CISCO™

Configuring the PowerKEY DVB System for System Release i4.3

Instructions

Please Read

Important

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

Notices

Trademark Acknowledgments

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

DVB is a registered trademark of the DVB project.

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 13 Configuring the System for Satellite and Terrestrial Support 163

Chapter 14 Messaging 173

Chapter 15 Troubleshooting 183

Chapter 16 Customer Information 199

Appendix A Sources and Services Naming Conventions 201

Glossary 205

About This Guide

Introduction

The PowerKEY® DVB System provides international markets with a cost-effective, field-proven, end-to-end platform for deploying digital video and interactive services. This guide for the PowerKEY DVB System describes the changes to the Digital Network Control System (DNCS) and the Digital Broadband Delivery System (DBDS) that are unique to the PowerKEY DVB System for System Release (SR) i4.3 and provides configuration and installation procedures.

The PowerKEY DVB System Application Server (AppServer) works with the DNCS to deliver digital applications to subscribers. The Application Server and the DNCS form the core of the DVB DBDS. The DBDS delivers broadcast data and digital applications from the headend to the subscribers' homes.

For simplicity, this guide does not always explicitly refer to the DVB products using the DVB prefix. For instance, all references to "Application Server" in this guide also imply the "DVB System Application Server."

The DBDS is our solution for broadband delivery conforming to the DVB-SI specifications.

Note: This guide contains procedures for defining digital applications as well as deleting and changing the definitions for these applications. You will not complete these procedures in the order they are presented here. Also, you will not necessarily use all of the procedures in this guide, depending on the applications that you offer to your subscribers.

Purpose

This guide presents a high-level overview of the PowerKEY DVB System. After reading this guide you will be able to better understand the changes to the DBDS and the DNCS that are specific to the PowerKEY DVB System, and you will be able to configure, install, operate, and maintain the PowerKEY DVB System for SR i4.3.

Scope

This guide primarily provides documentation for procedures that are *specific* to the PowerKEY DVB System for SR i4.3. For help with procedures that are common to both the North American system and the PowerKEY DVB System, refer to the online Help.

Audience

This guide is written for PowerKEY DVB System operators, installers, system engineers, and Cisco Services support engineers.

Document Version

This is the second formal release of this document.

1

Introducing the PowerKEY DVB System

Introduction

The PowerKEY DVB System is a real-time interactive network designed to support not only today's digital services, but also services in the future. The PowerKEY DVB System provides several key advantages for cable service providers:

- Future-proof design based on open standards and published interfaces allows quick and easy system upgrades

- Lowers operating and capital costs for deploying digital interactive services

- Saves time for launching interactive services

- Reduces technical risk and schedule slippage by providing pre-integrated, off-the-shelf, interactive applications such as Electronic Program Guide (EPG), video-on-demand (VOD), e-commerce, and e-mail

What's New for System Release i4.3?

Specifically, changes were made to the DBDS and the DNCS user interface to support the implementation of the following features in the PowerKEY DVB System for SR i4.3:

- External Download Interface Support

- EMM Carousel Improvements

- Database Support for Increased Number of Set-Tops

In This Chapter

What is the PowerKEY DVB System?

Introduction

The PowerKEY DVB System is a combination of state-of-the-art products that are pre-integrated, tested, and offered together as a complete solution to provide digital video and interactive TV services. The following list highlights some of the features of the PowerKEY DVB System:

- The PowerKEY DVB System utilizes a Direct ASI card installed in the DNCS that is configured during installation to process BFS data.

- The D96xx/DCM re-multiplexers transmit DVB SI data into the system.

- The PowerKEY DVB System uses DVB-compliant Digital Home Communications Terminals (DHCTs) that contain the ST operating system (OS).

- The PowerKEY DVB System uses MQAM modulators with a maximum of two RF output ports used in DVB mode.

- The encryption method is PowerKEY conditional access (PCG, SCS and DNCS) and the Transaction Encryption Device (TED) functions the same as in the non-PowerKEY DVB system.

Features

The PowerKEY DVB System offers the following features:

- A reliable, field-proven platform for digital video and interactive services

- An end-to-end solution for providing interactive services

  - DVB headend equipment

  - Interactive control center

  - DVB DHCTs with the ST OS

  - Middleware

  - Client applications

  - Professional support services

- PowerKEY conditional access system is a full-featured security system

DVB Headend Equipment

The PowerKEY DVB System uses various combinations of some or all of the following DVB headend equipment to allow flexibility for varying system requirements:

- Galaxy chassis

  - Titan satellite receiver

  - Indus descrambler

  - Spectra QAM demodulator

- MPEG encoders

  - Regulus controller (stat mux control)

  - Polaris encoder (multichannel)

  - Pyxis encoder

- Multiplexers

  - D96xx re-multiplexers

    Note: The D96xx re-multiplexers contain one output, and the number of inputs varies based on the model type.

  - DCM transrater

- ECMG

  - PCG

- QAM modulators

  - Quantum RF card

  - Quasar MKII modulator

  - Mercury QAM modulator

  - MQAM modulator

- BFS

- GoDB Servers

Remote Headend Configuration

The following diagram illustrates a typical PowerKEY DVB System network incorporating a remote headend:
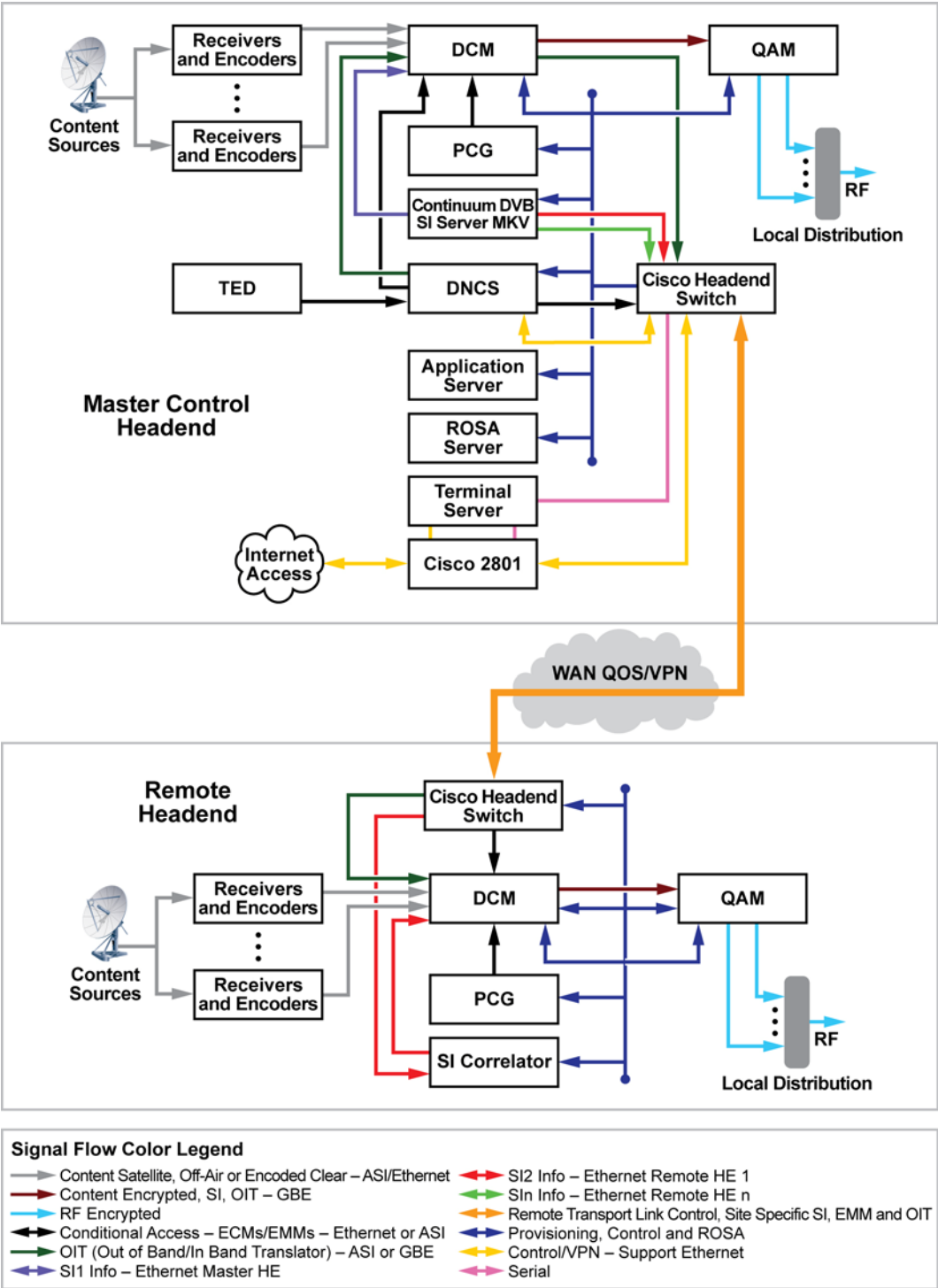
The Interactive Control Center

The PowerKEY DVB System control center consists of the following devices and corresponding service applications:

- DNCS
    - Interface to SMS/billing computer
    - Interactive session manager
    - DSM-CC data carousel for fast application downloads
    - DHCT configuration
    - Addressable Messaging and credit-based PPV
- TED high-performance conditional access system
- PowerKEY DVB System Applications Server provides digital applications, applications file storage, and pay-per-view (PPV) services
- ROSA™ Element Manager
    - Headend equipment configuration
    - Headend equipment monitoring and alarm management
- SI-Server for DVB SI generation and editing
- PowerKEY Conditional Access Gateway

DNCS Monitor Windows

DNCS Administrative Console Status Window

Use the DNCS Administrative Console Status window to determine the overall status of various processes. To determine the status of the individual Application Server processes, see *AppServer Control Window* (on page 7).

The DNCS Administrative Console Status window is divided into the following two areas:

- DNCS
- AppServer

The following illustration indicates that the DNCS and the Application Server (AppServer) are all running. If one of these elements was not running, the associated box would appear red (instead of green) and display **Inactive** (instead of **Running**).
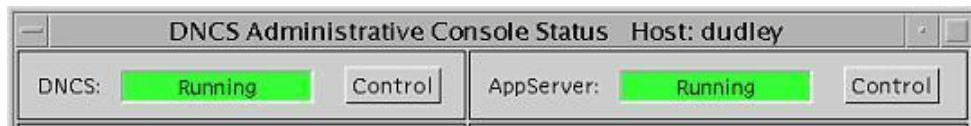
AppServer Control Window

If you click the **Control** button in the AppServer area of the DNCS Administrative Console Status window, the AppServer Control window appears. The AppServer Control window provides a list of all the processes on the Application Server workstation, along with the working state of each.

We recommend that you leave the AppServer Control window open and visible at all times to help you monitor the system. The following list describes the different working states that can appear on this window:

- Green—The process as a whole is running, although a sub-process may be paused.

- Yellow—The process has not finished starting up or shutting down, or the process is waiting for a sub-process to finish starting up or shutting down.

- Red—The process has stopped or did not start.

After the Application Server is up and running, all of these processes should be green. If any of them are red or yellow, there is a problem with that process, and you should contact Cisco Services.

Some processes restart automatically in response to an error. If this happens, the status indicator cycles through red, yellow, and green as the process shuts itself down, restarts itself, and then becomes active.

DNCS Administrative Console Window

Frequently called the Admin Console, the DNCS Administrative Console is the window you use most often as you operate the PowerKEY DVB system.
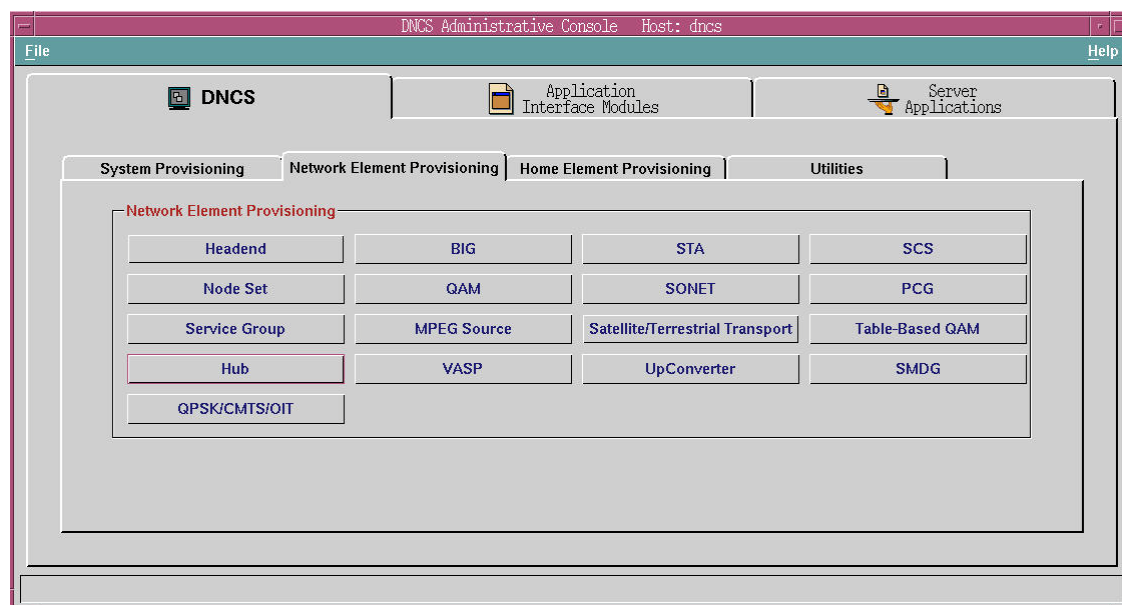
DNCS Administrative Console Window Tabs

Each of the three primary tabs on the DNCS Administrative Console provides access to specific functions.

The following table describes the specific functions of the primary tabs on the DNCS Administrative Console.

Tab	Description
DNCS	Allows you to provision basic digital services and manage DBDS hardware on the DNCS
Application Interface Modules	Allows you to set parameters for the DNCS to interact with DHCTs and service providers (for example, HBO or Internet services) to permit a smooth transfer of information between the service providers and DHCTs
Server Applications	Provides access to applications that reside on the Application Server so that you can enable DHCTs to offer services associated with those applications to subscribers **Note:** The options that appear on this tab vary depending on the applications available on your system.

Use the Server Applications tab to provision Application Server applications. For more information on using the other tabs in the DNCS tab, refer to the online Help.

Online Help

Introduction

The DNCS Online Help provides additional information about a window or a particular procedure. This section describes the different ways you can access the DNCS Online Help.

List Windows

If you are viewing a window that provides a list of items, access the Online Help by clicking **Help** on the toolbar as indicated in the following illustration.


A list appears with the following options:

- Version

- Online Help

If you select **Version**, the system opens the Internet browser with a list of software versions installed on your DNCS workstation.

If you click **Online Help**, the system opens the DNCS Online Help in the Internet browser.

Setup Windows

If you are viewing a window that allows you to set up a network element, access the Online Help by clicking the **Help** button located at the bottom of the window as indicated in the following illustration.
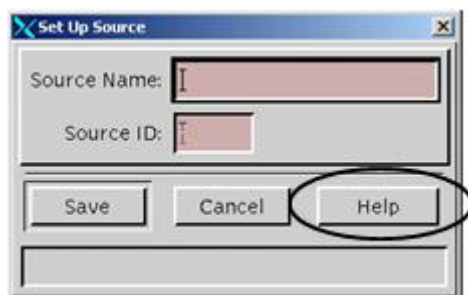
The system opens the DNCS Online Help in the Internet browser.

Finding Information

You can use any of the following methods to find information you need in the DNCS Online Help:

- Click the topic in the **Contents** list.

- Click the **Index** tab and type a keyword.

- Click the **Search** tab and type a keyword.

- Click the **Troubleshooting** topic in the **Contents** list for help resolving errors you may be experiencing.

- Click the **Glossary** topic at the bottom of the **Contents** list for definitions of terms used throughout the Online Help.

Conventions

At the beginning of most procedures in the DNCS Online Help is a Quick Path for getting to a specific GUI window to perform the procedure. The following example shows the Quick Path for opening the Source Definitions List window.

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Source Definitions

As you become more experienced in using the DNCS, these Quick Paths may be the only reminders you need of how to perform certain tasks. In this example, you would use the Quick Path to perform the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 On the DNCS tab, click the **System Provisioning** tab.

3 On the System Provisioning tab, click the **Source** button. The Source List window opens.

4 On the Source List window, click once on the source name (**[Source Name]**) whose definition you need.

5 Click on the **File** menu, and then select **Source Definitions**. The Source Definitions List window opens for the source you selected.

Navigation Tips

The following tips may help you to navigate more efficiently around the DNCS and the Online Help:

■ To open a window for an existing item on the DNCS, the procedures in the Online Help advise you to click once on the item name; then, click **File** and select **Open**. In most cases, you can simply double-click on the item name to open the window, if you prefer.

■ To return to a Help topic you have previously visited, click **Go** on your browser toolbar, and then choose **Back** from the drop-down menu that appears. You can also click the right mouse button in the Help topic window and select **Back** from the menu that appears.

■ Occasionally, a Help page may not display properly. This is especially true if you try to resize the Help window. If this happens, simply close the Online Help and then re-open it.

Printing Help Topics

If your system has print capabilities, you can print any Help topic by completing these steps:

1 Click once within the topic to select that area (frame).

2 Click File on your browser toolbar, and then select Print Frame from the menu.

2

Chapter 2

Configuring the PowerKEY DVB System

Introduction

To deploy the PowerKEY DVB System to function properly within your headend, you must configure the SI-Server, the D96xx re-multiplexers, the DCM and the remaining elements of the PowerKEY DVB System. This chapter provides a high-level overview of the procedures necessary to configure the SI-Server, the D96xx re-multiplexers, the DCM, and the PowerKEY DVB System.

In This Chapter

Configure the PowerKEY DVB System

Introduction

This section provides a high-level overview of the procedures required to configure the PowerKEY DVB System for SR i4.3 and lists the references in this guide that correspond with each procedure.

Important: Where the DNCS screens or procedures have changed, this guide provides a complete procedure. Where the screens and procedures are the same as non-PowerKEY DVB systems, refer to the online Help.

Note: Read this entire guide before configuring the PowerKEY DVB System, and follow these procedures in the order shown.

Configuring the PowerKEY DVB System

The following table shows the procedures you must follow to correctly configure the PowerKEY DVB System for SR i4.3.

