated cable modem - Registered integrated cable modem (across same/different CMTS)	Denied
	2.2	Registered integrated cable modem - Unregistered/Registered stand-alone cable modem (across same/different CMTS)	Denied
	2.3	Registered integrated cable modem - Unsubscribed/Subscribed PC CPE (across same/different CMTS)	Denied
	2.4	Registered integrated cable modem - DHCT CPE (across same/different CMTS)	Denied
	2.5	Unregistered/Registered stand-alone cable modem - DHCT CPE (across same/different CMTS)	Denied
	2.6	DHCT CPE - Unsubscribed /Subscribed PC CPE(across same/different CMTS)	Denied
	2.7	DHCT CPE - DHCT CPE (across same/different CMTS)	Denied
	2.8	Unsubscribed PC CPE - Unsubscribed /Subscribed PC (across same/different CMTS)	Cable Service Provider's Implementation
	2.9	Subscribed PC CPE- Subscribed PC CPE (across same/different CMTS)	Allowed

Data Path	Flow	Description	Allowed or Denied
3	3.1	Registered integrated cable modem - DBDS Network	Denied
	3.2	Unregistered/Registered stand-alone cable modem - DBDS Network	Denied
	3.3	DHCT CPE - DBDS Network	Allowed
	3.4	Unsubscribed/Subscribed PC CPE - DBDS Network	Denied
4	4.1	DOCSIS Server – Internet service provider Servers	Cable Service Provider's Implementation
5	5.1	Registered integrated cable modem – Internet	Denied
	5.2	DHCT CPE - Internet	Denied
	5.3	Unsubscribed PC CPE – Internet	Cable Service Provider's Implementation
	5.4	Subscribed PC CPE – Internet	Allowed
6	6.1	Application Servers Public Interface – Internet	Allowed
	6.2	Application Servers Private Interface – Internet	Denied
7	7.1	DBDS Network Elements – Internet	Denied
8	8.1	DBDS Network - DOCSIS Servers	Denied
	8.2	DBDS Network – non-DOCSIS Servers	Denied
	8.3	EMS - cable service provider's NMS server	Allowed
9	9.1	DBDS Network - DMZ	Denied
10	10.1	DHCT CPE - DMZ	Denied
	10.2	Registered integrated cable modem - DMZ	Denied
	10.3	Unsubscribed/Subscribed PC CPE - DMZ	Cable Service Provider's Implementation

DBDS Network Security

Introduction

This section provides a list of recommendations for the cable service provider to use to implement network security in their DBDS. The cable service provider may decide to implement packet filtering wherever they choose based on their network topology.

Because several of the security recommendations relate to each other, we assigned numbers to each recommendation for ease of reference. The recommendations are numbered in increments of 10 to allow for growth as new recommendations are added.

The way the cable service provider implements these recommendations can vary because each network topology is different and has its own unique features. This section provides security recommendations for Data Paths 1 through 10.

Data Path 1: Communication Between End-User Devices and DOCSIS Servers

Cisco recommends the following security measures for Data Path 1.

40

Configure Router 2 to *allow* IP traffic between:

- Registered integrated cable modems and DOCSIS servers
- DHCT CPE and DHCP servers
- Unsubscribed PC CPE and DOCSIS servers

50

Configure Router 2 to *deny* IP traffic between registered integrated cable modems and non-DOCSIS servers.

 # 60

Background: End-users may decide to forge their own DOCSIS configuration file that contains a higher level of service than what they paid for. The user may then use a variety of means to have their cable modem download this forged DOCSIS configuration file rather than the service provider's version of the file to receive an unauthorized level of service.

Recommendation: To reduce the risk of theft of service, take the following actions for CMTS:

- Specify a CMTS authentication string in the DOCSIS configuration file for integrated cable modems and stand-alone cable modems.
- Configure the CMTS authentication string per cable interface with this command (or other vendor-specific command): **cable shared-secret <string>**, where **<string>** must be identical to the CMTS authentication string specified in the configuration file.

Data Path 2: Communications Between End-User Devices

We recommend the following security measures for Data Path 2.

Note: Recommendations 70 and 90 apply to traffic across the *same* CMTS. Recommendations 100 through 120 apply to traffic across *different* CMTSs.

 # 70

Configure the CMTS to *deny* IP traffic among:

- Registered integrated cable modems and other remote registered integrated cable modems
- Registered integrated cable modems and unregistered/registered stand-alone cable modems
- Registered integrated cable modems and unsubscribed/subscribed PC CPEs
- Registered integrated cable modems and DHCT CPE
- Unregistered/registered stand-alone cable modems and DHCT CPE
- DHCT CPE and other remote DHCT CPE
- DHCT CPE and unsubscribed/subscribed PC CPE

 # 80

Configure the CMTS to *deny* any inbound IP traffic from the cable interface with a source IP address within the DBDS IP address subnet ranges. This recommendation reduces the risk of end users spoofing DBDS network elements in the HFC environment across the *same* CMTS.

 # 90

Configure the CMTS to *allow* IP traffic among subscribed PC CPEs.

 # 100

Configure Router 2 to *deny* IP traffic between:

- Registered integrated cable modems and other remote registered integrated cable modems
- Registered integrated cable modems and unregistered/registered stand-alone cable modems
- Registered integrated cable modems and unsubscribed/subscribed PC CPE
- Registered integrated cable modems and DHCT CPE
- Unregistered/registered stand-alone cable modems and DHCT CPE
- DHCT CPE and other remote DHCT CPE
- DHCT CPE and unsubscribed/subscribed PC CPE

 # 110

Configure Router 2 to *allow* IP traffic among subscribed PC CPEs (such as, those assigned public IP addresses).

 # 120

Configure Router 2 to *deny* any inbound IP traffic from the CMTS with a source IP address within the DBDS IP address subnet range. This recommendation reduces the risk of DBDS network element spoofing in the HFC environment (across different CMTSs).

 # 130

Background: This recommendation reduces the risk of spoofing of IP addresses by cable modems or their CPE devices. The "cable source-verify" command in the following recommendation can be configured per cable interface on a Cisco CMTS. This command allows the CMTS to verify that the upstream packets coming from each cable modem are associated with that cable modem. Packets with IP addresses that do not match those associated with the cable modem are dropped. When used with the dhcp option, the Cisco CMTS sends a DHCP LEASEQUERY message to the DHCP server to verify the IP address. If a valid response is received from the DHCP server, the CMTS updates its database with the new CPE device and allows future traffic through. If the DHCP server does not return a successful response, all traffic from the CPE is dropped.

Note: This feature requires that the DHCP server support the LEASEQUERY message. For example, the Cisco Cable Network Registrar (CNR) software supports LEASEQUERY in version 3.01(T) and later.

Recommendation: Configure the CMTS with the *cable source-verify (dhcp)* or vendor-specific equivalent command to verify that upstream packets are associated with the appropriate cable modem.

Data Path 3: Communication Between DBDS Private Network and End-User Devices

To implement the security recommendations for Data Path 3, the allocation of IP addresses to cable modems and PC CPEs operating on HFC nodes within the DBDS span of control should be within subnets distinct from DHCT CPE and all DBDS private network subnets, as described in recommendation #10. This type of allocation reduces the risk of data traffic from these devices entering the DBDS private network.

The cable service provider must include in their access list the specific subnets and port numbers that need to be filtered. A list of the ports specific to DBDS broadcast traffic can be obtained from Cisco.

Cisco recommends the following security measures for Data Path 3.

 # 140

Configure Router 1 to *allow* inbound IP traffic (from Router 2) destined to the DBDS private network from **only** DHCT CPE subnets.

 # 150

Background: Because access lists can affect performance, the cable service providers may choose to not implement Recommendation 150 if they implement Recommendation 140, even though the filter is closer to the source of the traffic if it is implemented on Router 2. However, according to the **High-Level View of Data Paths and Traffic Flows in the DBDS Network** diagram, earlier in this section, Router 1 is the gateway to the DBDS network and is an appropriate place to implement all the security policies pertaining to the DBDS private network.

Recommendation: Configure the CMTS or Router 2 to allow inbound IP traffic destined to the DBDS private network from *only* DHCT CPE subnets.

 # 160

Configure Router 1 to *deny* IP traffic between:

- Registered integrated cable modems and the DBDS private network
- Unregistered/Registered stand-alone cable modems and the DBDS private network
- Unsubscribed/Subscribed PC CPE and the DBDS private network

 # 170

Background: Any traffic destined to the DHCT CPE must originate from either the DBDS network or the DHCP server. Router 2 or the CMTS should use source address verification to reduce the risk of forwarding packets originating from other than the trusted DBDS network.

Recommendation: Configure Router 2 or the CMTS to *allow* IP traffic originated from only the DBDS or the DHCP server and destined to the DHCT CPE subnets.

 # 180

Background: A PC CPE connected to the Ethernet or USB port of a stand-alone cable modem can spoof a valid DHCT MAC address and thereby obtain a legitimate IP address from a DHCP server from the DHCT CPE IP address pool. Once the IP address is obtained, the PC CPE can now access the DBDS network.

To reduce the risk of access to the DBDS network in such a scenario, the cable service provider must add some specific filters in their deployed stand-alone cable modem configuration file that would deny access from *any* source (behind the cable modem) to the DBDS network. The cable service provider must carefully define the IP address range of the DBDS network that will be denied in the configuration file.

Recommendation: The configuration file for the stand-alone cable modem should contain filters that will specifically deny any traffic originated from the Ethernet or USB interface destined to the DBDS network. This recommendation reduces the risk of access to the DBDS network from any source behind a stand-alone cable modem.

 # 190

Background: If a PC CPE behind an integrated cable modem is configured with a valid DHCT CPE IP address, the PC CPE will have access to the DBDS network (if the CMTS is not properly configured with cable source-verify (dhcp) option (or an equivalent command from another vendor). In other words, a PC CPE can be configured to spoof a DHCT CPE IP address. To reduce the risk of spoofing of the DHCT CPE IP address behind the integrated cable modem, we recommend that you follow the security measures in the following recommendation:

Recommendation: The docsDevIpFilterTable filter in the integrated cable modem should be set to deny any traffic originated from the Ethernet or USB interface destined for the DBDS network. This recommendation reduces the risk of access to the DBDS network from a PC CPE configured with a valid DHCT CPE IP address (or spoofing a DHCT CPE) behind an integrated cable modem.

 # 200

Configure Router 1 to *deny* any inbound IP traffic (from Router 2 or Router 3) with a source IP address within the DBDS IP address subnet range. This recommendation reduces the risk of end users spoofing the DBDS network elements in the cable service provider's IP network.

 # 210

Background: The fewer programs, applications, and users that you allow on a host reduces the potential avenues that an attacker can use to compromise the host. Keeping services on any server to a minimum makes it tougher for the attackers to use that server as a springboard and therefore reduces the risk of other devices in the network getting compromised. Cisco recommends that you remove any unneeded programs, applications, users, and development tools from all DBDS servers. Examples of common network services and their associated ports that should be removed from any server unless absolutely required are DNS (53), FTP(21 and 20), HTTP (80), HTTPS (443), SMTP (25), POP (110), TFTP (69), DHCP (67 and 68), TOD (37), and telnet (23).

Recommendation: Remove any unnecessary programs, users, common network services, and associated ports from all DBDS network servers (for example, DNCS, Application servers, EMS), and leave only those required. This recommendation reduces the risk of vulnerability to attack on the DBDS.

 # 220

If telnet is required on any DBDS network element, the cable service provider should allow outbound telnet connections from that network element, but deny any inbound telnet connections unless authenticated.

 # 230

Background: As a general policy, Router 1 should allow outbound ICMP messages from the DBNDS network and allow selected inbound ICMP traffic. In addition to recommendations 230 through 260, you need to decide, based on your network needs, which other ICMP packets you wish to allow or restrict on the DBDS network.

Recommendation: Configure Router 1 to *deny* inbound ICMP redirect messages from any source.

 # 240

Configure Router 1 to *allow* outbound ICMP echo request messages from the DBDS network.

 # 250

Configure Router 1 to *deny* any inbound ICMP echo requests messages from any source. This recommendation reduces the risk of ping floods toward the DBDS network.

 # 260

Configure Router 1 to *allow* inbound ICMP echo reply messages only from DHCT CPE subnets.

 # 270

Background: An attacker inside the cable service provider's network may send a spoofed ICMP echo request packet (using any valid DBDS network element IP address) with a directed broadcast address (in this case a valid DHCT subnet, which is being used as a smurf reflector) as the destination and the victim's address as the source. This type of attack can cause unwitting accomplices to flood the victim. To reduce the risk of such attacks, Router 2 or the CMTS should be configured to *not* forward any IP directed broadcast traffic out of any interface. The command "no ip directed-broadcast" prevents a router from responding to ping packets that are addressed to the broadcast address.

Recommendation: Configure Router 2 or the CMTS on all interfaces with the command no ip directed-broadcast (or equivalent vendor-specific command). This recommendation reduces the risk of smurf attacks on the DBDS private network.

 # 280

Disable routing on all DBDS servers (for example, Application server and EMS) that are multi-homed (or have interfaces) on both the DBDS network *and* on the cable service provider's IP network.