Stage	Procedure	Reference
1	Configure the SI-Server, the D96xx re-multiplexers, and the DCM	Chapter 2
2	Set up hubs, MPEG sources, MQAM modulators, PowerKEY Conditional Access Gateways (PCGs), and simulcrypt synchronizers (SCSs)	Chapter 3
3	Set up OIT bridges and re-configure all D96xx re-multiplexers (including the Home D96xx)	Chapter 4
4	Set up Direct ASI and obtain MPEG program numbers	Chapter 5
5	Create sources and set up sessions	Chapter 6
6	Configure PPV services	Chapter 7
7	Configure the Broadcast File System	Chapter 8
8	Authorize Features with Named Entitlement	Chapter 9
9	Configure Multiple Bootloader Carousels	Chapter 10
10	Monitor the System Remotely	Chapter 11
11	Configure the System for State Administration of Radio, Film, and Television (SARFT)	Chapter 12
12	Configure the System for Satellite Support	Chapter 13
13	Configure Messaging	Chapter 14
14	Troubleshoot the System	Chapter 15

Configure the SI-Server, D96xx Re-multiplexers, and the DCM

Introduction

This section provides a high-level overview of the procedures for configuring the SI-Server, D96xx re-multiplexers, and the DCM for the PowerKEY DVB System in SR i4.3.

Configuring the SI-Server, D96xx Re-Multiplexers, and the DCM

1   On the SI-Server, access the ROSA Element Manager. For step-by-step instructions, refer to the following manuals for instructions for using the SI-Server and the ROSA Element Manager:

   ▪ *SI-Server Complete SI Solution User Manual*

   ▪ *ROSA Network Management System User's Guide*

2   On the SI-Server, add all D96xx re-multiplexers to the ROSA database.

3   Configure the D96xx re-multiplexers.

   Important: If used in scrambling mode, enable all scrambling licenses.

   Note: Refer to the *Continuum DVP D9600 Advanced Headend Processor Re-multiplexer and Transport Stream Processor Series Installation and Operation Guide* for additional information to configure the D96xx re-multiplexers.

4   Synchronize the time of day on the SI-Server using ROSA.

5   Pass services to the outputs of the D96xx re-multiplexers.

   Important: Write down all of the program numbers on each D96xx output. You will need these program numbers later when you create SI tables.

6   Configure the D96xx re-multiplexers to generate the time offset table (TOT).

7   On the SI-Server, generate the service descriptor table ([SDT] actual and other), and distribute the SDT to the corresponding D96xx re-multiplexers.

8   On the SI-Server, generate the network information table (NIT) and distribute the NIT to all D96xx re-multiplexers.

9   If applicable to your system, use the SI-Server to generate the bouquet association table (BAT) and then distribute the BAT to all D96xx re-multiplexers.

   Note: The BAT is a collection of services similar to a channel map.

10 On the SI-Server, set up the Electronic Preview Guide (EPG) scheduler and the event information table (EIT) to generate the EIT present/following and schedule tables for each D96xx re-multiplexer.

Enable PowerKEY DVB Features and Licenses

Introduction

This section provides procedures for enabling features and licenses for the PowerKEY DVB System in SR i4.3.

Enabling PowerKEY DVB Features

The following support features must be enabled using the AddDncsFEATURESupport script:

- PowerKEY DVB

- PowerKEY CAS Gateway (PCG)

- Direct ASI

Important:

- You must enable the PCG feature in order for the DNCS to support SCS/PCG devices.

- You must enable the Network Binding feature to bind the DHCTs to a hub in a multiple hub configuration and to set up EMM filtering.

- You must enable the satellite and Terrestrial support in order for the DNCS to support the conditional access system for satellite set-tops.

Note: Contact the representative who handles your account for additional information about obtaining and running the .AddDncsFEATURESupport script.

Enabling PowerKEY DVB Licenses

Use the licenseGen script to configure the PowerKEY DVB licenses required to operate the system. Contact the representative who handles your account for additional information about obtaining and running the licenseGen script.

Disabling the Application Server

In the PowerKEY DVB System, the Application Server is an optional feature. If you are not using the Application Server, or if the Application Server is not present, you must add the following environment variable to the /export/home/dncs/ .profile file:

export   PKDVB_APPSERV_NOT_PRESENT=1

Important: For the change to take effect, you must restart the DNCS processes after you change the environment variable.

Operational Considerations

This section includes some of the operational considerations you should be aware of when configuring the PowerKEY DVB system.

Changing the Home Transport Frequency

Under normal operating conditions, the Home Transport Frequency should not be changed. However, if an operator changes the MQAM Home Transport Stream frequency, the QAM frequency modified in the DNCS QAM GUI is not updated in the DNCS database. This causes the set-top to begin to search for the correct frequency. The result is that the set-top may lock on to an incorrect frequency.

Normally the home transport frequency is not touched by the operator. However, when the operator stops and restarts (bounces) the OSM/hctmInd process, the MQAM modulator should pick up the newly-assigned home transport frequency.

Workaround: If the home transport frequency is changed, then the OSM session (199) should be torn down and siManager should be bounced.

Enabling Feature Authorization

Feature authorization (also known as named entitlement) allows you to enable or disable specific set-top features from the DNCS. For example, you can enable or disable the games feature for a set-top from the DNCS.

To enable feature authorization, you must complete the following steps.

1   Type the following command to stop DNCS processes:
    dncsStop

2   Add the following entry in the .profile file:
    export CAM_NAMED_ENTITLEMENT=TRUE

3   Type **source /export/home/dncs/.profile** so the DNCS will use the updated .profile file.

4   Type the following command to start DNCS processes:
    dncsStart

Disabling Feature Authorization

To disable feature authorization, you must complete the following steps.

1 Type the following command to stop DNCS processes:
   dncsStop

2 Delete the following entry in the .profile file:
   export CAM_NAMED_ENTITLEMENT=TRUE

3 Type **source /export/home/dncs/.profile** so the DNCS will use the updated
   .profile file.

4 Type the following command to start DNCS processes:

   dncsStart

Enable External Download Interface Support

Prior to this release, the set-top Image (ROM) management was performed only on
the user interface of the DNCS. This release offers an external web (SOAP based)
interface to allow any third-party front-end application to perform the set-top image
management activities.

This external interface enables the third-party web service client applications to
perform the following set-top image management activities

■ Upload images to the DNCS

■ Delete images from the DNCS

■ Send CVT triggers to a set-top or group of set-tops through the DNCS

■ Query the DNCS for the list of firmware files uploaded, groups, DHCT versions,
  and CVT triggers available.

Add the Environment Variable for the External Download Support Feature

Complete the following steps to add the necessary environment variable to the
DNCS for the External Download Support Feature.

1 Type the following command to stop DNCS processes:
   dncsStop

2 Add the following entry in the .profile file:
   export DNCSINIT_IPADDR =[IP address of DNCS]

3 Type **source /export/home/dncs/.profile** so the DNCS will use the updated
   .profile file.

4 Type the following command to start DNCS processes:
   dncsStart

5 Continue with *Enable the External Download Support Feature* .

Enable the External Download Support Feature

Complete the following steps to enable external download support.

1 Open an xterm window and log into the DNCS as root.

2 Type **dncsStop** and press **Enter**.

3 Execute the following command to display the DNCS Features Configuration screen:
'.AddDncsFEATURESupport'

4 Navigate to the **External Download Interface** feature and set it to Enable.

5 Save the configuration settings.

6 Close the DNCS Features Configuration screen.

7 From the xterm window, restart the DNCS processes as follows:

8 Type **dncsStart** and press **Enter**.

9 Continue with *Set Up External Access for Third-Party Front-End Applications* (on page 21).

Set Up External Access for Third-Party Front-End Applications

Typically, the DNCS does not allow connections from external servers as a security measure. Complete the following steps to enable access from a specific IP address.

1 If necessary, log in as root from an xterm window on the DNCS as follows:

   a Type **su**; then, press **Enter**.

   b Type the root password; then, press **Enter**.

2 Execute the following command to stop the Apache web server:

   svcadm disable svc:/network/http:apache2

3 Type **vi /usr/local/apache/conf/httpd.conf** and then press **Enter**.

4 Navigate to the [Location] header and add the following line:
   Allow from [IP address]
   Note: Replace "IP address" with the IP address of the external server.
   Example: Allow from 192.168.100.1

5 Save the changes and close the httpd.conf file.

6 Execute the following command to start the Apache web server:
   svcadm enable svc:/network/http:apache2

7 Go to *Configure Additional Parameters for SOAP Requests* (on page 21) if you need to make additional configuration changes to the SOAP requests. Otherwise, setup is complete.

Configure Additional Parameters for SOAP Requests

Complete the following steps to enable or disable additional configuration parameters for the External Download Interface Support feature.

1 If necessary, log in as root from an xterm window on the DNCS as follows:

   a Type **su** and press **Enter**.

   b Type the root password and press **Enter**.

2 Type **cd /dvs/dncs/etc/** and press **Enter**.

3 Type **vi OsmSOAPCfg.cfg** and press **Enter**.

4 Set the parameters you wish to configure to Enable or Disable.

5 Type **:wq** and press **Enter** to save and close the file.

6 Restart the DNCS processes as follows:

   a Type **dncsStop** and press **Enter**.

   b Type **dncsStart** and press **Enter**.

Add the Environment Variables to Support EMM Carousel Improvements

For systems upgrading from release 1.4.2 or lower, you need to complete the following steps to implement the EMM Carousel improvements provided by your upgrade.

1   Type the following command to stop DNCS processes:

dncsStop

2   Add the following entries in the .profile file:

export EMM_DIST_CYCLE_HOURS=[number of Hours]

3   Type **source /export/home/dncs/.profile** so the DNCS will use the updated .profile file.

4   Type the following command to start DNCS processes:

dncsStart

5   Type the following command to stop DNCS processes again:

dncsStop

6   Add the following entries in the .profile file:

export CAM_INSTANT_HIT_MULTIPLE_ENABLE=TRUE

export CAM_INSTANT_HIT_MULTIPLE_NUMBER=[number]

export CAM_INSTANT_HIT_MULTIPLE_DELAY=[delay]

Note: Replace number with the the numeric value for how many times the instant hit should be repeated. Replace delay with the the numeric value for the delay between the instant hit repeat in the order of seconds.

7   Type **source /export/home/dncs/.profile** so the DNCS will use the updated .profile file.

8   Type the following command to start DNCS processes:

dncsStart

9   Continue with *Allocate Bandwidth for the EMM* (on page 22).

Allocate Bandwidth for the EMM

Complete the following steps to allocate the bandwidth for the EMM transmission parameters.

1   From the DNCS administration console, click the Network Element Provisioning tab.

2   Click the **QPSK/CMTS/OIT** button.

3   Select an OIT Bridge; then, click **File**.

4   Select **OIT Bandwidth Config**. The OIT Bandwidth page appears.

5   Enter the desired percentage of bandwidth to be allocated for the following parameters.
Note: Default values are indicate in parentheses.

- Adhoc EMM Percentage (25%)
- Staging EMM Percentage (0%)
- Staging EMM Percentage (0%)
- Renewal EMM Percentage (70%)
- PPV EMM Percentage (5%)

6 Click **Save**.

7 Close the OIT Bandwidth OIT Bridge windows.

3

Setting Up Hubs, MPEG Sources, MQAM Modulators, PCGs, and SCSs

Introduction

This chapter provides procedures for setting up hubs, MPEG sources, MQAM modulators, PowerKEY Conditional Access Gateways (PCGs), and Simulcrypt Synchronizers (SCSs) for the PowerKEY DVB System in SR i4.3.

In This Chapter

Create, Modify, or Delete Hubs

Introduction

If you are setting up the PowerKEY DVB System for the first time, you must first create a headend and new hubs. A hub is a logical element that represents the point at which data is modulated and transmitted to subscribers through the radio frequency (RF) network. You can also modify or delete a hub after you create it.

Important: The procedure for creating, modifying, or deleting hubs depends on the following possible system configurations:

- Distributed DNCS license enabled or disabled

- Network binding license enabled or disabled

Note: This section provides four different procedures for creating new hubs along with procedures for modifying or deleting hubs based on your specific network configuration.

Before You Begin

Before you create, modify, or delete a hub, you must have your network map readily available. If you cannot locate your network map, refer to *Customer Information* (on page 199).

Operational Considerations

This section provides several operational considerations you should be aware of when creating, modifying, or deleting hubs.

- When Network Binding is enabled and a hub is associated with a package, set-tops will need to be authorized for this package in order to operate properly with this hub.

- If a package is removed from a DHCT, the DHCT will display an "unauthorized" barker. Authorizing the package again will allow the set-top to operate normally.

- If the Network Binding package of a hub is set to "None," any set-top will be able to operate within this hub.

- A package that is associated with a hub (a Network Binding package) cannot be deleted without first removing its association from any hubs.

Configuration One: Distributed DNCS Disabled and Network Binding Disabled

Creating New Hubs

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub List window opens.

3 From the Hub List, select **File** and choose **New**. The Set Up Hub window opens.

4 Click the **Headend Name** arrow and select a headend name from the list.

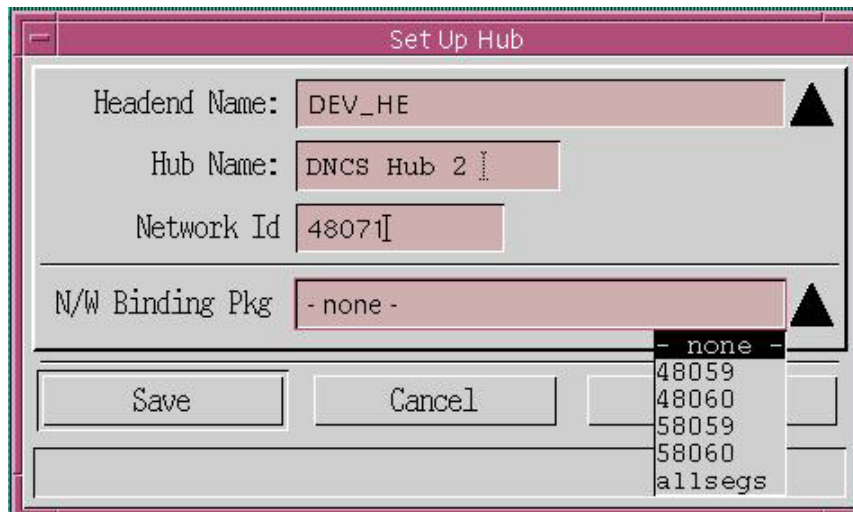**5** Click in the **Hub Name** field and type the name you will use to identify this hub (for example, **HE1_Hub1**). You can use up to 15 alphanumeric characters.

   Note: Be sure to use a name that is consistent with the naming scheme used on your network map.

6 Click in the **Network Id** field and type a unique Network ID.

   Note: The Network ID is the identifier of the network information table (NIT) table in DVB ASI. You need this Network ID when you create the NIT tables on the SI-Server.

7 Click **Save**. The system saves the hub information in the DNCS database and closes the Set Up Hub window. The Hub List window updates to include the new hub.

8 Do you need to modify a hub?

   ◼ If **yes**, go to *Modifying a Hub* (on page 27).

   ◼ If **no**, go to *Set Up MPEG Sources* (on page 39).

   Note: If you need to delete a hub, go to **Deleting a Hub,** later in this section.

Modifying a Hub

After you have created and saved a hub, you can only modify the hub name.

Important: To change any *other* parameters, you must delete the hub, and then re-add it to the DNCS, using the new information. To delete a hub, go to **Deleting a Hub**, next in this section.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **Hub**. The Hub List window opens.

3   Click once on the row containing the hub you want to modify.

4   Click **File** and choose **Open**. The Set Up Hub window opens for the hub you selected.

5   To change the name of this hub, click in the **Hub Name** field and change the name as desired. You can use up to 15 alphanumeric characters.

   Note: Be sure to use a name that is consistent with the naming scheme used on your network map.

6   To change the Networking Binding package, select the new package from the N/W Binding Pkg drop-down list.

7   When you finish making changes, click **Save**.

   Results:

   ▪ The system saves the new hub information in the DNCS database and closes the Set Up Hub window.

   ▪ The Hub List window updates to include the new hub information.

8   Change your network map to reflect these changes.

9   Do you need to modify another hub?

   ▪ If **yes**, repeat steps 3 through 7.

   ▪ If **no**, click **File**, and then choose **Close** to close the Hub List window and return to the DNCS Administrative Console. Then, go to step 10.

10   Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

11   Do you want to delete a hub?

   ▪ If **yes**, go to **Deleting a Hub**, next in this section.

   ▪ If **no**, go to *Set Up MPEG Sources* (on page 39).

Deleting a Hub

You may want to delete a hub because you are no longer using it, or because you need to redefine the headend or hub ID.

Important: Before you can delete a hub, you must delete all of the network elements that are associated with it, including any OIT bridges. In addition, you must have your network map readily available. If you cannot locate your network map, refer to *Customer Information* (on page 199).

1   Are there any node sets associated with this hub?

   ▪ If **yes**, delete those node sets first. When finished, return to this procedure.

   ▪ If **no**, go to step 2.

2   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

3 Click **Hub**. The Hub List window opens.

4 Click once on the row containing the hub you want to delete.

5 Click **File** then choose **Delete Selected Hub**. A confirmation window opens.

6 Click **Yes**. The confirmation window closes and the system removes the hub information from the DNCS database and from the Hub List window.

7 Delete the hub from your network map.

8 Click **File** and choose **Close** to close the Hub List window and return to the DNCS Administrative Console.

9 Do you need to delete another hub?

- If **yes**, repeat steps 1 through 8. When finished go to *Set Up MPEG Sources* (on page 39).