Data Path 4: Communication Between Cable Service Provider Servers and Internet Service Provider Servers

It is assumed that security policies are already in place between the cable service provider's servers and the Internet service provider servers. Therefore, security measures for these servers are outside the scope this guide. If the cable service provider is the Internet service provider for the end-user, then Data Path 4 does not exist.

Data Path 5: Communication Between Cable Modems, CPEs, and the Internet

 # 290

Configure Router 3 to deny any regular traffic and broadcast traffic originating from the Internet to any cable modem or to any CPE with a private destination IP address.

 # 300

Background: After an end-user has subscribed to an Internet service provider, the PC CPE is assigned a public IP address that allows the user to access the Internet.

Recommendation: Configure Router 3 or the cable service provider's firewall to *allow* IP traffic from the subscribed PC CPE public IP address subnet to the Internet.

 # 310

Background: This recommendation reduces the risk of any spoofing of the stand-alone cable modem, integrated cable modem, DHCT CPE, Unsubscribed/ Subscribed PC CPE, and DOCSIS servers.

Recommendation: Configure Router 3 or the cable service provider's firewall to *deny* any traffic from the Internet with the following components:

- A private IP source address
- Any IP source address within the public Internet service provider address range reserved to the Internet service provider PC CPE customers

 # 320

Configure Router 3 or the cable service provider's firewall to *deny* IP and ICMP traffic from the HFC network (integrated cable modem, stand-alone cable modem, Unsubscribed PC CPE, or DHCT CPE) with a private source IP address destined to the Internet.

 # 330

Cable service providers must carefully manage the bandwidth that they allocate (using integrated cable modem configuration files) to high speed data customers connected to DHCTs. This recommendation reduces the risk of traffic flooding that could impair core DHCT functionality.

Data Path 6: Communication Between the Internet and the Application Servers

Data Path 6 is implemented with the standard configuration of the Cisco DNCS. It is assumed that the application servers communicate with specific servers on the Internet on specific ports designated by the application vendor, and that the security policies regarding this path are already in place on the cable service provider's network. Since the physical connectivity of those servers to the DBDS network is server-specific, it is assumed (and is recommended, if not implemented as such today) that those servers support two network interfaces. One interface handles internal DBDS traffic, and the other handles Internet traffic. It is also assumed that the application server vendor provides network address translation (NAT) functionality through a proxy server for any bi-directional traffic from DHCT CPE to the Internet.

 # 340

You must configure the application servers that require access to the Internet with support for two network interfaces. Configure one interface with a private IP address for DBDS traffic, and configure the other interface with a public IP address for Internet traffic.

 # 350

Background: Recommendation 350 is the same as Recommendation 280, but is repeated here specifically for the application servers.

Recommendation: Disable routing on all application servers that are multi-homed (or have interfaces) to both the DBDS network *and* the cable service provider's network.

Data Path 7: Communication Between DBDS Network Elements and the Internet

 # 360

Configure Router 3 or the cable service provider's firewall to *deny* IP and ICMP traffic from any network element in the DBDS private network destined to the Internet.

 # 370

Configure Router 3 or the cable service provider's firewall to *deny* any traffic from the Internet with a private source IP address. This recommendation reduces the risk of any DBDS network element spoofing (DNCS, EMS, QPSK, QAM, BIG, and so forth).

 # 380

Configure Router 3 or the cable service provider's firewall to *deny* IP and ICMP traffic coming from the Internet destined to any private IP address.

Data Path 8: Communication Between Server Farm and the DBDS Network

The physical connection of the Element Management System (EMS) server to both the DBDS network and to the cable service provider's network will be dependent on the cable service provider. It is assumed that the server will be multi-homed, but the cable service provider may ultimately choose to do otherwise. If multi-homed, then no traffic originated from the cable service provider is expected to cross Router 1. Therefore, you must apply security filters on Router 1 to deny any traffic originating from the cable service provider. If single-homed, then in addition to Router 1, the cable service provider should install some stateful inspection devices to filter at the application layer all traffic originated by the cable service provider.

 # 390

Configure Router 1 to *deny* any IP and ICMP traffic between the DBDS network and any server (DOCSIS and non-DOCSIS) for the cable service provider.

Data Path 9: DBDS Network – DMZ

DMZ, sometimes called a perimeter network, is defined as a segment or network added between a protected network and an external network, in order to provide an additional layer of security without compromising services. Cable service providers should keep the external untrusted side separate from the internal trusted side of their network.

The cable service provider can use the DMZ to connect hosts that need to have external access to the Internet. Examples of hosts that can be connected to a DMZ are Web servers and public mail servers.

 # 400

Configure Router 1 to *deny* any IP and ICMP traffic between the DBDS network and the DMZ segment.

Data Path 10: End-User Device – DMZ

 # 410

Configure Router 3 or the cable service provider's firewall to *deny* IP and ICMP traffic between the DMZ network and any end-user device with a private IP address.

Chapter 4
Configuring Mixed DOCSIS/DAVIC on the DNCS

Overview

Introduction

After implementing your security guidelines, you can configure Mixed DOCSIS/DAVIC on your DNCS. This chapter describes how to configure Mixed DOCSIS/DAVIC on your DNCS.

Assumptions

The instructions in this chapter assume that your DBDS will operate in a Mixed DOCSIS/DAVIC mode.

In This Chapter

This chapter contains the following topics.

Configure Mixed DOCSIS/DAVIC

Introduction

To configure Mixed DOCSIS/DAVIC on your DNCS, you must change the DHCT Communication Mode (DCM) of the bridge from DAVIC to Mixed DOCSIS/DAVIC. After changing the communication mode, you must send a DCM update message to all of the affected DHCT types and bridges so that the previously booted DHCTs can operate in the new Mixed DOCSIS/DAVIC mode.

This section provides instructions for configuring Mixed DOCSIS/DAVIC in your DBDS.