- If **no**, continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account. Go to *Set Up MPEG Sources* (on page 39).
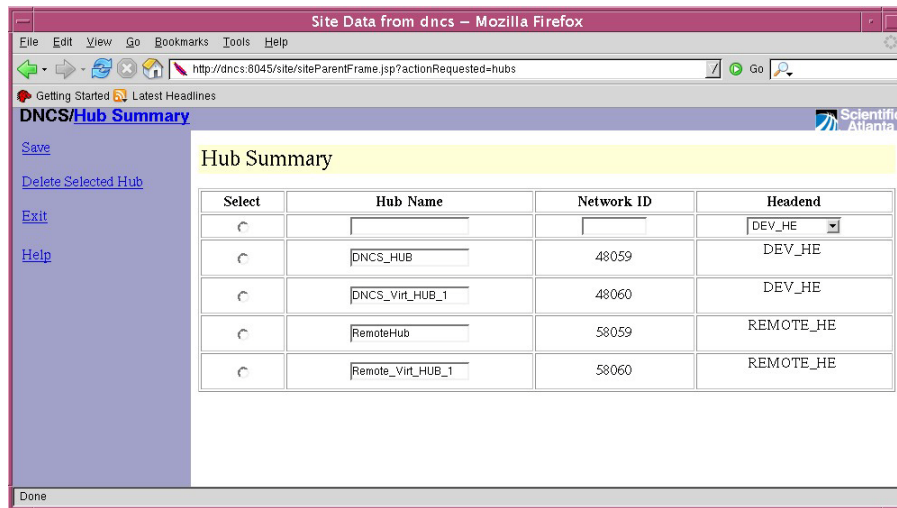
Configuration Two: Distributed DNCS Disabled and Network Binding Enabled

Creating New Hubs

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub List window opens.

3   From the Hub List, select **File** and choose **New**. The Set Up Hub window opens.

4   Click the **Headend Name** arrow and select a headend name from the list.

5   Click in the **Hub Name** field and type the name you will use to identify this hub (for example, **HE1_Hub1**). You can use up to 15 alphanumeric characters.

   Note: Be sure to use a name that is consistent with the naming scheme used on your network map.

6   Click in the **Network Id** field and type a unique Network ID.

   Note: The Network ID is the identifier of the network information table (NIT) table in DVB ASI. You need this Network ID when you create the NIT tables on the SI-Server.

7   Click the **N/W Binding Pkg** arrow and select a package from the list to be associated with this hub.

   Notes:

   ▪ Only subscription packages can be used as Network Binding packages. (Only these packages will be visible in the drop down list.)

   ▪ When no network binding package is selected (N/W Binding Pkg = none), a set-top can operate in that hub without being authorized for a specific package

8   Click **Save**. The system saves the hub information in the DNCS database, adds network binding, and closes the Set Up Hub window. The Hub List window updates to include the new hub.

Modifying a Hub

After you have created and saved a hub, you can only modify the following parameters for that hub:

- Hub name

- Network binding package

Important: To change any *other* parameters, you must delete the hub, and then re-add it to the DNCS, using the new information. To delete a hub, go to **Deleting a Hub**, next in this section.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub List window opens.

3 Click once on the row containing the hub you want to modify.

4 Click **File** and choose **Open**. The Set Up Hub window opens for the hub you selected.

5 To change the name of this hub, click in the **Hub Name** field and change the name as desired. You can use up to 15 alphanumeric characters.

   Note: Be sure to use a name that is consistent with the naming scheme used on your network map.

6 When you finish making changes, click **Save**.

   Results:

   - The system saves the new hub information in the DNCS database and closes the Set Up Hub window.

   - The Hub List window updates to include the new hub information.

7 Change your network map to reflect these changes.

8 When finished, send a copy of your updated network map to the representative who handles your account.

9 Do you want to delete a hub?

   - If **yes**, go to **Deleting a Hub,** next in this section.

   - If **no**, go to *Set Up MPEG Sources* (on page 39).

Deleting a Hub

You may want to delete a hub because you are no longer using it, or because you need to redefine the headend or hub ID.

Important: Before you can delete a hub, you must delete all of the network elements that are associated with it, including any OIT bridges. In addition, you must have your network map readily available. If you cannot locate your network map, refer to *Customer Information* (on page 199).

1   Are there any node sets associated with this hub?

- If **yes**, delete those node sets first. When finished, return to this procedure.

- If **no**, go to step 2.

2   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

3   Click **Hub**. The Hub List window opens.

4   Click once on the row containing the hub you want to delete.

5   Click **File** then choose **Delete Selected Hub**. A confirmation window opens.

6   Click **Yes**. The confirmation window closes and the system removes the hub information from the DNCS database and from the Hub List window.

7   Delete the hub from your network map.

8   Click **File** and choose **Close** to close the Hub List window and return to the DNCS Administrative Console.

9   Do you need to delete another hub?

- If **yes**, repeat steps 1 through 8. When finished go to *Set Up MPEG Sources* (on page 39).

- If **no**, continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account. Go to *Set Up MPEG Sources* (on page 39).

Configuration Three: Distributed DNCS Enabled and Network Binding Disabled

Creating New Hubs

1   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **Hub**. The Hub Summary window opens.
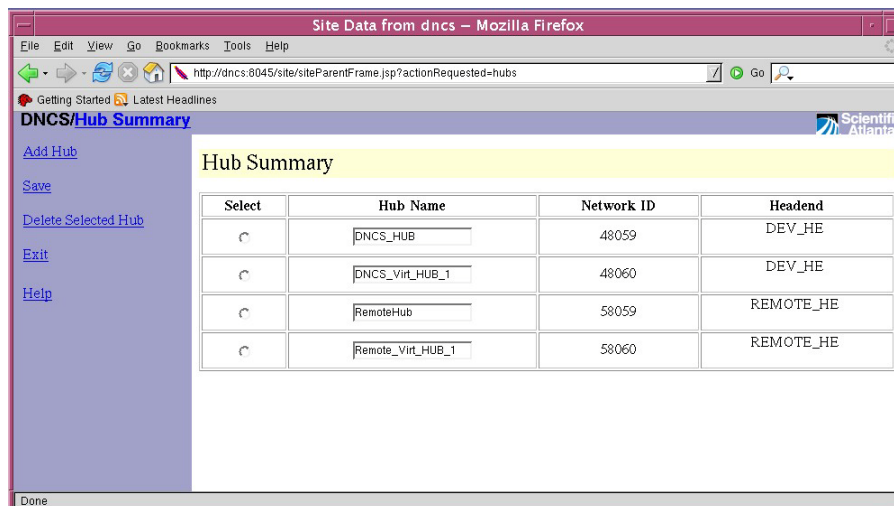
3   Click **Add Hub**. An empty row is added to the user interface.

4 Enter the correct **Hub Name** and **Network ID** in the blank fields.

5 Select the headend for this hub.

6 Click **Save**. The system saves the hub information in the DNCS database and updates the Hub Summary window to include the new hub.

   Note: The entries are sorted based on the Network ID.

Modifying a Hub

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub List window opens.

3 Click the **Select** button on the row containing the hub you want to modify.

4 Click **File** and choose **Open**. The Set Up Hub window opens for the hub you selected.

5 To change the name of this hub, click in the **Hub Name** field and change the name as desired. You can use up to 15 alphanumeric characters.

   Note: Be sure to use a name that is consistent with the naming scheme used on your network map.

6 Select the headend for this hub.

7 When you finish making changes, click **Save**.

   Results:

   ▪ The system saves the new hub information in the DNCS database and closes the Set Up Hub window.

   ▪ The Hub List window updates to include the new hub information.

8 Change your network map to reflect these changes.

9   Do you need to modify another hub?

- If **yes**, repeat steps 3 through 7.

- If **no**, click **File**, and then choose **Close** to close the Hub List window and return to the DNCS Administrative Console. Then, go to step 9.

10   Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

11   Do you want to delete a hub?

- If **yes**, go to **Deleting a Hub,** next in this section.

- If **no**, go to *Set Up MPEG Sources* (on page 39).

Deleting a Hub

You may want to delete a hub because you are no long using it, or because you need to redefine the headend or hub ID.

Important: Before you can delete a hub, you must delete all of the network elements that are associated with it, including any OIT bridges.

1   Are there any node sets associated with this hub?

- If **yes**, delete those node sets first. When finished, return to this procedure.

- If **no**, go to step 2.

2   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

3   Click **Hub**. The Hub Summary window opens.

4   Click the **Select** button on the row containing the hub you want to delete.

5   Click **File** then choose **Delete Selected Hub**. A confirmation window opens.

6   Click **Yes**. The confirmation window closes and the system removes the hub information from the DNCS database and from the Hub List window.

7   Delete the hub from your network map.

8   Click **File** and choose **Close** to close the Hub List window and return to the DNCS Administrative Console.

9   Do you need to delete another hub?

- If **yes**, repeat steps 1 through 8. When finished go to *Set Up MPEG Sources* (on page 39).

- If **no**, continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account. Go to *Set Up MPEG Sources* (on page 39).

Configuration Four: Distributed DNCS Enabled and Network Binding Enabled

Creating New Hubs

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub Summary window opens.

Note: When *both* Distributed DNCS and Network Binding are enabled, an additional column titled **N/W Binding Pkg** is displayed.

3 Click **Add Hub**. An empty row is added to the user interface.

4 Enter the correct **Hub Name**, **Network ID**, and **N/W Binding Pkg** in the blank fields.

Notes:

- Only subscription packages can be used as Network Binding packages. (Only these packages will be visible in the drop down list.)

- When no network binding package is selected (N/W Binding Pkg = none), a set-top can operate in that hub without being authorized for a specific package.

5 Select the headend.

6 Click **Save**. The system saves the hub information in the DNCS database and updates the Hub Summary window to include the new hub.

Note: The entries are sorted based on the Network ID.

Modifying a Hub

After you have created and saved a hub, you can only modify the hub name

Important: To change any *other* parameters, you must delete the hub, and then re-add it to the DNCS, using the new information. To delete a hub, go to **Deleting a Hub**, next in this section.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **Hub**. The Hub Summary window opens.

Note: When *both* Distributed DNCS and Network Binding are enabled, an additional column titled **N/W Binding Pkg** is displayed.

3 Enter the correct **Hub Name**, **Network ID**, and **N/W Binding Pkg** in the blank fields.

Notes:

- Only subscription packages can be used as Network Binding packages. (Only these packages will be visible in the drop down list.)

- When no network binding package is selected (N/W Binding Pkg = none), a set-top can operate in that hub without being authorized for a specific package.

4 Select the headend.

5 Click **Save**. The system saves the hub information in the DNCS database and updates the Hub Summary window to include the new hub.

Note: The entries are sorted based on the Network ID.

Deleting a Hub

You may want to delete a hub because you are no long using it, or because you need to redefine the headend or network ID.

Important: Before you can delete a hub, you must delete all of the network elements that are associated with it, including any OIT bridges.

1   Are there any node sets associated with this hub?

- If **yes**, delete those node sets first. When finished, return to this procedure.

- If **no**, go to step 2.

2   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

3   Click **Hub**. The Hub Summary window opens.

4   Click the **Select** button on the row containing the hub you want to delete.

5   Click the link **Delete Selected Hub**. A confirmation window opens.

6   Click **Yes**. The confirmation window closes and the system removes the hub information from the DNCS database and from the Hub List window.

7   Delete the hub from your network map.

8   Click **File** and choose **Close** to close the Hub List window and return to the DNCS Administrative Console.

9   Do you need to delete another hub?

- If **yes**, repeat steps 1 through 8. When finished go to *Set Up MPEG Sources* (on page 39).

- If **no**, continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account. Go to *Set Up MPEG Sources* (on page 39).

Set Up MPEG Sources

Introduction

After you create new hubs, you must set up MPEG sources. The first step in setting up elements that process program or service data is to add an MPEG source. The PowerKEY DVB System receives program and service information through the D96xx re-multiplexers. The D96xx re-multiplexers are called MPEG sources, because they receive program and service data from satellites and convert it into MPEG transport streams. You must create a source for every D96xx re-multiplexer in the system. This section provides procedures for setting up, modifying, and deleting MPEG sources.

Important: You must create a source for every D96xx re-multiplexer in your system, and you must also assign one of the D96xx re-multiplexers as the "Home D96xx." The Home D96xx receives BFS data input from the Direct ASI output on the PowerKEY DVB System.

Note: Refer to *Appendix A, Sources and Services Naming Conventions* (on page 201) before setting up MPEG sources.

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, refer to *Customer Information* (on page 199). You must also have the following information:

- Name of the headend containing the MPEG source

- Name used to identify the MPEG source

- Type of MPEG source (for example, D96xx)

- IP address for the MPEG source

- MAC address for the MPEG source

- Type of output card installed in the MPEG source (for example, ASI)

- Number identifying the output port on the MPEG source that is physically connected to the input port on the associated program MQAM modulator/SCS

- Number identifying the transport stream going from the MPEG source to the associated program MQAM modulator/SCS

Note: All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.

Process Overview

Be sure to allow yourself adequate time to complete this procedure. Adding an MPEG source takes approximately 30 minutes. To add an MPEG source to the DNCS, you must complete the following tasks.

1   Set up the MPEG source basic parameters.

2   Set up the connection from the MPEG source to the program MQAM modulator.

    Important: You can only add up to two MPEG sources per MQAM modulator.

Setting Up MPEG Source Basic Parameters

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.
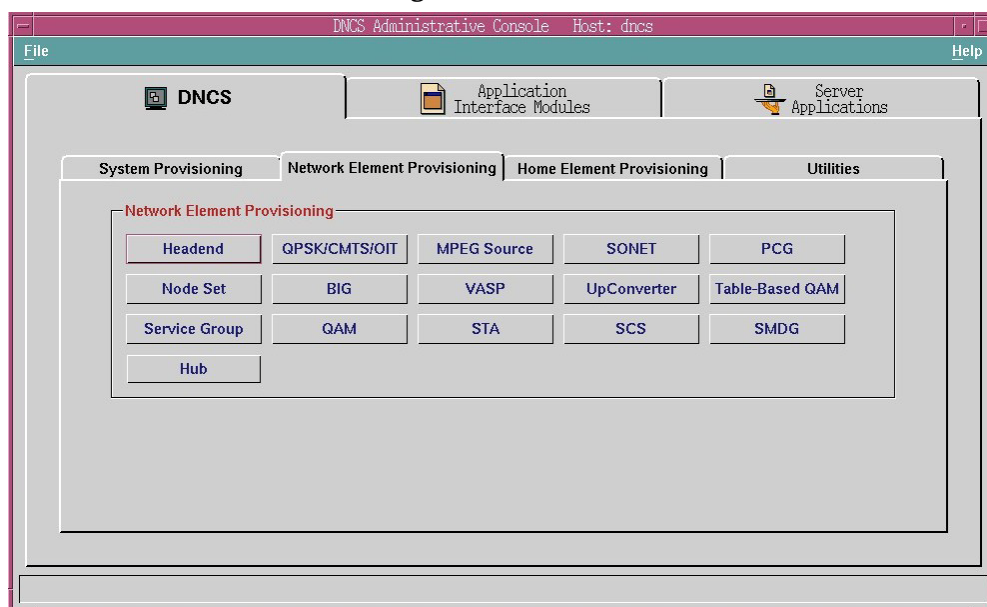
2   Click **MPEG Source**. The MPEG Source List window opens.

3   Click **File** then select **New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.

4 Click the **Headend Name** arrow and select the headend associated with this MPEG source.

5 Click in the **MPEG Source Name** field and type the name of this MPEG source (for example, **HE1_D96xx1**). You can use up to 20 alphanumeric characters.

Important: You must create a source for every SCS/MQAM in the system.

6 Click the **Device Type** arrow and select the type of MPEG source you are adding (for example, **MUX**).

Important: If the device type *MUX* is not in the list, you must type **MUX** (all uppercase) in the Device Type field.

7 Click in the **IP Address** field and type the IP address for this MPEG source. Be careful to place the dots (**.**) correctly between numbers.

Note: You can locate this IP address from the front panel LCD on the D96xx re-multiplexer.

8 Click in the **Physical Address** field and type the MAC address for this MPEG source.

Note: You can locate this MAC address from the address resolution protocol (ARP) entry table on the router. Refer to the documentation for your router for instructions on locating the ARP entry table.

9 Click **Apply**. The system saves the basic parameters for this MPEG source in the DNCS database and the previously disabled Connectivity tab becomes available.

10 Your next step is to set up the connection from the MPEG source to the SCS/MQAM. Go to *Setting Up MPEG Source Connections* (on page 42).

Setting Up MPEG Source Connections

After you set up the basic parameters for an MPEG source, complete these steps to set up the connections from the MPEG source to its associated SCS/MQAM modulator.

1 On the Set Up MPEG Source window, click the **Connectivity** tab. The Connectivity tab information moves to the forefront with an illustration of any devices already connected to this MPEG source. (If no device is connected, the illustration field will be empty).
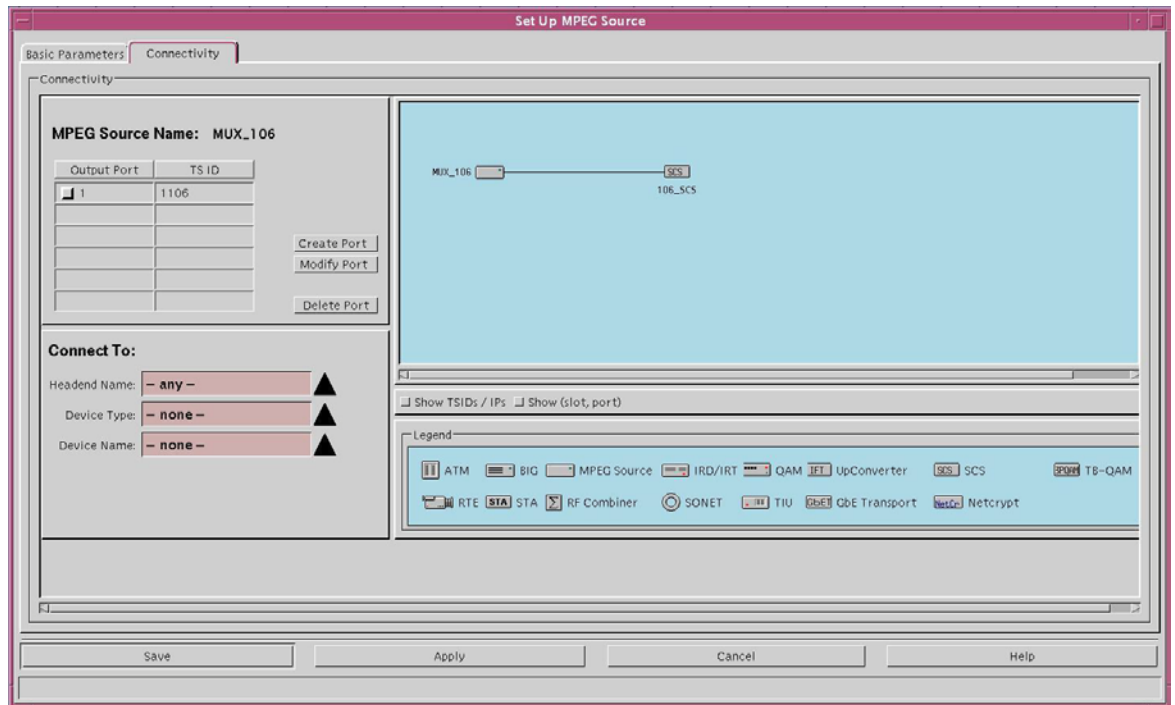
2 Click **Create Port**. The Port Number Prompt window opens.

Note: If multiple ports are created on the SCS (when a DCM is used as the SCS), corresponding ports must be created and modeled accordingly.

3 Click in the **Port Number** field and type the first available port number.

Important:

■ When the output port on the D96xx Re-multiplexer is logically connected to the input port on the SCS, enter a value of **1** (one) in the Port Number field.

■ When the output port on the D96xx Re-multiplexer is physically connected to the input port on the MQAM modulator, enter a value of **0** (zero).

4 Click in the **Transport Stream ID** field and type the number that identifies the transport stream going from this MPEG source to the associated simulcrypt synchronizer (SCS) or MQAM modulator. This number must correspond with the ASI input (usually on your network map) on the associated SCS or MQAM modulator. See *Appendix A, Sources and Services Naming Conventions* (on page 201) for the correct naming and numbering conventions.

Important: You will need this number when you set up the SCS or MQAM modulator.

5   Click **OK**.

Results:

- The system saves this information in the DNCS database and closes the Port Number Prompt window.

- The Connectivity tab updates with the new port and transport stream information.

- The Modify Port and Delete Port options become available.

Note: When you set up the associated program MQAM modulator, the system will automatically complete the Connect To fields on this window.

6   Click **Apply**. The system saves the MPEG source information in the DNCS database and updates the Connectivity illustration to include the new port information.

7   Is the MPEG source connected to another ASI input port on a program MQAM modulator?

- If **yes**, repeat steps 2 through 6. When finished, go to step 8.

- If **no**, go to step 8.

8   Click **Save**.

Results:

- The system saves the MPEG source information in the DNCS database and closes the Set Up MPEG Source window.

- The MPEG Source List window updates to include the new MPEG source.

9   Do you need to add another MPEG source?

- If **yes**, go back to *Setting Up MPEG Source Basic Parameters* (on page 40).

- If **no**, click **File** then choose **Close** to close the MPEG Source List window and return to the DNCS Administrative Console. Go to step 10.

10 Do you want to modify an MPEG source?

- If **yes**, go to *Modifying an MPEG Source* (on page 44).

- If **no**, your next step is to add the SCS or the program MQAM modulator that will be receiving data from this MPEG source. Depending on your configuration, go to either *Add a Program MQAM Modulator* (on page 46) or *Add an SCS* (on page 59).

Note: If you want to delete an MPEG source, go to *Deleting an MPEG Source* (on page 44).

Modifying an MPEG Source

After you have created and saved an MPEG source, you can modify any of its parameters, except for the headend associated with it and the device type. Complete these steps to modify an MPEG source.

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **MPEG Source**. The MPEG Source List window opens.

3   Click once on the row containing the MPEG source you want to modify.

4   Click **File** then choose **Open**. The Set Up MPEG Source window for the MPEG source you selected opens.

5   Make the desired changes. If you need help completing any fields, refer to the procedure for *Setting Up MPEG Source Basic Parameters* (on page 40).

    Note: If you would like to save your changes to the database without closing the window, you can click **Apply** at any time.

6   When you finish making changes, click **Save**.

    Results:

    ■   The system saves the new MPEG source information in the DNCS database and closes the Set Up MPEG Source window.

    ■   The MPEG Source List window updates to include the new MPEG source information.

7   Change your network map to reflect these changes.

8   Do you need to modify another MPEG source?

    ■   If **yes**, repeat steps 3 through 7.

    ■   If **no**, click **File** and choose **Close** to close the MPEG Source List window and return to the DNCS Administrative Console. Go to step 9.

9   Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

10 Do you want to delete an MPEG source?

    ■   If **yes**, go to *Deleting an MPEG Source* (on page 44).

    ■   If **no**, go to *Add a Program MQAM Modulator* (on page 46).

Deleting an MPEG Source

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **MPEG Source**. The MPEG Source List window opens.

3   Click once on the row containing the MPEG source you want to delete.

4   Click **File** then choose **Delete**. A confirmation window opens.

5   Click **Yes**. The confirmation window closes and the system removes the MPEG source information from the DNCS database and from the MPEG Source List window.

6   Delete the MPEG source from your network map.

7   Do you need to delete another MPEG source?

   ■   If **yes**, repeat steps 3 through 6.

   ■   If **no**, click **File** and choose **Close** to close the MPEG Source List window and return to the DNCS Administrative Console. Go to step 8.

8   Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

Multiple Home Transport Streams

With the Distributed DNCS license enabled, there can be more than one site configured in a DNCS and each site can have its own Home Transport Stream (TS). Therefore, multiple edge devices can be configured as Home Transport Stream edge devices as long as each one belongs to a different site.

There can be only one edge device within a site that can be actually designated as a Home Transport Stream (Home TS). However, each site can have more than one hub configured in it. Each additional hub in a site should have an edge device whose frequency is a duplicate of the Home TS edge device of the site. The bootloader program must be distributed to all the Home TS edge devices in all of the hubs.

Only one Home TS edge device per headend/site can be an MQAM. All other Home TS edge devices (in the main headend and at the remote headends) must be SCS devices.

Add a Program MQAM Modulator

Introduction

Important: This section applies only to systems using MQAM modulators. If you are using an SCS, go to *Add a PCG* (on page 53).

After you add an MPEG source, if you are using a program MQAM modulator to receive data from that source, you must add the MQAM modulator. A program MQAM modulator (sometimes called a *service MQAM modulator*) receives program and service data (for example, audio/video programming and Web services). The MQAM modulator then encrypts the data, if needed, and modulates it onto an RF carrier for distribution to DHCTs.

Note: A program MQAM modulator can receive program and service data from up to two MPEG sources.

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, refer to *Customer Information* (on page 199). You must also have the following information:

- Name of the headend containing the MQAM modulator

- Name used to identify the MQAM modulator

- IP address for the MQAM modulator (from your system administrator)

- MAC address for the MQAM modulator

- Subnet mask for the MQAM modulator (from your system administrator)

- Default Gateway for the MQAM modulator

- Number(s) identifying the transport stream(s) going from the MQAM modulator out to the hubs on your system

- Type of modulation and symbol rate the MQAM modulator uses

- Frequency of the channel(s) being used to send data from the MQAM modulator to the hubs on your system

- Number(s) identifying the transport stream(s) of the associated MPEG source(s) that are physically connected to the input port(s) on this MQAM modulator

- Number(s) identifying the input port(s) on this MQAM modulator that are physically connected to the associated MPEG source(s)

- Name of the headend containing the associated MPEG source(s)

- Type of MPEG source device(s) being used to send data to this MQAM modulator (for example, D96xx)

- Name of the associated MPEG source(s)

- Number(s) identifying the output port(s) of the associated MPEG source(s) that are physically connected to the input port(s) on this MQAM modulator

Note: All of this information should be recorded on your network map. However, if it is not, contact your system administrator to obtain the information.
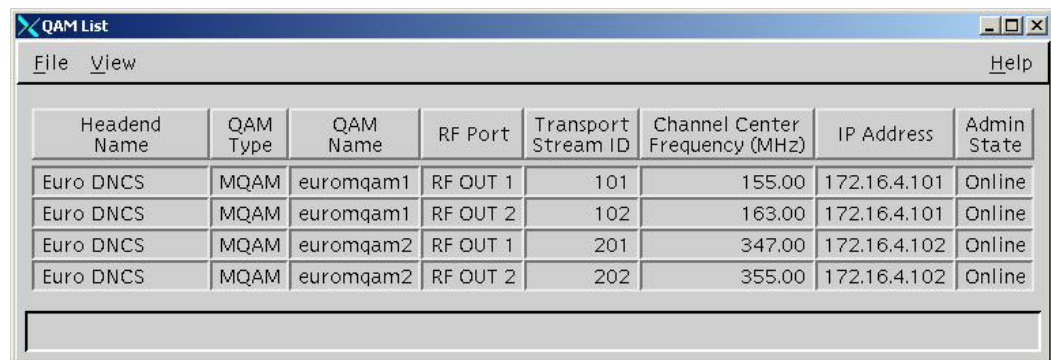
Process Overview

Be sure to allow yourself adequate time to complete this procedure. Adding a program MQAM modulator takes approximately 30 minutes. To add a program MQAM modulator to the DNCS, you must complete the following tasks:

1 Set up the program MQAM modulator basic parameters.
2 Set up the program MQAM modulator advanced parameters.
3 Set up the program MQAM modulator connection to the MPEG source(s).
4 Activate the program MQAM modulator.

Setting Up Program MQAM Modulator Basic Parameters

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.
2 Click **QAM**. The QAM List window opens.

Headend Name	QAM Type	QAM Name	RF Port	Transport Stream ID	Channel Center Frequency (MHz)	IP Address	Admin State
Euro DNCS	MQAM	euromqam1	RF OUT 1	101	155.00	172.16.4.101	Online
Euro DNCS	MQAM	euromqam1	RF OUT 2	102	163.00	172.16.4.101	Online
Euro DNCS	MQAM	euromqam2	RF OUT 1	201	347.00	172.16.4.102	Online
Euro DNCS	MQAM	euromqam2	RF OUT 2	202	355.00	172.16.4.102	Online

3 Click **File**, choose **New**, and then select **MQAM**. The Set Up MQAM window opens with the Basic Parameters tab in the forefront.

4 Click the **Headend Name** arrow and select the headend in which this program MQAM modulator resides.

5 Click in the **QAM Name** field and type the name of this MQAM modulator. You can use up to 15 alphanumeric characters.

Important: We recommend that you establish a naming scheme that allows you to easily identify the MQAM modulator and where it resides.

Example: A name of **hub1MQ43** could represent an MQAM modulator whose IP address ends in 43 and that processes data for Hub 1.

6 Click in the **IP Address** field and type the IP address for this MQAM modulator. Be careful to properly place the dots (.) between numbers.

7 Click in the **Physical Address** field and type the MAC address for this MQAM modulator.

8 Click in the **Subnet Mask** field and type the subnet mask where this MQAM modulator resides, based on the following guidelines:

- If your system uses a standard network configuration, type **255.255.255.0**.

- If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator.

9 Click the **Modulation Type** arrow and select the modulation this MQAM modulator uses. For example, if this is a 256 MQAM that uses ITU A modulation, you should select **ITU J83 Annex A (8 MHz)**.

10 Click in the **Default Gateway** field and type the default gateway address for this MQAM modulator.

11 For each ASI Input Transport Stream ID on this MQAM modulator, click in the **ASI INPUT 1 (2) Transport Stream ID** field and type the number identifying the transport stream(s) receiving the data from the associated MPEG source(s) that are physically connected to the input port(s) on this MQAM modulator.

12 For each output port on this MQAM modulator, click in the **Transport Stream ID** field in each **RF OUT** row, and type the number identifying the transport stream(s) carrying data from this MQAM modulator out to the hubs on your system.

    Note: You must specify unique transport stream IDs for both output ports on the MQAM modulator.

13 For each output port on this MQAM modulator, click the **Modulation Type** arrow in each **RF OUT** row, and select the type of modulation this MQAM modulator uses. For example, if this is a 256 MQAM modulator that uses ITU A modulation, you would select **256-QAM**.

14 For each output port on this MQAM modulator, click in the **Channel Center Frequency (MHz)** field in each **RF OUT** row, and type the frequency of the channel you will use to send data from this MQAM modulator to the hubs on your system. We recommend that you enter a value in 8 MHz increments from 108 to 858.

15 For each output port on this MQAM modulator, click in the **Symbol Rate (Ms/s)** field in each **RF OUT** row, and type the symbol rate.

16 Is **Spectral Inversion** enabled?

    ■ If **yes**, clear the selection, then go to step 17.

    ■ If **no**, go to step 17.

    Important: The recommended setting is *not* enabled.

17 Click **Apply**. The system saves the MQAM modulator information you have entered into the DNCS database.

18 Your next step is to set up the advanced parameters for the program MQAM modulator. Go to *Setting Up Program MQAM Modulator Advanced Parameters* (on page 49).

Setting Up Program MQAM Modulator Advanced Parameters

After you set up the basic parameters for a program MQAM modulator, complete these steps to set up the advanced parameters.

1 On the Set Up MQAM window, click the **Advanced Parameters** tab. The Advanced Parameters tab information moves to the forefront.

Important: The system inserts the **Configuration File Name** automatically. Do not change this field without first consulting our technical support. Refer to *Customer Information* (on page 199) for detailed information. The system configuration file tells the MQAM modulator which version of software it should be running.
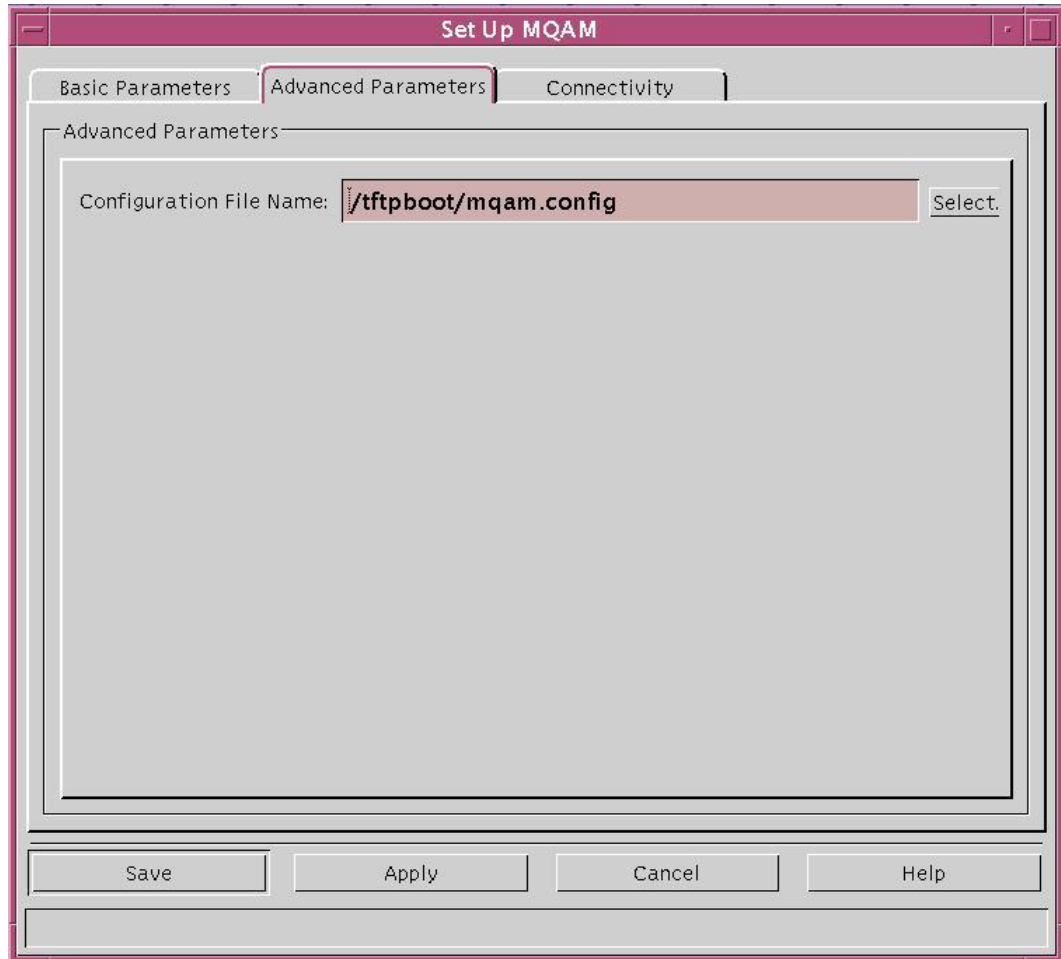
2   Click **Apply**. The system saves this information into the DNCS database.

3   Your next step is to set up the connections between the program MQAM modulator and its associated MPEG source(s). Go to *Setting Up Program MQAM Modulator Connections* (on page 50).

Setting Up Program MQAM Modulator Connections

After you set up the program MQAM modulator advanced parameters, complete these steps to set up the connections between the modulator and its associated MPEG source.

1   On the Set Up MQAM window, click the **Connectivity** tab. The Connectivity tab information moves to the forefront with an illustration of the devices already connected to this MQAM modulator.

2   If not already selected, click to select the **Input 1 Port** option.

3   In the **Connect To** area, click the **Headend Name** arrow and select the headend that contains the MPEG source that is physically connected to the selected input port on this MQAM modulator.

4   Click the **Device Type** arrow and select the type of MPEG source device being used to send data to the selected input port on this MQAM modulator (for example, **MUX**).

   Note: The Device Type should always be **MUX**.

5   Click the **Device Name** arrow and select the name previously defined for the MPEG source associated with the selected input port on this MQAM modulator.

6   Click in the **Port Number** field and select the corresponding port of the MPEG source.

7   The options that appear on this window after step 6 are dependent upon what you selected for the Device Type in step 4. As you finish completing this window, keep in mind that the information being requested is about the MPEG source associated with the selected input port on this MQAM modulator.

   Note: You need to specify the number that identifies the output port on the MPEG source that is physically connected to the input port on this MQAM modulator.

8   Click **Apply**. The system saves this information into the DNCS database and updates the illustration so that it shows the information you entered.

9   Is an MPEG source sending data to Input Port 2 on this MQAM?

   ■   If **yes**, click the **Input 2 Port** option. Repeat steps 3 through 8 to define and save the connectivity parameters for the second input port on the MQAM modulator. When finished, go to *Activating a Program MQAM Modulator* (on page 51).

   ■   If **no**, go to *Activating a Program MQAM Modulator* (on page 51).

Activating a Program MQAM Modulator

After you set up the connections between a program MQAM modulator and its associated MPEG source(s), complete these steps to activate the modulator by placing it online.

Note: You can activate an MQAM modulator only after all parameters for the modulator have been saved to the DNCS database, and only after the modulator has finished its booting process. Therefore, you may have to wait a few minutes before you can complete this task.

1   On the Set Up MQAM window, click the **Basic Parameters** tab. The Basic Parameters tab information moves to the forefront.

2   At the **Administrative State** field, click the **Online** option.

3   Do you need to make this MQAM the Home Transport MQAM modulator?

- If **yes**, click **Apply** and then click **Allow SI**. When prompted, click **Yes** and go to step 4.