Before you Configure Mixed DOCSIS/DAVIC in the DBDS

Before you configure Mixed DOCSIS/DAVIC in your DBDS, you *must* complete the following tasks in the order in which they appear to ensure proper operation:

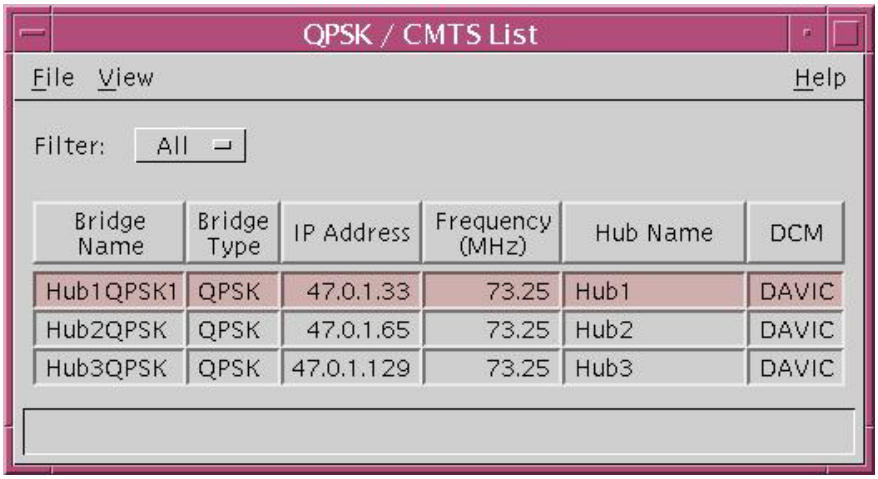
1. Install System Release 3.0. Refer to *System Release 3.0 Unipak Upgrade Installation Instructions*.
2. Install SARA 1.41 and PowerTV Home Gateway Edition 1.0. Refer to *SARA 1.41 and PowerTV Home Gateway Edition 1.0 Installation Instructions*.
3. Obtain a list of all the bridges that cover the targeted DHCTs from the site administrator. This list contains the QPSKs and CMTSs that need to have their DCMs set to Mixed DOCSIS/DAVIC.

Configuring Mixed DOCSIS/DAVIC Bridges in the DNCS

Complete the following steps to configure Mixed DOCSIS/DAVIC bridge(s) in your DNCS.

1. On the DNCS tab of the DNCS Administrative Console, click the **Element Provisioning** tab.
2. Click **QPSK/CMTS**.

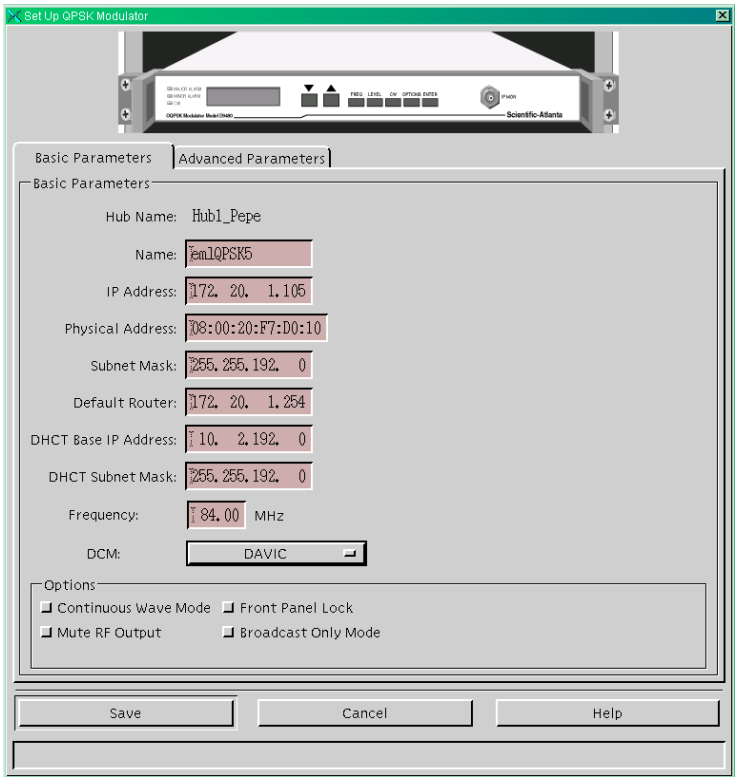
   Result: The QPSK/CMTS list window opens.



3. Select the row with the bridge name associated with the QPSK whose DCM you want to change.

4. Click the **File** menu and select **Open**.

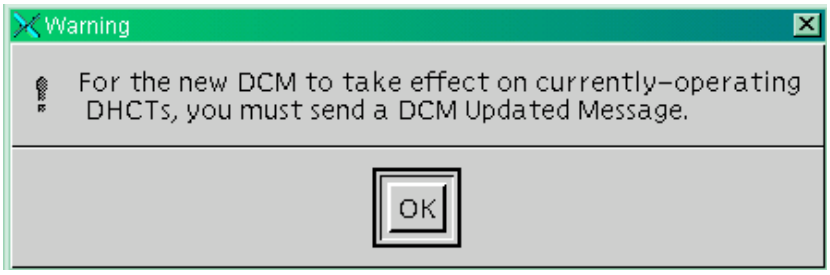
   Result: The QPSK Modulator window opens.



5. Click the DCM field and select **Mixed DOCSIS/DAVIC**.

6. Click **Save**.

   Result: The following warning appears.



7. Click **OK**.

   Result: The system returns to the QPSK Modulator window and the Cancel button changes to Close. The DHCTs can now boot in Mixed DOCSIS/DAVIC mode at startup.

8. Repeat steps 3 through 7 for each bridge that you need to configure.

9. Click **Close** to return to the QPSK/CMTS list window.

10. Leave the QPSK/CMTS list window open.

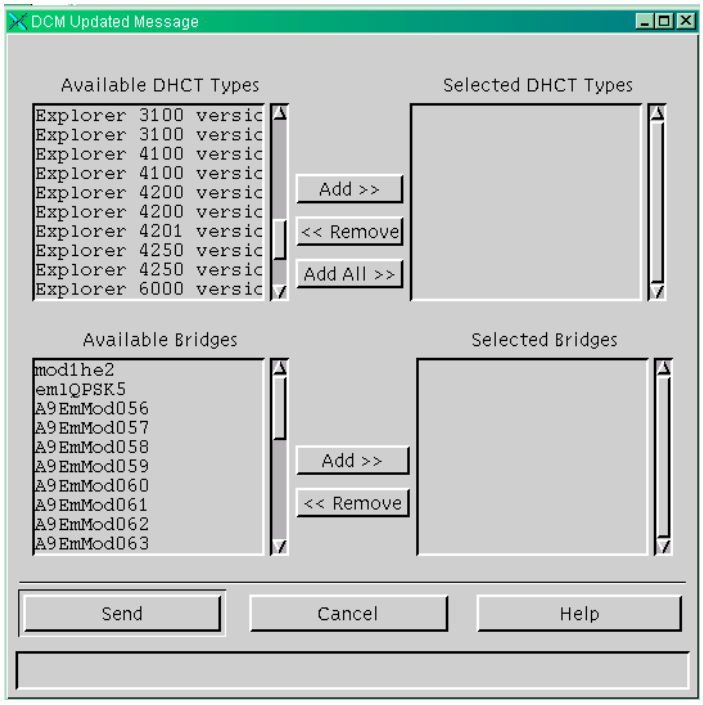
11. Your next step is to send a DCM Updated message to the selected DHCT types and bridges to allow the DHCTs to boot in the Mixed DOCSIS/DAVIC mode. Go to **Sending a DCM Updated Message,** next in this section.