- If **no**, go to step 4.

4   Click **Save**.

Results:

- The system saves the MQAM modulator information in the DNCS database and closes the Set Up MQAM window.

- The QAM List window updates to include the new MQAM modulator.

Note: The new MQAM modulator is listed two times to show its two output streams.

5   Add the new program MQAM modulator to your network map.

6   If this MQAM modulator is the Home Transport MQAM modulator, go to Configuring the Direct ASI Cards.

7   Do you need to add another program MQAM modulator?

- If **yes**, go back to *Setting Up Program MQAM Modulator Basic Parameters* (on page 47).

- If **no**, click **File** then choose **Close** to close QAM List window and return to the DNCS Administrative Console. Go to step 8.

8   Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

Add a PCG

Introduction

After you add an MPEG source, if you are using a third-party Event Information Scheduler (EIS) and a third-party scrambler (on a third-party SCS) for scrambling the stream, you must add the PowerKEY Conditional Access Gateway (PCG) to the DNCS database. The PCG is responsible for generating the entitlement control messages (ECMs) for a given service. The PCG receives the program data and the Control Word (CW) with which it generates the ECMs. The PCG does that with a skeleton ECM received from the DNCS. The SCS is responsible for encrypting the transport stream with the given CW and inserting the ECMs into the stream.

The PCG needs one interface to communicate with the SCS on a private network, and it needs another interface to communicate with the DNCS.

Before You Begin

Before you begin, you must have your network map and the PCG provisioning parameters. If you cannot locate your network map, refer to *Customer Information* (on page 199). You must also have the following information:

- Name used to identify the PCG

- NIC-IP address on the PCG to communicate with the DNCS (from your system administrator)

- MAC address for the above interface on the PCG (from your system administrator)

- Subnet mask for the above interface on the PCG (from your system administrator)

- Gateway IP for the above interface on the PCG (from your system administrator)

- NIC-IP address on the PCG to communicate with the associated SCS(s) on a private network (from your system administrator)

- Subnet mask for the above interface on the PCG (from your system administrator)

- Gateway IP for the above interface on the PCG (from your system administrator)

- Maximum PCG session count

- ID given for the PCG device

- The timeout (in seconds) for the communication from the DNCS to the PCG

- The configuration file that needs to be sent to the PCG from the DNCS

- Maximum streams allowed on the PCG

- Name of the headend containing the PCG

- The Control Word Provision Message Delay (in seconds)

- The Nominal Crypto period duration (in seconds)

- The SCG Provision Timeout (in seconds)

Note: All this information should be recorded for setting up the PCG with any third-party SCS devices. However, if it is not, contact your system administrator to obtain the information.

Setting Up PCG Provisioning Parameters

Be sure to allow yourself adequate time to complete this procedure. Adding a PCG takes approximately 30 minutes. Complete the following procedure to add a PCG to the DNCS.

Important: Verify that you have gathered all of the information identified in the previous section *Before You Begin* (on page 53).

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **PCG**. The PowerKEY CAS Gateway window opens.
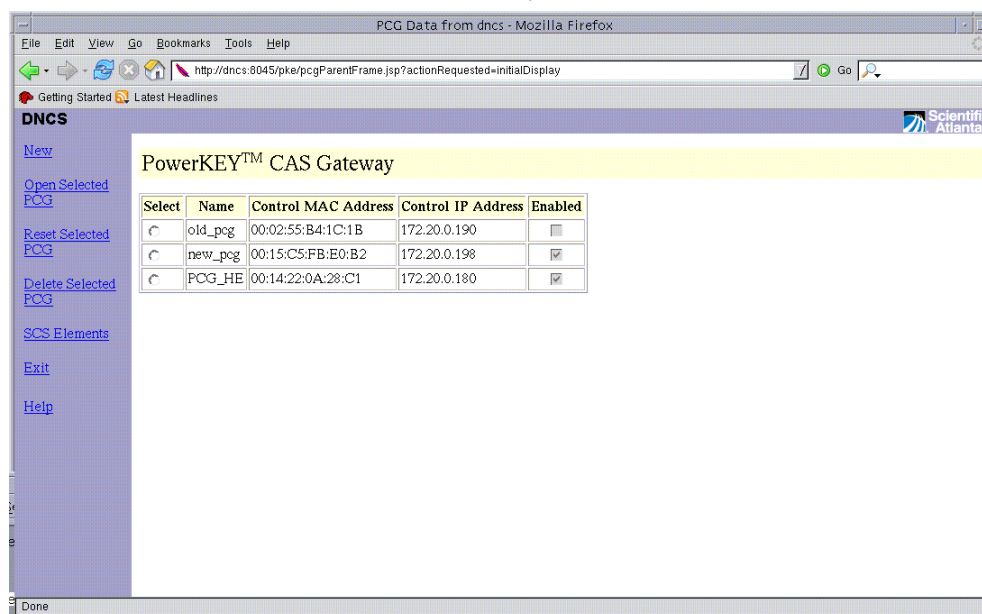
3   Click **New**. The New PowerKEY CAS Gateway window opens.

4 Click in the **Name** field and type the name of this PCG. You can use up to 20 alphanumeric characters *without* spaces between the characters.

Important: We recommend that you establish a naming scheme that allows you to easily identify the PCG and where it resides.

Example: A name of PCG12 could represent a PCG, whose IP address ends in 12.

5 Click in the **Control NIC IP Address** field and type the IP address for this PCG. Be careful to properly place the dots (.) between numbers.

6 Click in the **Subnet Mask** field and type the subnet mask where the PCG resides (for the above NIC IP address), based on the following guidelines:

- If your system uses a standard network configuration, type 255.255.255.0.

- If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator.

7 Click the **Control NIC MAC Address** field and type the MAC address for this NIC on the PCG. Be careful to properly place the colon (:) between the numbers.

8 Click the **Default Gateway** field and type the default gateway IP for the above NIC IP address. Be careful to properly place the dots (.) between the numbers.

9 Click the **Max Sessions** field and type the maximum sessions allowed on the PCG. This is any integer value between 1 and 1000.

10 Click the **Enabled** check box to activate the PCG.

11 Click the **DNCS=>PCG Msg Timeout** field and type any integer value between 5 and 60.

12 Click the **PCG=>SCS Timeout** field and type any integer value between 5 and 60.

13 Click the **CW_Provision Msg Repetition Rate** field and type **1**.

14 Click the **ID** field and type any integer value which uniquely identifies this PCG.

15 Click the **Config File** field and type the config file name used to send to the PCG (For example, pcg.config).

> **Important:** Confirm that the config file name exists in the /tftpboot directory.

16 Click the **Max Streams** field and type the maximum encrypted streams allowed on the PCG. This is any integer value between 1 and 1000.

17 Click the **Headend** arrow and select the headend in which this PCG resides.

18 Click in the **SCS Ethernet IP Address** field and type the IP address on this PCG which will talk to the SCS. Be careful to properly place the dots (.) between numbers.

> **Important:** If only one interface of the PCG is used, enter the same Control NIC IP Address that you entered in step 5 of this procedure.

19 Click in the **SCS Subnet Mask** field and type the subnet mask where the SCS Interface resides (for the above NIC IP address), based on the following guidelines:

- If your system uses a standard network configuration, type 255.255.255.0.

- If your system uses another type of network configuration, type the subnet mask as assigned by your system administrator.

20 Click the **SCS Default Gateway** field and type the default gateway IP for the above SCS Interface IP address. Be careful to properly place the dots (.) between numbers.

21 Click the **SCS Test Timeout (Seconds)** field and type any integer value between 5 and 20. This is the number of seconds the PCG waits for communication from the SCS.

22 Click the **CW Message Delay (Seconds)** field and type **10**. This is the number of seconds the PCG waits to receive a control word.

23 Click the **Nominal Crypto Period** field and type any integer value between 4 and 10. This is the number of seconds that each crypto period will last.

24 Click the **SCS Provision Timeout (Seconds)** field and type any integer value between 5 and 20. This is the number of seconds the SCS waits to receive provisioning information from the PCG.

25 Click **Save**. The system saves this information into the DNCS database.

Modifying PCG Provisioning Parameters

After you have created and saved a PCG, you can modify any of its parameters, except for the Control NIC MAC Address where the PCG resides, Maximum PCG Session Count, ID and Max Streams. Complete the following steps to modify a PCG.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **PCG**. The PowerKEY CAS Gateway window opens.

3 Select the radio button to select one PCG you want to modify and click **Open Selected PCG**. The Update PowerKEY CAS Gateway window opens.

4 Make the desired changes. If you need help completing any fields, refer to the procedure for *Setting Up PCG Provisioning Parameters* (on page 54).

5 When you finish making changes, click **Update**.

Results:

- The system saves the new PCG information in the DNCS database and closes the Update PowerKEY CAS Gateway window.

- The PCG list window updates to include the new PCG information.

6 Change your network map to reflect these changes.

7 Do you need to modify another PCG?

- If **yes**, repeat steps 3 through 6.

- If **no**, click **Exit** to close the PCG List window and return to the DNCS Administrative Console. Go to step 8.

8 Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

9 Do you want to delete a PCG?

- If **yes**, go to *Deleting a PCG* (on page 57).

- If **no**, you have completed this procedure.

Deleting a PCG

Important: Before deleting a PCG make sure that you do not have an SCS associated with this PCG.

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **PCG**. The PowerKEY CAS Gateway window opens.

3   Click the radio button to select one PCG you want to delete.

4   Click **Delete Selected PCG**. A confirmation window opens.

5   Click **Yes**. The confirmation window closes and the system removes the PCG information from the DNCS database and from the PCG List window.

6   Delete the PCG from your network map.

7   Do you need to delete another PCG?

■   If **yes**, repeat steps 3 through 6.

■   If **no**, click **Exit** to close the PCG List window and return to the DNCS Administrative Console. Go to step 8.

8   Continue making any other changes that you need to make to your network. When finished, send a copy of your updated network map to the representative who handles your account.

Add an SCS

Introduction

After you add an MPEG source, if you are using a third-party EIS and a third-party scrambler (on a third-party SCS) for scrambling the stream, you must add this SCS to the DNCS database. An SCS is responsible for generating the CWs (for every Crypto-period cycle) for a given session. The SCS requests the ECMs from the PCG via the SCS interface (for every Crypto-period cycle) by sending the CW with session information for every Crypto-period cycle. The PCG then sends the completed ECM to the SCS. The SCS will encrypt the transport stream with the CW and insert the ECM in the stream.

The SCS needs an interface to communicate with the PCG on a private network, and it needs another interface to communicate with the SI-Server.

Before You Begin

Before you begin, you must have your network map and the SCS modeling parameters. If you cannot locate your network map, refer to *Customer Information* (on page 199). You must also have the following information:

- Name used to identify the SCS

- NIC-IP address for the interface on the SCS that will communicate with the PCG on a private network (from your system administrator)

- MAC address for the interface on the SCS that will communicate with the PCG on a private network on the SCS (from your system administrator)

- ID given for the SCS device

- Maximum SCS session count

- Name of the PCG to which it will talk to for ECM

- Name of the headend containing the PCG

- Number identifying the transport stream going from the SCS out to the hubs on your system

- Number(s) identifying the transport stream(s) of the associated MPEG source that is logically connected to the input port on this SCS

- Type of modulation the SCS device uses

- Frequency of the channel being used to send data from the SCS to the hubs on your system

- Symbol Rate of the channel being used to send data from the SCS to the hubs on your system

- Number identifying the input port on this SCS that is logically connected to the associated MPEG source

Note: All this information should be recorded for setting up the SCS. However, if it is not, contact your system administrator to obtain the information.
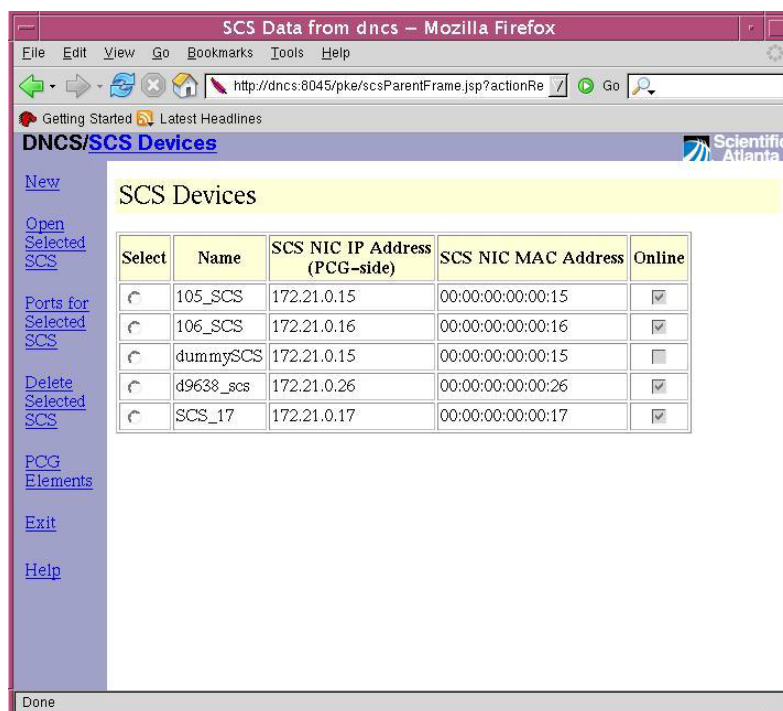
Process Overview

Be sure to allow yourself adequate time to complete this procedure. Adding an SCS takes approximately 30 minutes. To add an SCS to the DNCS, you must complete the following procedures:

- *Setting Up SCS Modeling Parameters* (on page 60)

- *Setting Up SCS Ports Modeling Parameters* (on page 63)

- *Setting Up SCS Connections* (on page 66)
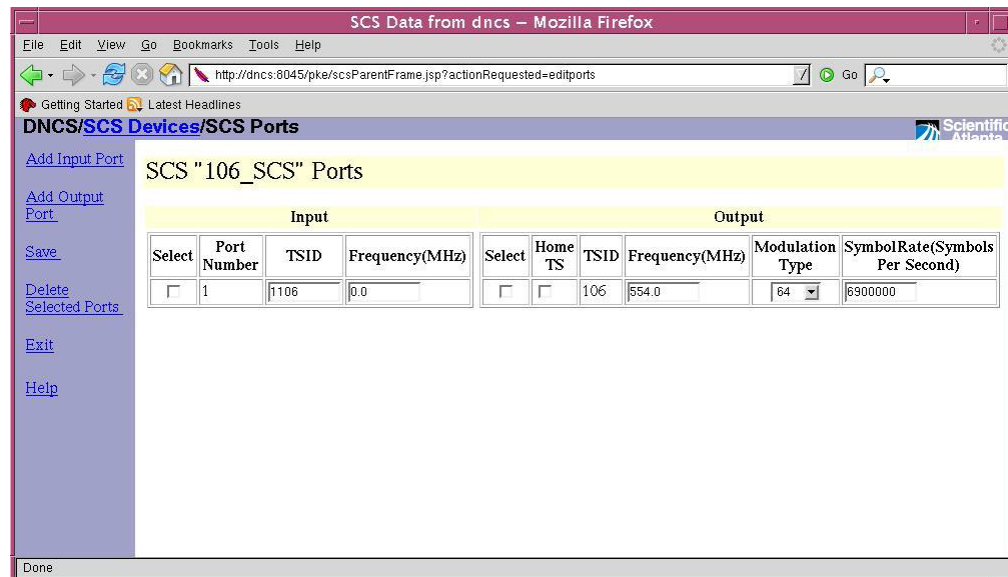
Setting Up SCS Modeling Parameters

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **SCS**. The SCS Devices window opens.

3 Click **New**. The New SCS Device window opens.

4   Click in the **Name** field and type the name of this SCS. You can use up to 20 alphanumeric characters *without* spaces between the characters.

Important: We recommend that you establish a naming scheme that allows you to easily identify the SCS and where it resides.

Example: A name of SCS12 could represent an SCS whose IP address ends in 12.

5   Click in the **IP Address** field and type the IP address for the interface on the SCS which will talk to the PCG on a private network. Be careful to properly place the dots (.) between the numbers.

6   Click the **MAC Address** field and type the MAC address for this interface on the SCS. Be careful to properly place the colon (:) between the numbers.

7   Click the **ID** field and type a unique ID for this SCS.

8   Click the **Primary PCG** and select the primary PCG with which this SCS would communicate and get the ECMs.

9   Click the **Headend** arrow and select the headend in which the PCG resides.

10 Click the **Max Sessions** field and type the maximum sessions allowed on the SCS device. This value is any integer value between 1 and 999.

11 Click **Save**. The system saves this information into the DNCS database. Your next step is to set up the connections between the SCS and its associated MPEG source. Go to *Setting Up SCS Ports Modeling Parameters* (on page 63).

Modifying SCS Modeling Parameters

After you have created and saved an SCS, you can modify any of its parameters, except for the ID. Complete these steps to modify the SCS.

> ⚠️ **CAUTION:**
>
> **If you need to make changes to the SCS modeling parameters, such as changing the IP address, all sources on the device should be stopped to allow the change to be made.**

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **SCS**. The SCS Devices window opens.

3   Select an SCS and click **Open Selected SCS**. The Update SCS Device window opens.

4   Make the desired changes. If you need help completing any fields, refer to the procedure for *Setting Up SCS Modeling Parameters* (on page 60).

5   When you finish making changes, click **Update.** The system saves this information into the DNCS database.

6   Change your network map to reflect these changes.

7   Click **Exit**. Your next step is to set up the connections between the SCS and its associated MPEG source. Go to *Setting Up SCS Connections* (on page 66).

Deleting the SCS

After you have created and saved an SCS, you are allowed to delete any SCS. Make sure you tear down the session on the SCS, then delete the ports on the SCS before proceeding further, refer to *Deleting SCS Ports Modeling Parameters* (on page 65).

Note: For detailed procedures for tearing down sessions, refer to the **Online Help for SR i4.2.2.**

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **SCS**. The SCS Devices window opens.
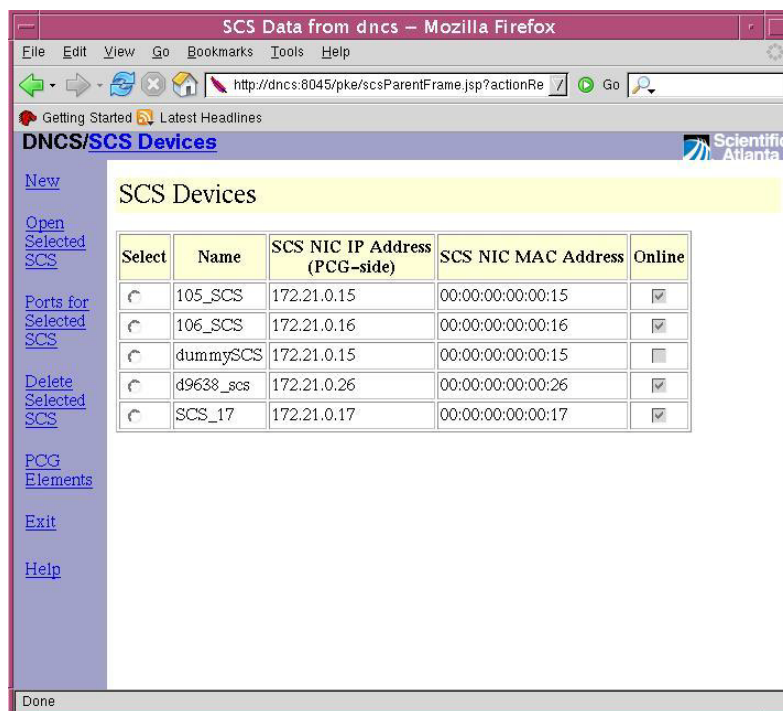
3 Select the radio button and choose the SCS you want to delete. Click **Delete Selected SCS**.

4 Change your network map to reflect these changes.

5 Click **Exit.**

Setting Up SCS Ports Modeling Parameters

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **SCS**. The SCS Devices window opens. Select an SCS and choose one of the following options:

- Click **Ports for selected SCS.**

- Click **Open Selected SCS** and then click **Maintain Ports**.

Result: The SCS <Name of SCS> Ports window opens.

3 Click **Add Input Port**. You can add the input port values.

4 For input port on this SCS, click in the **Port Number** field, and type the number identifying the input port.

Important: The first port number should always be 1 (one).

5 For input port on this SCS, click in the **TSID** field, and type the number identifying the transport stream on this SCS input port.

Notes:

- You must specify unique transport stream IDs for input and output ports on the SCS.

- The Input Frequency supports any devices that can use Intermediate Frequency (IF). For D96xx devices that receive ASI input, leave this field empty.

6 Click **Save**. The system saves this information into the DNCS database and updates the illustration so that it shows the information you entered.

7 Click **Add Output Port**. You can add the output port values.

8 For output port on this SCS, click in the **TSID** field, and type the number identifying the transport stream carrying data from this SCS out to the hubs on your system.

Note: You must specify unique transport stream IDs for input and output ports on the SCS.

9 For the output port on this SCS, click in the **Frequency field (MHz)**, and type the frequency of the channel you will use to send data from this SCS to the hubs on your system. We recommend that you enter a value in 8 MHz increments from 108 to 858.

10 For the output port on this SCS, click the **Modulation type** arrow, and select the type of modulation this SCS uses.

Note: When a DCM is used as the SCS, create multiple input and output ports with a unique TSID for each input/output pair. Also ensure that for each input port, there is a corresponding output port.

11 For the output port on this SCS, click in the **Symbol Rate** field, and type the symbol rate (s/s).

12 For output port on this SCS, click the **Home TS** check box to enable this frequency as Home TS.

13 Click **Save**. The system saves this information into the DNCS database and updates the illustration so that it shows the information you entered.

14 Click **Exit**. Your next step is to set up the connections between the SCS and its associated MPEG source. Go to *Setting Up SCS Connections* (on page 66).

Modifying SCS Ports Modeling Parameters

After you have created and saved an SCS port, you can modify any of its parameters, except for the input port number and the output TSID. Complete these steps to modify SCS ports.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **SCS**. The SCS List window opens.

3 Select an SCS and select one of the following options:

- Click **Ports for selected SCS.**
- Click **Open Selected SCS** and then click **Maintain Ports**.

Result: The SCS <Name of SCS> Ports window opens.

4 Make the desired changes. If you need help completing any fields, refer to the procedure for *Setting Up SCS Ports Modeling Parameters* (on page 63).

5 When you finish making changes, click **Save**. The system saves this information into the DNCS database and updates the illustration so that it shows the information you entered.

6 Change your network map to reflect these changes.

7 Click **Exit**. Your next step is to set up the connections between the SCS and its associated MPEG source. Go to *Setting Up SCS Connections* (on page 66).

Deleting SCS Ports Modeling Parameters

Important: After you have created and saved SCS Ports, you can delete the SCS ports. Complete these steps to delete SCS ports.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **SCS**. The SCS Devices window opens.

3 Select an SCS and select one of the following options:

- Click **Ports for selected SCS.**
- Click **Open Selected SCS** and then click **Maintain Ports**.

Result: The SCS <Name of SCS> Ports window opens.

4   Click the **Select** check box for the port(s) you want to delete. Then click **Delete Selected Ports**.

5   The system removes the SCS port information from the DNCS database.

6   Delete the SCS port from your network map.

7   Click **Exit**.

Setting Up SCS Connections

After you set up the SCS ports, complete these steps to set up the connections between the SCS and its associated MPEG source.

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2   Click **MPEG Source**. The MPEG Source List window opens.

3   Highlight the MPEG Source you want to associate, select **File**, and then click **Open**. The Set Up MPEG Source window opens.

4   On the Set Up MPEG Source window, click the **Connectivity** tab. The Connectivity tab information moves to the forefront with an illustration of the devices already connected to this MPEG source.

5   If a port is not already created, click the **Create Port** button. The Port Number Prompt window opens.

6   Click in the **Port Number** field and type 1 (one).

   Important: The first port number on the MPEG should always be 1 (one).

7   Click in the **Transport Stream ID** field and type the TSID associated with the input port of the SCS device to which you want to associate this MPEG source.

8   Click the **Transport Protocol** arrow and select the type of transport protocol being used to send the data to the SCS (for example, ASI).

   Note: The Transport Protocol will always be ASI.

9 Click **OK**.

10 In the Connect to area, click the **Headend Name** arrow and select the headend that contains the MPEG source.

11 Click the **Device Type** arrow and select the type of device being used to receive the data (for example SCS).

Note: To associate the SCS with MPEG source, the Device Type will always be SCS.

12 Click the **Device Name** arrow and select the name previously defined for the SCS associated with the selected output port on this MPEG source.

13 Click the **Port number** arrow and select the input port number on the SCS device.

14 Click **Apply**. The system saves this information into the DNCS database and updates the illustration so that it shows the information you entered.

15 Click **Save**. Go to *Activating the SCS* (on page 67).

Activating the SCS

After you set up the connections between the SCS and its associated MPEG source, complete these steps to complete the SCS modeling in the DNCS.
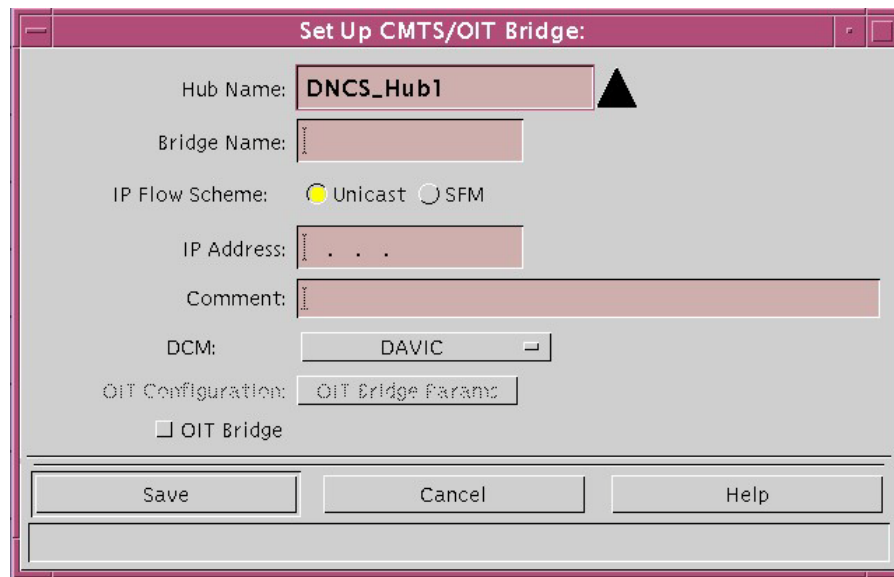
1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

2 Click **SCS**. The SCS Devices window opens.

3 Select an SCS and click **Open Selected SCS**. The Update SCS Device window opens.

4 Click the **Online** check box to allow the SCS to be modeled in the DNCS.

5 Click **Update**. The system saves this information into the DNCS database.

6 Click **Exit**.

4

Chapter 4

Setting Up CMTS or OIT Bridges

Introduction

After you have created sources and set up sessions, you must next set up Out-of-Band to InBand Translator (OIT) bridges depending on the types of DHCTs used in your system. This chapter provides procedures for setting up the OIT bridges on the PowerKEY DVB System.

The purpose of the OIT is to provide inband data on the PowerKEY DVB System. This inband data will be used in headend systems that require support for broadcast-only DHCTs. The OIT merely provides an additional inband data path for system information.

OIT data will be encapsulated into MPEG transport streams that will be written to an ASI card. The Direct ASI Card is currently used in the PowerKEY DVB System by the BFS and OSM processes. The OIT will share the Direct ASI Card with the BFS and OSM streams.

Important: An OIT bridge must be configured for each hub in the system.

In This Chapter

Configure OIT Bridges

1   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.
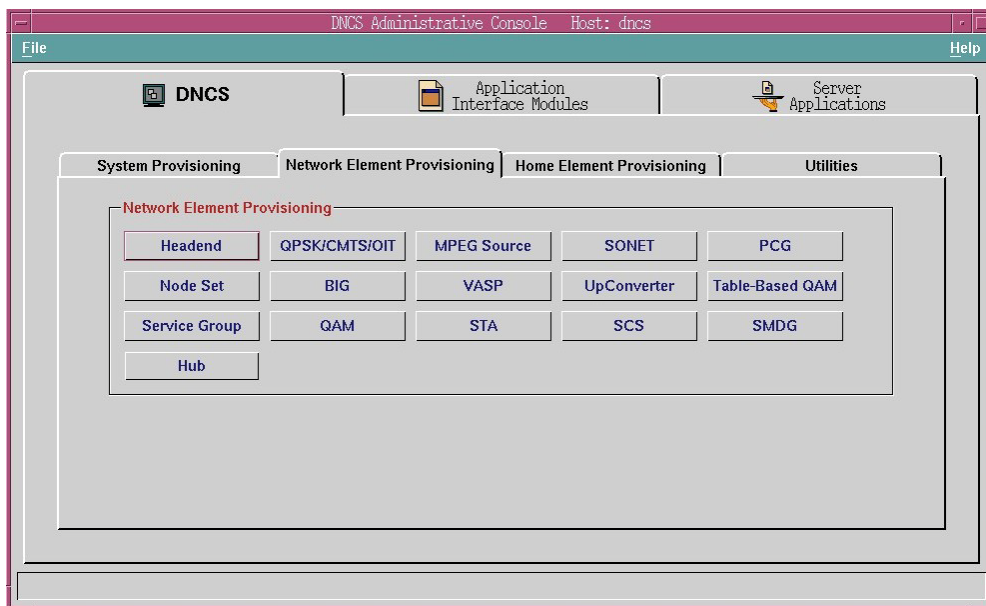
2   Click **QPSK/CMTS/OIT**. The QPSK/CMTS/OIT List window opens.
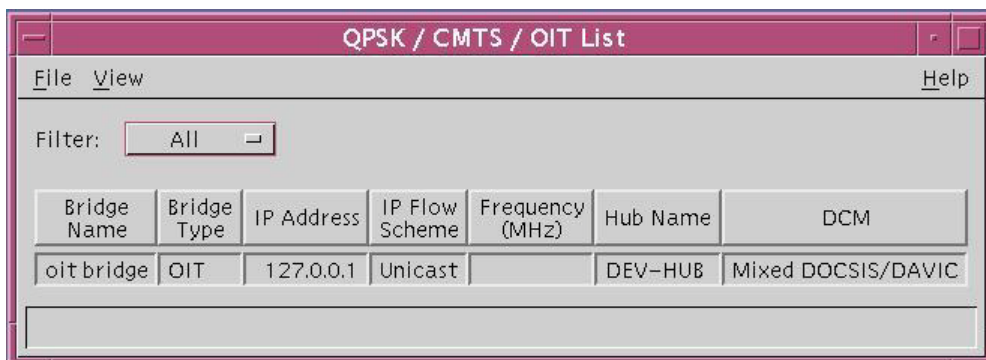
3   Click **File**, select **New,** and then choose **CMTS/OIT**. A Set Up CMTS/OIT Bridge window similar to the following opens.

Important:

■   All bridges on the RNCS must be virtual IP addresses.

■   The first OIT Bridge for the main DNCS should be given the loop back IP Address "127.0.0.1."

■   The OIT Bridge for every additional hub on the headend should be given a virtual IP address configured on the DNCS/RNCS. See *Configuring Virtual IP Addresses* (on page 76).

Note: The TED interface should not be used to create the sub interfaces.

4 Select a **Hub Name** from the Hub Name list.

5 Type a **Bridge Name** into the Bridge Name field.

6 Select **Unicast** for the IP Flow Scheme.

7 Type the **IP Address** into the IP address field.

8 Type a description of this bridge into the Comment field

9 Select **Mixed DOCSIS/DAVIC** from the DCM drop-down list.

10 To enable OIT Bridges, select the **OIT Bridge** checkbox in the Set Up CMTS/OIT Bridge window. The OIT Bridge Params button is now enabled as shown in the following example.

Important: You can only create one OIT Bridge per hub.

11 Click **OIT Bridge Params** in the Set Up CMTS/OIT Bridge window. A Set Up OIT Screen window similar to the following opens.

Note: The values shown in this screen are our recommended values for Max Data Rate. You can edit these values as your system requires.

12 Configure the following items in the **OIT Data Configuration** area of the Set Up OIT Screen window:

a In the **PID** column, click in the **EMM** field and type the hexadecimal PID value for the PowerKEY EMM stream. Allowable values=0x20-0x25.

   Note: This setting selects the PID that carries inband EMMs on the Direct ASI feed from the DNCS. This must be a unique value.

b In the **PID** column click in the **Fast Refresh EMM** field and type the hexadecimal PID value for the Fast Refresh EMM stream. Allowable values=0x20-0x25.

   Note: This setting selects the PID that carries Fast Refresh EMMs on the Direct ASI feed from the DNCS. This must be a unique value.

c In the **PID** column, click in the **System Messages** field and type the hexadecimal PID value for the System Messages stream. Allowable values=0x20-0x25.

   Note: This setting selects the PID that carries system messages and information on the Direct ASI feed from the DNCS. This must be a unique value.

d In the **PID** column, click in the **CAT** field and type the hexadecimal PID value for the CAT stream. This value is always set to one (1).

e In the **PID** column, click in the **Messaging** field and type the hexadecimal PID value for the Messaging stream. Allowable values=0x20-0x25.

f In the **Dncs ASI Pid** column, click in the **EMM** field and type the hexadecimal PID value for the PowerKEY EMM stream.

g In the **Dncs ASI Pid** column, click in the **Fast Refresh EMM** field and type the hexadecimal PID value for the Fast Refresh EMM stream.

h In the **Dncs ASI Pid** column, click in the **System Messages** field and type the hexadecimal PID value for the System Messages stream.

i In the **Dncs ASI Pid** column, click in the **CAT** field and type the hexadecimal PID value for the CAT stream.

j In the **Dncs ASI Pid** column, click in the **Messaging** field and type the hexadecimal PID value for the Messaging stream.

k In the **Max Data Rate** column, click in the **EMM** field and type the maximum data rate for this stream in megabits per second (Mbps). Allowable values=0.01-1.0 Mbps.

l In the **Max Data Rate** column, click in the **Fast Refresh EMM** field and type the maximum data rate for this stream in megabits per second (Mbps). Allowable values=0.51-3.0 Mbps.

m In the **Max Data Rate** column, click in the **System Messages** field and type the maximum data rate for this stream in megabits per second (Mbps). Allowable values=0.01-3.0 Mbps.

n In the **Max Data Rate** column, click in the **CAT** field and type the maximum data rate for the CAT stream in megabits per second (Mbps). Allowable values=0.01-1.0 Mbps.

o In the **Max Data Rate** column, click in the **Messaging** field and and type the maximum data rate for this stream in Mbps. Allowable values=0.01–1.0 Mbps.

13 Click **OK**. The OIT Data Configuration window closes.

14 Click **Save** on the Set Up CMTS/OIT Bridge window. Your OIT Bridge Configuration settings are saved.

Important:

- After you save your OIT Data Configuration settings, the Hub Name, Bridge Name, and the OIT Bridge checkbox cannot be changed.

- If you need to set up CMTS bridges, refer to the online Help.

15 After you have configured the OIT bridges, you must now use the SI-Server to re-configure all of your D96xx re-multiplexers (including the Home D96xx) to pass OIT programs and PIDs.

Important: The programs 0x1FF8 and 0x1 should also be passed to the SI-Server along with the three programs listed in items a. through c. in step 5 (EMM, Fast Refresh EMM, and System Messages).

Note: For more information, refer to step 5 of *Configuring the SI-Server, D96xx Re-Multiplexers, and the DCM* (on page 16).
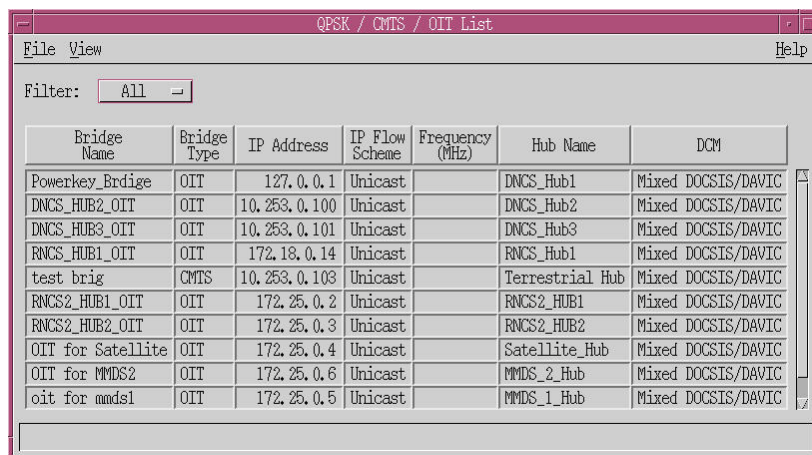
Configure Satellite OIT Bridge

For each of the satellite hubs configured, you must configure a separate out-of-band to in-band translator (OIT) bridge. The OIT bridge inserts MPEG private sections into the DNCS outbound transport stream. This bridge is used for the following:

- Sends PowerKEY EMMs and PowerKEY system information

- Sends DSM-CC Passthrough and UN-Config messages

- Uses reserved PIDs 32, 33, 34, and 35 for transporting information as follows:

  - PID 32 and 33 are used for EMMs

  - PID 34 is used for PowerKEY system information and DSM-CC messages

  - PID 35 is used for multimedia messages

To configure an OIT bridge, complete the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Home Element Provisioning** tab.