Sending a DCM Updated Message

Complete the following steps to send a DCM Updated message for the affected bridges.

1. On the QPSK/CMTS list window, click the **File** menu and select **DCM Updated message**.

   Result: The DCM Updated message window opens.



2. In the Available DHCT Types column, select the DHCT type(s) that you want to operate in Mixed DOCSIS/DAVIC mode, and then click **Add**.

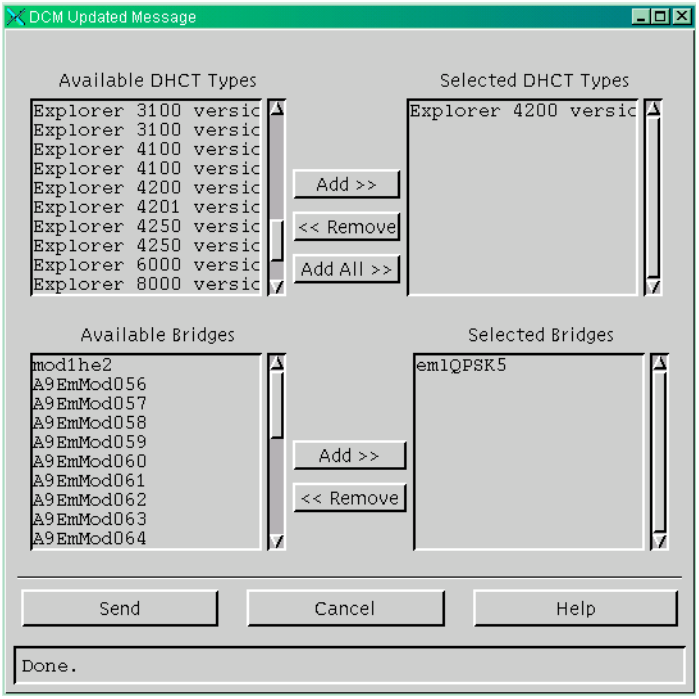
   Result: The selected DHCT type(s) move to the Selected DHCT Types column.

3. In the Available Bridges column, scroll through the list and select the bridge(s) whose DCM(s) you want to update, and then click **Add**.

   Result: The bridge name(s) move to the Selected Bridges column.

4. Click **Send**.

   Result: The system sends the DCM Updated message to cause the affected DHCTs to reboot and obtain the new DCM. When the update is complete, the message **Done** appears in the status field.



5. Click **Cancel** to return to the QPSK/CMTS list window.

6. Click the **File** menu and select **Close**.

   Result: The system closes the QPSK/CMTS list window and you return to the DNCS Administrative Console.

7. Click the **File** menu and select **Close** to exit.

Chapter 5
Staging DOCSIS-Capable DHCTs

Overview

Introduction

Staging is the process needed to prepare a DHCT for use by a subscriber. This DHCT may be a brand new unit, a field-return unit, or a Return Material Authorization (RMA) unit. Staging a DHCT involves two main tasks:

- Loading the current client release software onto the DHCT, including the Operating System (OS) and the Resident Application (ResApp)
- Loading authorization Entitlement Management Messages (EMMs) onto the DHCT

When a DHCT is properly staged, it has all of the software and the authorization information that it needs to display programming and other data in the subscriber's home and to function as an integrated cable modem.

This chapter explains how client release software is loaded and describes the various methods for loading authorization EMMs. For detailed staging procedures, refer to the *Explorer Digital Home Communications Terminal Staging Guide*, part number 734375.

Important: This application guide refers only to a PowerKEY CA environment.

In This Chapter

This chapter contains the following topics.

Load Client Release Software

CVT Download Process

The DNCS uses the Code Version Table (CVT) to load client release software into DHCTs. The CVT is a table that contains information about download channels and information to map client release software versions to DHCT types. Every QAM broadcasts the information contained in this table once per second, and the DNCS broadcasts it every 10 minutes on every QPSK and DSG CMTS.

If a DHCT does not have valid client release software installed, the DHCT will begin to search QAM frequencies for software download information. When the DHCT finds this information, it can begin to download valid client release software.

Load Authorization EMMs

Introduction

There are three methods for loading authorization EMMs. This section describes each of those methods and describes how to prepare your system to perform each process. These provisioning options are listed as follows:

- ModifyDhctConfiguration
- DhctInstantHit
- Fast Refresh List

For detailed staging procedures, refer to the *Explorer Digital Home Communications Terminal Staging Guide*, part number 734375.

ModifyDhctConfiguration

The ModifyDhctConfiguration process enables all PowerKEY configuration parameters of the DHCT or, in the case of a field return, reauthorizes it for default services. The first time you stage a DHCT and place it into an active inventory status, the ModifyDhctConfiguration transaction is sent to the DNCS.

The first time you stage a DHCT, when the DNCS receives a request to perform the ModifyDhctConfiguration transaction, it transmits at least 33 EMMs *twice* on the out-of-band QPSK and DSG CMTS Forward Data Channel to the DHCTs. Thereafter, every time the ModifyDhctConfiguration transaction is initiated, only the Service Authorization EMMs (typically four EMMs) will be transmitted. EMMs are transmitted regardless of the Admin Status of the DHCT.

You should wait 10 minutes after scanning the DHCTs into the billing system before booting the DHCTs or the conditional access data may not be received.

Note: If the DHCT did not receive the initial ModifyDhctConfiguration transaction, you cannot send an instant hit to the DHCT. The DhctInstantHit transaction, sometimes called an “instant hit,” initiates the transmission of all existing EMMs to the DHCTs.

DhctInstantHit

The DhctInstantHit transaction, sometimes called an "instant hit," initiates the transmission of all existing EMMs to the DHCTs. The DNCS and some billing systems can send an instant hit. During a DhctInstantHit, the DNCS transmits the EMMs regardless of the Admin Status of the DHCT. The DNCS transmits the PowerKEY information for the DHCT on the out-of-band QPSK or DSG CMTS channel.

You should send a DhctInstantHit transaction in the following circumstances:

- The ModifyDhctConfiguration transaction was initiated before the DHCT was ready to receive the EMMs.
- You wish to refresh the 30-day time stamp for the Service Authorization EMMs on a staged DHCT.
- You wish to perform a DhctInstantHit during certain troubleshooting situations, such as the following:
  - You are unable to enter the DHCTs into the billing system.
  - You are staging the DHCT in the subscriber's home.