3 Click **QPSK/CMTS/OIT**. The QPSK/CMTS/OIT List window opens.

Bridge Name	Bridge Type	IP Address	IP Flow Scheme	Frequency (MHz)	Hub Name	DCM
Powerkey_Brdige	OIT	127.0.0.1	Unicast		DNCS_Hub1	Mixed DOCSIS/DAVIC
DNCS_HUB2_OIT	OIT	10.253.0.100	Unicast		DNCS_Hub2	Mixed DOCSIS/DAVIC
DNCS_HUB3_OIT	OIT	10.253.0.101	Unicast		DNCS_Hub3	Mixed DOCSIS/DAVIC
RNCS_HUB1_OIT	OIT	172.18.0.14	Unicast		RNCS_Hub1	Mixed DOCSIS/DAVIC
test brig	CMTS	10.253.0.103	Unicast		Terrestrial Hub	Mixed DOCSIS/DAVIC
RNCS2_HUB1_OIT	OIT	172.25.0.2	Unicast		RNCS2_HUB1	Mixed DOCSIS/DAVIC
RNCS2_HUB2_OIT	OIT	172.25.0.3	Unicast		RNCS2_HUB2	Mixed DOCSIS/DAVIC
OIT for Satellite	OIT	172.25.0.4	Unicast		Satellite_Hub	Mixed DOCSIS/DAVIC
OIT for MMDS2	OIT	172.25.0.6	Unicast		MMDS_2_Hub	Mixed DOCSIS/DAVIC
oit for mmds1	OIT	172.25.0.5	Unicast		MMDS_1_Hub	Mixed DOCSIS/DAVIC
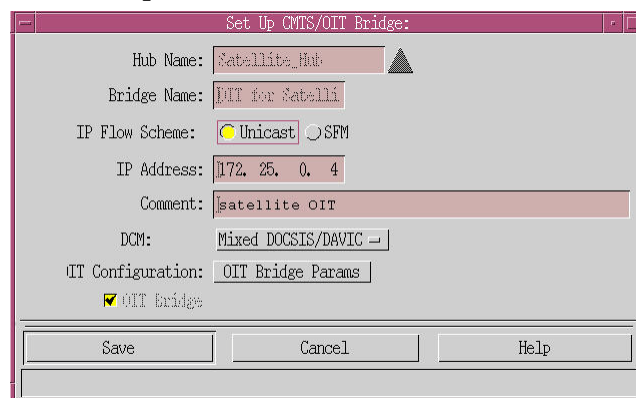
4 Click **File** and **New** and select **CMTS/OIT**. A Set Up CMTS/OIT Bridge window opens.

5 Select the Satellite Hub.

6 In the **Bridge Name** field, enter the name of the bridge.

7 In the **IP Address** field, enter the virtual IP address for the OIT bridge. You must use this IP address for this bridge.

8 Select **Unicast** for the IP Flow Scheme.

9 In the **Comment** field, enter a description of this bridge.

10 From the **DCM** drop-down list, select **Mixed DOCSIS/DAVIC**.

11 To enable OIT Bridges, select the **OIT Bridge** checkbox in the Set Up CMTS/OIT Bridge window. The OIT Bridge Params button is now enabled.

   Important: You can only create one OIT Bridge per hub.

12 Click **OIT Bridge Params** to enable the bridge. A Set Up CMTS/OIT Screen window opens.

13 Complete the fields as follows:

- For **EMM,** enter the following values:
  - **20** for the PID
  - **20** for the DNCS ASI PID
  - **0.10 Mbps** for the Max Data Rate

- For the **Fast Refresh EMM**, enter the following values:
  - **21** for the PID
  - **21** for the DNCS ASI PID
  - **1.00 Mbps** for the Max Data Rate

- For **System Messages**, enter the following values:
  - **22** for the PID
  - **22** for the DNCS ASI PID
  - **0.40 Mbps** for the Max Data Rate

- For **CAT**, enter the following values:
  - **1** for the PID
  - **1** for the DNCS ASI PID
  - **0.10 Mbps** for the Max Data Rate

- For **Messaging**, enter the following values:
  - **23** for the PID
  - **23** for the DNCS ASI PID
  - **0.10 Mbps** for the Max Data Rate

14 Click **OK** to enter the parameters in the database.

15 Click **Save**.

Configuring Virtual IP Addresses

Complete the procedure listed in this section to create a virtual IP address.

Important: Before you begin, obtain the **hostname** and the **IP address** you want to use.

1 Open an xterm window on the DNCS and log on as **root**.

2 Locate the IP address of the TED using the following command:

ping –a dncsted

A result similar to the following appears:

dncsted (192.168.1.2) is alive

3 Run the following command to list all available interfaces:
ifconfig –a

Example: (output may vary significantly)

```
lo0: flags=2001000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4,
VIRTUAL> mtu 8232 index 1 inet 127.0.0.1 netmask ff000000

ce0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 2 inet 10.253.0.1 netmask ffffc000 broadcast
10.253.63.255

ce1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 3 inet 10.78.192.176 netmask fffff800 broadcast
10.78.199.255

eri0: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu
1500 index 4 inet 192.168.1.1 netmask ffffff00 broadcast
192.168.1.255

ci0: flags=1001000842<BROADCAST,RUNNING,MULTICAST,IPv4,
FIXEDMTU> mtu 9180 index 5 inet 10.253.0.1 netmask ffffc000
broadcast 10.253.63.255
```

Notes:

- The alphanumeric combination in the left column is the name of the interface.

- These interface names are possible: ce, hme, eri, bge, lo, ci. Any combination of these interfaces may be present.

- In this example, there are 5 interfaces shown:

    – lo0 (127.0.0.xxx)

    Note: The "l" in this example is a lowercase "L" and not the number 1 (one).

    – ce0 (10.253.0.xxx)

    – ce1 (10.78.192.xxx)

    – eri0 (192.168.1.xxx)

    – ci0 (10.253.0.xxx)

4 Determine which interface is the TED interface.

Note: In this example the TED interface is the one with the same three octets as the TED IP address. In this case, the eri0 (192.168.1.xxx) is the TED interface.

5 Select the interface to use to create the virtual IP address.

Important:

- The interface cannot be the TED interface

- The interface cannot be the lo interface

- The interface cannot be a ci interface

- The interface cannot be a dncsatm interface

    Note: In this case, you may choose either the ce0 or the ce1 interface for creating virtual IP addresses. For our example we will select the ce0 interface.

6   Using the following command, create a new file and save:

vi /etc/hostname.ce1:x

Note: The "x" will represent the number of the virtual interface (1, 2, 3, etc.).

7   Edit the /etc/hostname.ce1:x file and add the following row to the file:

 <Virtual IP Hostname> or <Virtual IP Address>

Example row: dncsv1

8   Make a backup copy of the /etc/hosts file.

9   Edit the /etc/hosts file and add the following row to the file:

<ipaddress><tab space><hostname>

Notes:

- The <ipaddress> entry can be any available IP address that has the same three octets as the interface. (In this case: 10.78.192.xxx)

- The <hostname> entry is the name you want to give this interface (e.g. dncsvirt1, rncs1virt1, or dncsv2).

   Example row:

   10.78.192.01   dncsv1

10   Plumb the virtual interface using the following command:

Ifconfig plumb <virutual Interface>

Example: Ifconfig plumb ce1:1

11   After you have created all the virtual IP addresses that you need, in order for the changes to take effect, you must restart the service using the following commands in the xterm window:
svcadm –v disable svc:/network/physical:default
svcadm –v enable svc:/network/physical:default

12   Repeat this entire procedure for each RNCS.

5

Setting Up Direct ASI

Introduction

Direct ASI is a vehicle for delivering inband BFS data directly from the DNCS to the to the SCS/MQAM modulators using an ASI link. This chapter provides procedures for setting up Direct ASI, tearing down and rebuilding sessions, and switching the system to Direct ASI mode.

In This Chapter

Configure the Direct ASI Cards

Introduction

The PowerKEY DVB System uses Direct ASI input to an ASI card installed in the DNCS.

Configuring the Direct ASI Cards

1   From the DNCS Administrative Console, click the **Applications Interface Modules** tab.
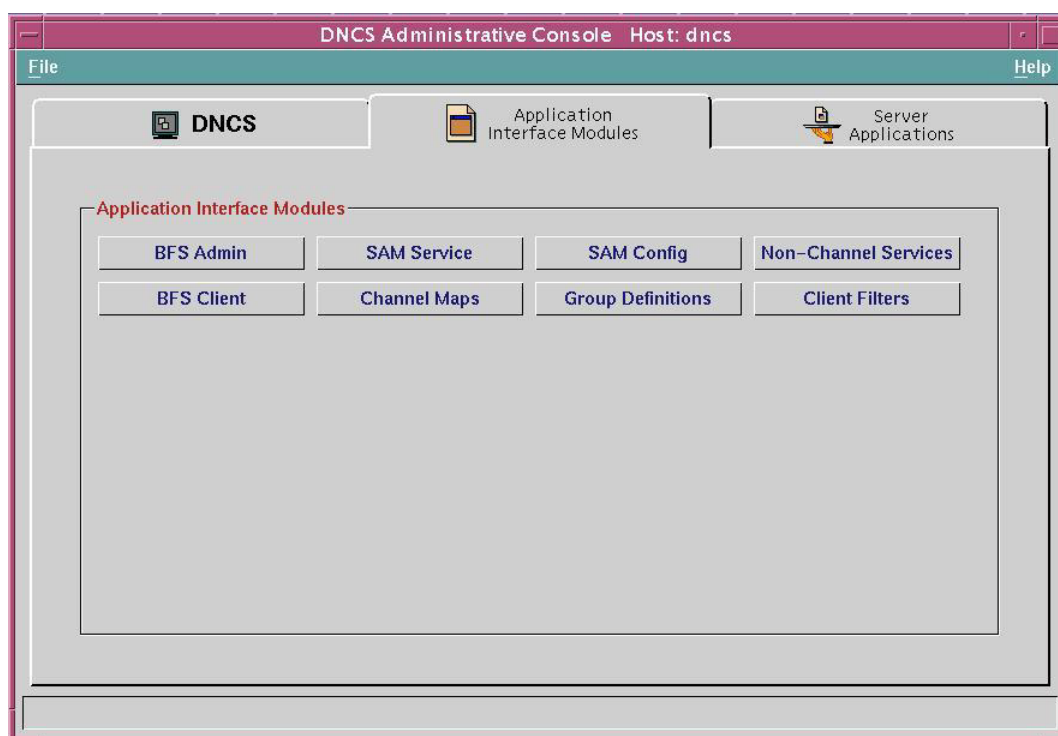
2   Select **BFS Admin**.

3   Is Distributed DNCS licensed and enabled?

- If **yes**, go to step 4.

- If **no,** go to step 5.

4   The BFS Admin Sites window opens displaying a list of configured sites. Select one of the listed sites, click **File > All Sites** and then go to step 5.
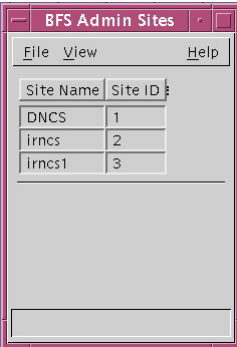
5 The Site DNCS BFS Administration window opens with the Servers tab in the forefront.
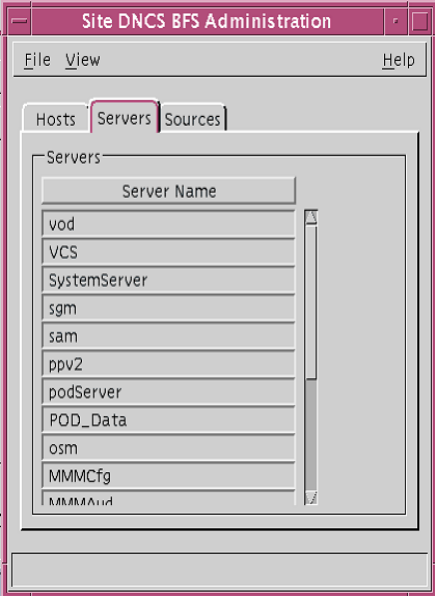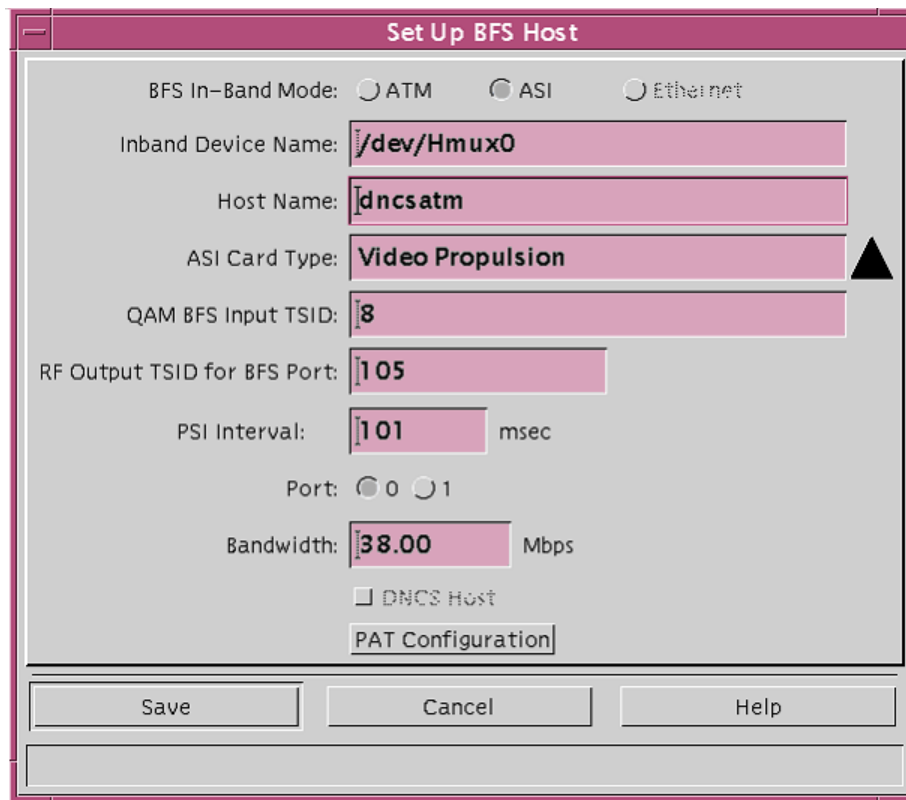
6 From the Site DNCS BFS Administration window, click the **Hosts** tab.
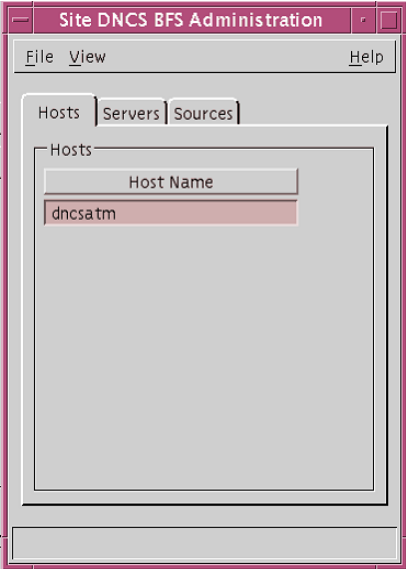
7   Double-click **dncsatm** in the Host Name field. The Set Up BFS Host window opens.

Important: If no entry is present in the Set Up BFS Host window, return to the Site DNCS BFS Administration window and create a new entry by selecting **File > New** from the menu. Make sure that the host name is **dncsatm**.

8 Does **/dev/Hmux0** appear in the Inband Device Name field?

- If **yes**, go to step 9.

- If **no**, click in the Inband Device Name field, type **/dev/Hmux0**, then go to step 9.

9 Does the transport stream (TS) ID shown in the QAM BFS Input TSID field match the Home SCS/MQAM TSID that you defined when you configured the MPEG sources?

- If **yes**, go to step 10.

- If **no**, click in the Transport Stream ID field, type the correct TS ID, then go to step 10.

10 Verify that the RF Output TSID for BFS Port entry is correct.

Important: The RF Output TSID for BFS Port field specifies the RF output port number corresponding to the MQAM/SCS device output. The value for this field will be the value in the output TSID found on the SCS page. For additional details, see *Setting Up SCS Ports Modeling Parameters* (on page 63).

11 Verify that the PSI Interval setting is correct.
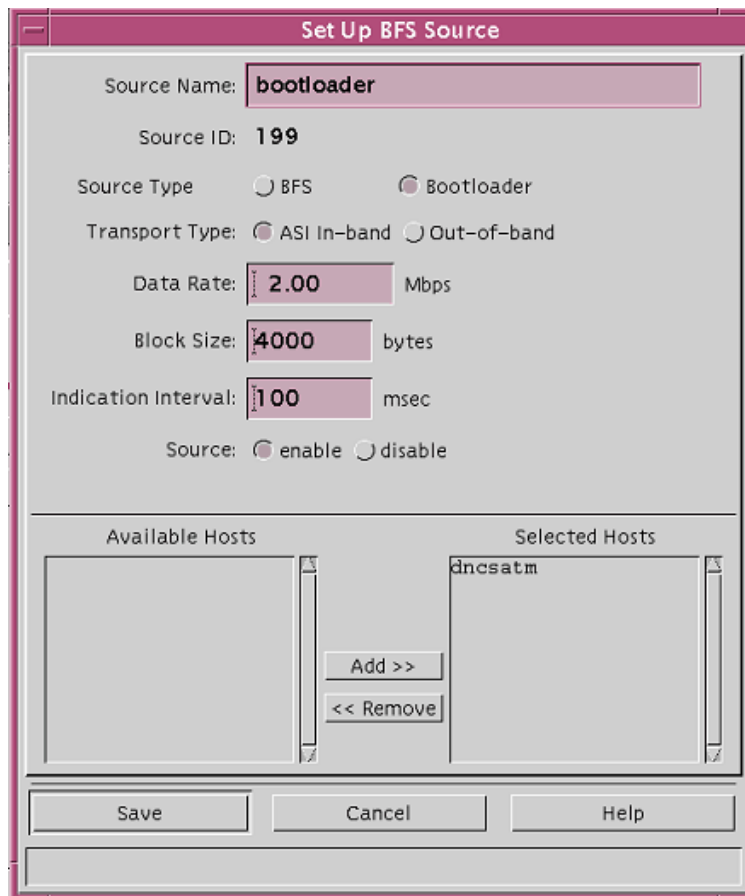
Note: The PSI interval is the interval at which the PAT and the PMT are transmitted by the ASI card. The default value is **80** msec.