Fast Refresh List

The Fast Refresh List is a queue of EMMs that the data carousel within the Broadcast File Server (BFS) distributes during or after the OS and ResApp downloads. The DNCS rebuilds the Fast Refresh List every 5 minutes. During the staging process, the billing system sends the ModifyDhctConfiguration transaction to the DNCS to add a DHCT to the Fast Refresh List. When the DNCS rebuilds the Fast Refresh List, the data carousel sends PowerKEY information to the new DHCT.

Every 5 minutes, the DNCS searches for DHCTs that have the following settings and adds them to the Fast Refresh List:

- FRL enabled
- Admin Status set either to In Service Two-Way or In Service One-Way (set by the ModifyDhctAdminStatus transaction)

The data carousel uses the inband QAM channel to distribute these EMMs to the DHCTs either during or after the OS and ResApp download.

If a DHCT boots and an Entitlement Agent (EA) is not present, the DHCT tunes to the inband QAM data channel and attempts for 5 minutes to receive its PowerKEY information. The 5-minute tuner lockout begins after the DHCT receives its System Information (SI) and BFS data. If the DHCT was enabled to use the Fast Refresh List and the Fast Refresh List has been rebuilt with the PowerKEY information for the DHCT, the DHCT receives its information during this time.

EMMs remain on the Fast Refresh List for 48 hours unless you send a ModifyDhctConfiguration transaction to remove the DHCTs from the Fast Refresh List. The Fast Refresh List can hold up to 250 DHCTs at one time.

Chapter 6
Setting Up a Home Network

Overview

Introduction

With the new DOCSIS-capable Explorer DHCT, subscribers can set up a network in their home. A home network adds a new level of interactivity to the digital cable TV experience and provides high-speed Internet access to other digital home devices, such as the PC. This chapter provides instructions for setting up a home network.

This section provides the instructions for setting up the home network. The subscriber can set up a home network by connecting the DOCSIS-capable DHCT directly to a PC or through a hub or a router. This section assumes that the DHCT is properly connected to the cable network and to the television. For connection diagrams, refer to the *Explorer 4200 Home Gateway User's Installation Guide*, part number 745461.

In This Chapter

This chapter contains the following topics.

Connect the DOCSIS-Capable DHCT Directly to a PC

Introduction

This section covers the equipment the subscriber must have to connect the DOCSIS-capable DHCT directly to a PC, and provides a procedure for connecting the equipment.

Equipment Needed

To connect a DOCSIS-capable DHCT directly to a PC, the subscriber must have the following equipment:

- A PC with an Ethernet port

  Note: Instead of an Ethernet port, a USB port may be used in conjunction with a USB-Ethernet adapter; this document refers to either configuration as an Ethernet port.
- The documentation on the Ethernet port
- A crossover Ethernet cable

Connecting the DOCSIS-Capable DHCT Directly to a PC

Complete these steps to connect a DOCSIS-capable DHCT directly to a PC.

1. Verify that the PC has an Ethernet port.
2. Connect the PC to the DOCSIS-capable DHCT using the crossover Ethernet cable.
3. Power on or reboot the PC and confirm that the DOCSIS-capable DHCT is powered on.

   Result: A link light appears on the Ethernet port of the PC indicating that the DOCSIS-capable DHCT and the PC are connected properly.

   Note: Refer to the documentation for the Ethernet port to determine the location of the link light.
4. Does the link light appear on the PC?
   - If **yes**, go to step 7.
   - If **no**, go to step 5.

5. Verify that the subscriber has completed the configuration properly by completing the following steps:
   a) Verify that the subscriber is using a crossover cable.
   b) Verify that the cable is plugged in on both sides.
   c) Verify that both the PC and the DOCSIS-capable DHCT are powered on.
6. Does the link light appear now?
   - If **yes**, go to step 7.
   - If **no**, call the cable service provider for assistance.

   Important: If the link light does not appear, there is a problem in the configuration. Call the cable service provider.
7. Confirm that the PC can connect to the Internet by opening a browser and browsing a Web site such as www.cisco.com. Can the subscriber browse the Web site?
   - If **yes**, the connections are made properly, and the subscriber has completed this procedure.
   - If **no**, go to step 8.
8. Open a command prompt (MS DOS prompt) and type **ipconfig /release** and press **Enter**.

   Result: The network interface releases any previously held addresses.
9. At the command prompt, type **ipconfig /renew** and press **Enter**.

   Result: The network interface attempts to get a new IP address, and then displays the network interface configuration.
10. Does the Ethernet port in use have an IP address that is not 0.0.0.0 and does not start with 169.254?
    - If **yes**, go to step 11.
    - If **no**, call the cable service provider for assistance.
11. Confirm that the PC can connect to the Internet by opening a browser and browsing a Web site such as www.cisco.com. Can the subscriber browse the Web site?
    - If **yes**, the connections are made properly, and the subscriber has completed this procedure.
    - If **no**, call the cable service provider for assistance.

Connect the DOCSIS-Capable DHCT to a PC Through a Hub

Introduction

This section covers the equipment the subscriber must have to connect the DOCSIS-capable DHCT to a PC through a hub, and provides a procedure for connecting the equipment.

Equipment Needed

To connect a DOCSIS-capable DHCT to a PC through a hub, the subscriber must have the following equipment:

- A PC with an Ethernet port

  Note: Instead of an Ethernet port, a USB port may be used in conjunction with a USB-Ethernet adapter; this document refers to either configuration as an Ethernet port.
- The documentation on the Ethernet port
- Two straight-through Ethernet cables
- A hub
- The documentation on the hub

Connecting the DOCSIS-Capable DHCT to a PC Through a Hub

Complete these steps to connect a DOCSIS-capable DHCT to a PC through a hub.

1. Connect a non-uplink port of the hub to the DOCSIS-capable DHCT using a straight-through Ethernet cable.
2. Power on the hub and the DOCSIS-capable DHCT.

   Result: A link light appears on the hub indicating that the hub is properly connected to the DOCSIS-capable DHCT.

   Note: Refer to the hub's documentation to determine the location of the link light.
3. Does the link light appear on the hub?
   - If **yes**, go to step 6.
   - If **no**, go to step 4.

4. Verify that the subscriber has completed the configuration properly by completing the following steps:

   a) Verify that the subscriber is using a straight-through Ethernet cable.

   b) Verify that the cable is plugged in on both sides.

   c) Verify that the DOCSIS-capable DHCT is powered on.

   d) Verify that the hub port in use is in non-uplink mode. (If applicable, ask the subscriber to try toggling the port mode using the Uplink button on the hub until the link light appears.)

5. Does the link light appear now?
   - If **yes**, go to step 6.
   - If **no**, call the cable service provider for assistance.

   Important: If the link light does not appear, there is a problem in the configuration. Call the cable service provider.

6. Connect a PC to another non-uplink port of the hub.

7. Power on or reboot the PC.

   Result: A link light appears on the hub port to which the PC is connected.

8. Does the link light appear on the hub?
   - If **yes**, go to step 10.
   - If **no**, verify that the subscriber has completed the configuration properly by completing the following steps:

     a) Verify that the subscriber is using a straight-through Ethernet cable.

     b) Verify that the cable is plugged in on both sides.

     c) Verify that the PC is powered on.

     d) Verify that the hub port in use is in non-uplink mode. (If applicable, ask the subscriber to try toggling the port mode using the Uplink button on the hub until the link light appears.)

9. Does the link light appear now?
   - If **yes**, go to step 10.
   - If **no**, call the cable service provider for assistance.

   Important: If the link light does not appear, there is a problem in the configuration. Call the cable service provider.

10. Confirm that the PC can connect to the Internet by opening a browser and browsing a Web site such as www.cisco.com. Can the subscriber browse the Web site?
    - If **yes**, the connections are made properly, and the subscriber has completed this procedure. Ask the subscriber to repeat steps 6 through 10 for any additional PCs he or she wants to connect to the DOCSIS-capable DHCT through the hub.

      Note: To connect the additional PCs, the subscriber must have received multiple public IP addresses from the cable service provider.
    - If **no**, go to step 11.

11. Open a command prompt (MS DOS prompt) and type **ipconfig /release** and press **Enter**.

    Result: The network interface releases any previously held addresses.

12. At the command prompt, type **ipconfig /renew** and press **Enter**.

    Result: The network interface attempts to get a new IP address, and then displays the network interface configuration.

13. Does the Ethernet port in use have an IP address that is not 0.0.0.0 and does not start with 169.254?
    - If **yes**, go to step 14.
    - If **no**, call the cable service provider for assistance.

14. Confirm that the PC can connect to the Internet by opening a browser and browsing a Web site such as www.cisco.com. Can the subscriber browse the Web site?
    - If **yes**, the connections are made properly, and the subscriber has completed this procedure.
    - If **no**, call the cable service provider for assistance.

Connect the DOCSIS-Capable DHCT to a PC Through a Router

Introduction

This section covers the equipment the subscriber must have to connect the DOCSIS-capable DHCT to a PC through a router, and provides a procedure for connecting the equipment.

Equipment Needed

To connect a DOCSIS-capable DHCT to a PC through a router, the subscriber must have the following equipment:

- A PC with an Ethernet port

  Note: A USB port may be used in conjunction with a USB-Ethernet adapter instead of an Ethernet port; this document refers to either configuration as an Ethernet port.
- The documentation on the Ethernet port
- Two straight-through Ethernet cables
- A router
- The documentation on the router

Connecting the DOCSIS-Capable DHCT to a PC Through a Router

Complete these steps to set up a home network by connecting the PC to the DOCSIS-capable DHCT through a router.

Important: If the subscriber is using a wireless router, Cisco recommends that the subscriber connect the PC through an Ethernet port on the router first, using the following procedure. After the subscriber successfully connects the PC to the DOCSIS-cable DHCT, the subscriber can then change the link between the router and the PC from Ethernet to wireless.

1. Connect the router's upstream or Internet port to the Ethernet port of the DOCSIS-capable DHCT using a straight-through Ethernet cable.
2. Power on the router and the DOCSIS-capable DHCT.

   Result: A link light appears on the router indicating that the router is properly connected to the DOCSIS-capable DHCT.

   Note: Refer to the router's documentation to determine the location of the link light.
3. Does the link light appear on the router?
   - If **yes**, go to step 6.
   - If **no**, go to step 4.

4. Verify that the subscriber has completed the configuration properly by completing the following steps:
   a) Verify that the subscriber is using a straight-through Ethernet cable.
   b) Verify that the cable is plugged in on both sides.
   c) Verify that the DOCSIS-capable DHCT is powered on.
   d) Adjust the upstream or Internet switch on the router until the link light appears.
5. Does the link light appear now?
   - If **yes**, go to step 6.
   - If **no**, call the cable service provider for assistance.

   Important: If the link light does not appear, there is a problem in the configuration. Call the cable service provider.
6. Connect a PC to a non-upstream port of the router.
7. Power on or reboot the PC.

   Result: A link light appears on the router to which the PC is connected.
8. Does a link light appear on the router?
   - If **yes**, go to step 10.
   - If **no**, verify that the subscriber has completed the configuration properly by completing the following steps:
     a) Verify that the subscriber is using a straight-through Ethernet cable.
     b) Verify that the cable is plugged in on both sides.
     c) Verify that the PC is powered on.
     d) Verify that the router port in use is in non-upstream mode. (If applicable, ask the subscriber to try adjusting the upstream or Internet switch on the router until the link light appears.)
9. Does the link light appear now?
   - If **yes**, go to step 10.
   - If **no**, call the cable service provider for assistance.

   Important: If the link light does not appear, there is a problem in the configuration. Call the cable service provider.

10. Confirm that the PC can connect to the Internet by opening a browser and browsing a Web site such as www.cisco.com. Can the subscriber browse the Web site?
    - If **yes**, the connections are made properly, and the subscriber has completed this procedure. Ask the subscriber to repeat steps 6 through 10 for any additional PCs he or she wants to connect to a DOCSIS-capable DHCT through a router.
    - If **no**, go to step 11.
11. Open a command prompt (MS DOS prompt) and type **ipconfig /release** and press **Enter**.

    Result: The network interface releases any previously held addresses.
12. At the command prompt, type **ipconfig /renew** and press **Enter**.

    Result: The network interface attempts to get a new IP address, and then displays the network interface configuration.
13. Does the Ethernet port have an IP address that is not 0.0.0.0 and does not start with 169.254?
    - If **yes**, the connection is working. Go to step 14
    - If **no**, call the cable service provider for assistance.
14. Confirm that the PC can connect to the Internet by opening a browser and browsing a Web site such as www.cisco.com. Can the subscriber browse the Web site?
    - If **yes**, the connections are made properly, and the subscriber has completed this procedure.
    - If **no**, check the configuration for the network access translation (NAT) and internal DHCP server or router, if the customer has NAT/DHCP functionality on the router; or call the cable service provider for assistance.

Chapter 7
Frequently Asked Questions

Overview

Introduction

This chapter provides answers to the most frequently asked questions about setting up DOCSIS in a DBDS environment.

In This Chapter

This chapter contains the following topic.

Questions and Answers

Introduction

This section provides the most frequently asked questions and answers about setting up DOCSIS in a DBDS environment.

List of Questions and Answers

Is the DOCSIS cable modem that resides in the DOCSIS-capable DHCT CableLabs Certified?

The cable modem in the DOCSIS-capable DHCT fully implements the DOCSIS 1.0 specification. At this time, there is no CableLabs certification process for DOCSIS cable modem functionality embedded in a DHCT. Cisco has conducted extensive tests to ensure that the DOCSIS-capable DHCT interoperates with any CMTS qualified by CableLabs for DOCSIS 1.0 or DOCSIS 1.1 operation.

Since there is a DOCSIS modem in the DHCT, doesn't that create a high-speed path directly to the TV? Won't this provide an easy conduit for IP-streamed movies?

There is no "direct" high-speed data path to the TV. IP data that is forwarded by the internal cable modem must be processed by some application. This application may be running on the DHCT or it may be running on a PC CPE that is receiving high-speed data service through the DOCSIS-capable DHCT. The cable system operator controls which applications can run on the DHCT.

Do both the DHCT CPE (RF) and cable modem (data) portions of the DOCSIS-capable DHCT have MAC addresses assigned to them?

Yes. The CM MAC address (or Ethernet MAC address) is derived by taking the RF MAC address and adding one (CM MAC = RF MAC + 1). The RF MAC address label is located on the back panel of the DHCT. To confirm the MAC address, please refer to the label found on the back of each DHCT. The arrow in the sample label below points to the MAC address.

Note: You can also locate the CM MAC address and RF MAC address on page 3 of the diagnostic screens, Versions and Serial Numbers. For more information, refer to *Understanding Diagnostic Screens for the Explorer® Digital Home Communication Terminals Application Guide,* part number 749244.

Do both the DHCT CPE (RF) and cable modem (data) portions of the DOCSIS-capable DHCT have IP addresses assigned to them?

Yes. The DHCP server assigns IP addresses to both the DHCT CPE and the cable modem.

If I press the Power button on the front of the DOCSIS-capable DHCT, will it turn off the cable modem as well?

No. The cable modem is always on until the power is disconnected from the DHCT. The Power button simply toggles on-and-off the video portion of the DHCT.

Are there any differences in staging a DOCSIS-capable DHCT compared to other Cisco DHCTs that are not DOCSIS-capable, such as the Explorer 3250?

Yes. Because the DOCSIS-capable DHCT has an internal cable modem, the staging process requires additional steps for the cable modem. As for previous generations of Explorer DHCTs, each DHCT has an RF MAC address that must be made known to the DNCS. The RF MAC address is present on the CD-ROM issued by Cisco for each shipment of DHCTs, and is printed on the rear label of the DHCT.

The cable modem within the DOCSIS-capable DHCT uses the DHCT's Ethernet MAC address. The Ethernet MAC address is one number higher than the RF MAC address. DOCSIS registration is keyed to this MAC address. An IP address must be issued to the cable modem by the cable system's DHCP server. Depending on the operator's policy, this server may require prior knowledge of a DHCT's Ethernet MAC address before issuing an IP address. To implement this policy, DHCT Ethernet MAC address may be manually loaded into the DHCP server, or entered using custom scripts .

An alternative to prior knowledge of all DHCT Ethernet MAC address is to allow the DHCP server to issue an IP address to the cable modem based on "option 43 suboption 5" in the DHCP DISCOVER/REQUEST message. This field identifies the cable modem as residing within the DOCSIS-capable DHCT. This type of policy requires that the operator enter a rule on the DHCP server so that the relevant field is recognized.

Does the CMTS need to "talk" to the DNCS since the DOCSIS-capable DHCT will be interacting with both?

Ethernet connections between the CMTS and the DNCS must be present, but the CMTS and DNCS do not need any customized host-to-host communication. As far as the DNCS is concerned, the CMTS is merely an IP router or Ethernet bridge on the path to the DHCT. From the CMTS perspective, the DNCS is simply a host that legitimately communicates with selected CPE that resides on the CMTS's RF interface.

How does the OOB data get to the CMTS so that it can use the DOCSIS path to the DOCSIS-capable DHCT?

DBDS-specific downstream broadcast data that is originated at the DNCS can be forwarded through DAVIC QPSK modulators (for DAVIC and Mixed DOCSIS/DAVIC mode only) and also through the DOCSIS CMTS's (for DOCSIS mode only). The DNCS sends the data to the CMTS by encapsulating it within IP packets and setting the destination IP address to a value that has been configured on the CMTS. (This same mechanism is used for the DAVIC QPSK transmitters.) For this data to pass through the CMTS, the CMTS must implement the *CableLabs DOCSIS Set-top Gateway (DSG) Interface Specification*. Essentially, the DSG function in a CMTS accepts data addressed to some provisioned IP address and forwards it to the DOCSIS downstream channel. The CMTS places a well-known Cisco MAC address in the "destination address" field of these Ethernet frames. DHCTs that are operating in DOCSIS mode and are tuned to the DSG CMTS receive the out-of-band data by accepting all frames with the well-known Cisco MAC address.

Will the DOCSIS-capable DHCT still be able to decode video if the DOCSIS path/CMTS fails?

Yes. Video functions continue to work without interruption. Advanced services that do not require immediate message exchange also continue to work, though some interruptions will occur if interactive communication is not restored before protocols time out. Interactive services are interrupted until the DOCSIS cable modem system returns to its operational state. The impact of losing the DOCSIS channel is covered in **DHCT Behavior After Initialization** in Chapter 1 of this guide.

I have not implemented DOCSIS completely in my system, or I have not yet installed System Release 3.0 – can the DOCSIS-capable DHCT be installed in a DAVIC-only mode?

Yes. When the DOCSIS portion of the system is functional at a later date, the DHCT can be rebooted or updated (with a DCM Updated message) to begin using OOB and high-speed data using the DOCSIS path.

What are the basic OS/SARA/SR requirements for the DOCSIS-capable DHCT?

To use a DOCSIS-capable DHCT, your system must be operating with the following software versions:

- System Release (SR) 3.0
- Cisco Resident Application (SARA) 1.41/Home Gateway Edition 1.0

Note: Sites using another vendor's resident application need to contact the vendor for their version of DOCSIS compatible operating system and resident application.

Is there anything special that needs to happen if the subscriber wants to connect the DOCSIS-capable DHCT directly (rather than through a router or hub) to a computer using an Ethernet cable?

Yes. For this connection, the subscriber must use a crossover Ethernet cable to connect the DOCSIS-capable DHCT directly to a PC rather than using a straight-through Ethernet cable.

Index

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

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

March 2012 Printed in USA

Part Number 4000358 Rev B