12 Is **Port 0** (zero) selected?

- If **yes**, go to step 13.

- If **no**, select 0 (zero), then go to step 13.

13 Verify the setting in the **Bandwidth** field.

Note: The recommended setting is 38.80 Mbps.

14 Click **Save** to save your settings. Your settings are saved and the BFS Administration window opens.

15 From the Site DNCS BFS Administration window, click the **Sources** tab. A list of sources similar to the following example opens.
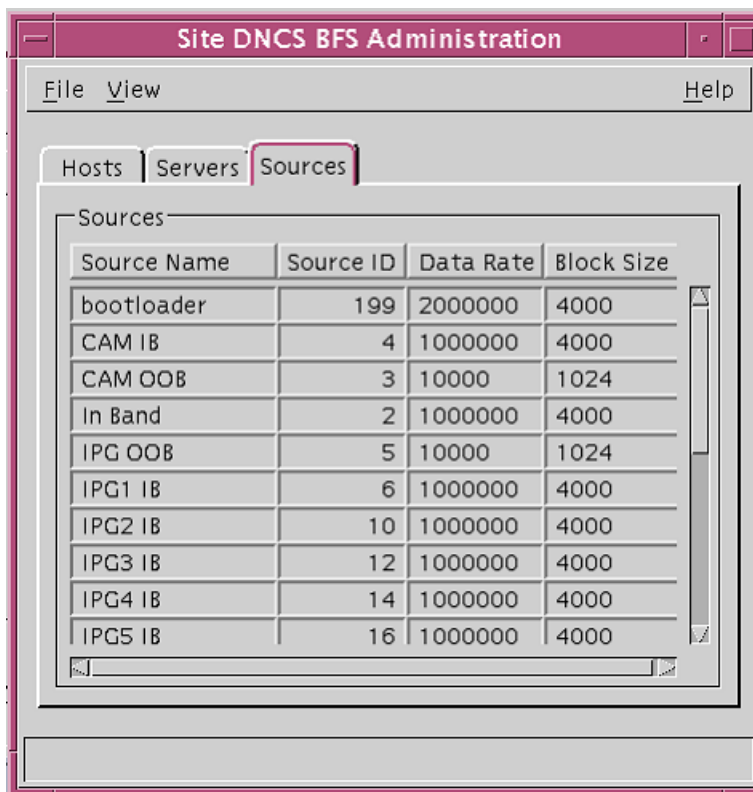
16 In the BFS Administration window, double-click a Source Name. A Set Up BFS Source window similar to the following example opens and displays information for Bootloader.

17 Verify the following information only for Bootloader and not for each source:

    p   If the source is not enabled, select **enable**.

    q   If **dncsatm** is not listed in the Selected Hosts field, move it from the Available Hosts field to the Selected Hosts field.

    r   Did you make any changes?

        – If **yes**, click **Save** to save your settings. Your new settings are saved, the Set Up BFS Source window closes, and the Site DNCS BFS Administration window re-opens.

        – If **no**, click **Cancel**. The Set Up BFS Source window closes and the BFS Administration window re-opens.

18 In the Site DNCS BFS Administration window, click **File** then select **Close**. The BFS Administration window closes.

Obtain BFS MPEG Program Numbers

Introduction

You must use the SI-Server to provision the Home SCS/MUX for the home MQAM to pass BFS services to all of the re-multiplexers in the system. First, however, you must obtain the BFS MPEG program numbers for each session. This section provides a procedure for obtaining the BFS MPEG program numbers.

Obtaining BFS MPEG Program Numbers

1   On the DNCS Administrative Console, select the **Utilities** tab, and then click **Session List**. The Session Filter window opens.
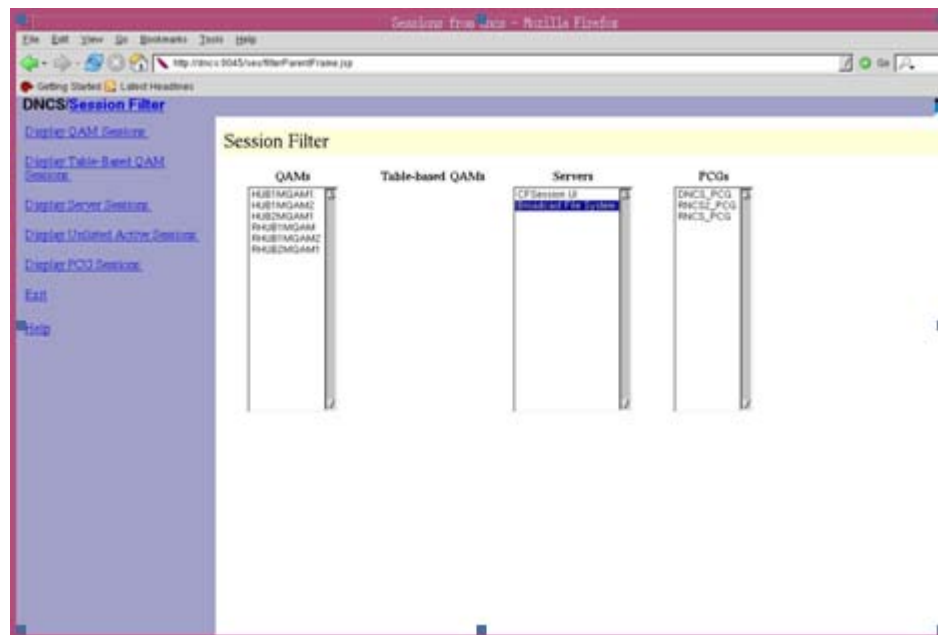
2   In the Session Filter window, highlight **Broadcast File System** in the Servers column, and then click **Display Server Sessions**. The Session Data for selected Servers window opens.
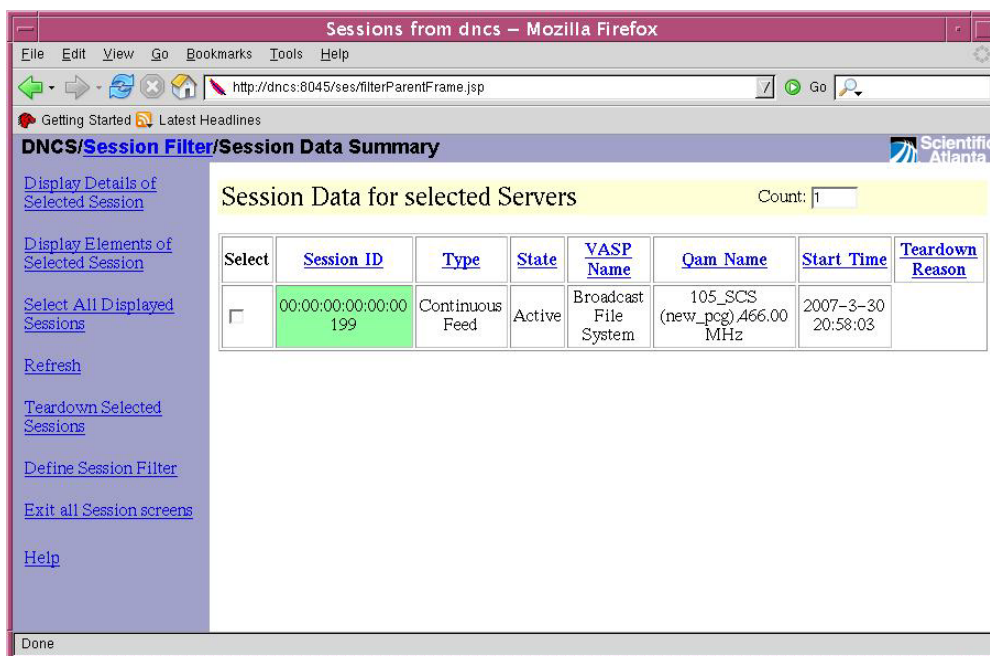
3 In the Session Data for selected Servers window, select the Session ID, and then click **Display Details of Selected Session**.

Example: 00:00:00:00:00:00: 199

Note: BFS sessions are numbered 2 through 22, and also include the Bootloader session 199. Select only the Bootloader (199) session.

Result: The Details of Session 00:00:00:00:00:00: 199 window opens.
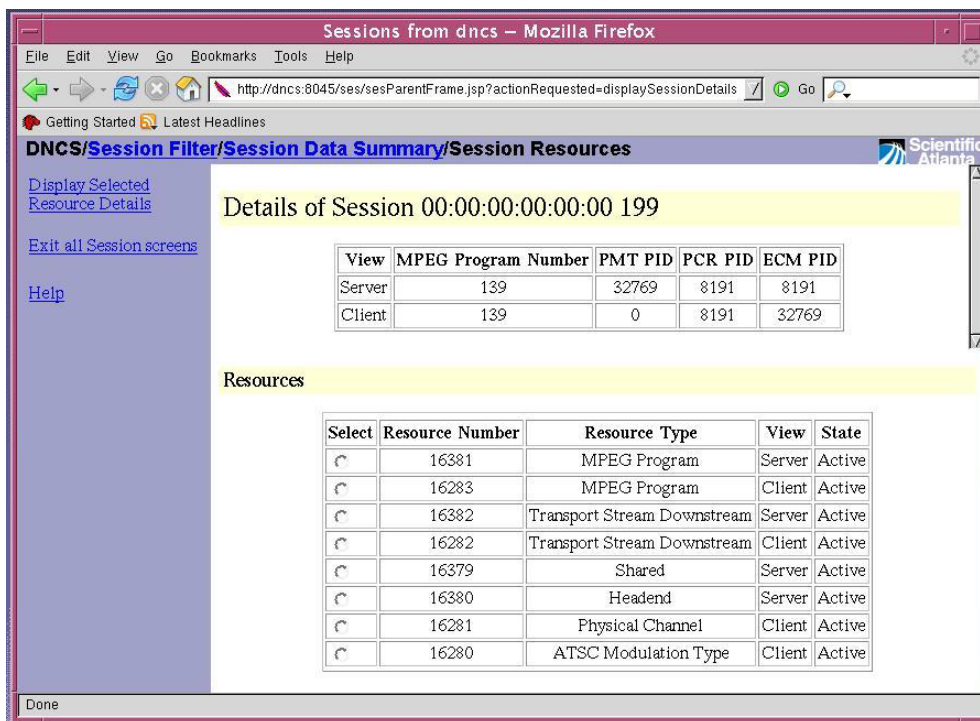
4 In the Resources section of the Details of Session 00:00:00:00:00:00: 199 window, select an MPEG Program listed in the Resource Type column, and then click **Display Selected Resource Details**. The MPEG Program Resource Details window opens.
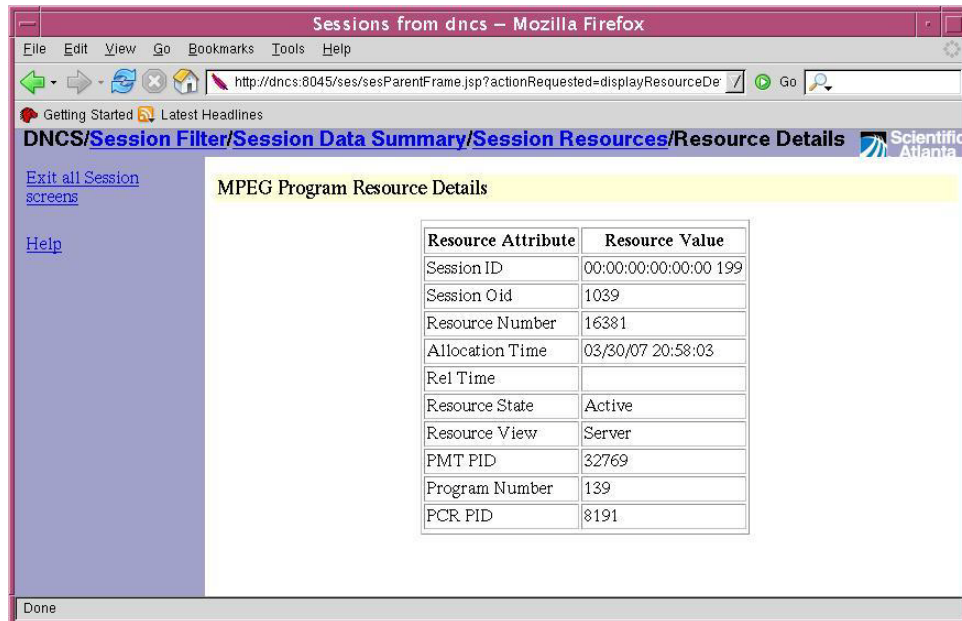
5 Write down the MPEG program resource details for that session.

6 Click **Exit all Session screens** to close the MPEG Program Resource Details window.

7 Use these MPEG program resource details to provision the BFS service on the Home SCS/MUX for the home MQAM in the SI-Server.

8 When you have completed the configuration, close all DNCS windows.

9 Use the SI-Server to re-configure the SCS/MUX for the MQAM to pass DNCS Direct ASI programs and PIDs.

10 Go to *Creating Sources and Setting Up Sessions* (on page 89).

6

Creating Sources and Setting Up Sessions

Introduction

After completing the Direct ASI setup, you must create sources and set up sessions. This chapter provides procedures for creating sources and setting up sessions.

In This Chapter

Add a Service Source

Introduction

After you have set up all of your network elements, the next step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the service source. In this case, a service source is the digital or analog signal that the PowerKEY DVB System uses to deliver a service to subscribers.

For example, you can use the signal from Fox Sports World (FOXSW) to create different services, just as a processing plant might take a raw material like sugar and add other ingredients to it to create different kinds of soft drinks. To illustrate, you could define three different kinds of services from a single FOXSW signal:

- You could offer the FOXSW broadcast as a clear service to all subscribers.

- By encrypting the FOXSW broadcast, you could offer it as a secure, subscription-based service only to subscribers who have paid extra for it.

- By encrypting it and setting it up as a PPV service, you could offer a portion of it, maybe a special sporting event, only to subscribers who have paid for the event.

Important: Refer to *Appendix A, Sources and Services Naming Conventions* (on page 201) before adding and defining service sources.

Time to Complete

Adding a service source takes approximately 5 minutes to complete.

Performance Impact

Adding a service source does not impact network performance. You can complete this procedure at any time.

Adding a Service Source

Complete the following steps to add a source for a service.
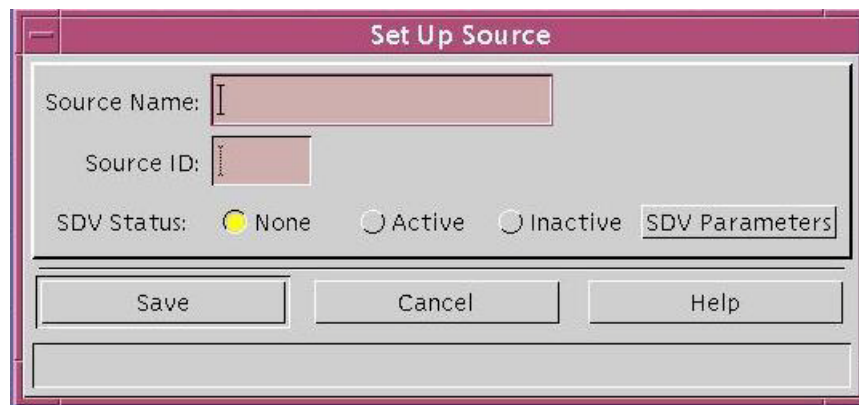
1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

2 Click **Source**. The Source List window opens.

3 Click **File** then choose **New**. The Set Up Source window opens.

4 Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

Important: We recommend that you use a naming scheme that indicates the source type (analog or digital), the channel number the service will use, and the service name. For example, a source name of **D02 WeatherScan** indicates that this is a digital source (**D**) providing content on channel 2 (**02**) for the WeatherScan service.

5 Click in the **Source ID** field and type the number you will use to identify this source.

Notes:

■ Remember the Service Source ID. You will need it as you continue to set up the service.

■ Use the Source ID values that are above 200.

- See *Appendix A, Sources and Services Naming Conventions* (on page 201) for the convention for numbering the source ID in the PowerKEY DVB System.

Important: The Source ID should be unique across the programs provisioned in the DNCS. It should be the same as the one assigned in the SI-Server.

6   Click **Save**.

Results:

- The system saves the service source information in the DNCS database and closes the Set Up Source window.

- The Source List window updates to include the new service source.

7   Next you must define parameters for the service source. See the following sections to complete this process:

- *Encrypt a Service* (on page 93)

- *Add an Unlimited Segment* (on page 95)

- *Add a Service Package* (on page 97)

- *Add a Secure Service to a Package* (on page 99)

- *Define Service Sources and Build Sessions* (on page 102).

Encrypt a Service

After you define a secure or PPV service source, you must set the system to encrypt all of the content coming from that source. Encryption ensures that this content is available only to authorized subscribers.

Complete these steps to encrypt service content.

Note: This procedure applies to secure and PPV services. It does not apply to clear services.

1 Is the Source List window open?

- If **yes,** go to step 5.

- If **no**, go to step 2.

2 On the DNCS Administrative Console, click the **DNCS** tab.

3 Click the System Provisioning tab.

4 Click **Source**. The Source List window opens.

5 Click once on the row containing the service source you need to encrypt.

6 Click **File > Security Modes**. The Security Mode List window opens for the service source you selected.

7 Click **File > New**. The Set Up Security Mode window opens.

8 In the Security Mode field, click the **Encrypted** option.

9 Do you want the content to be encrypted immediately?

- If **yes**, in the **Date/Time** field, click the **Now** option and go to step 13.

- If **no**, in the **Date/Time** field, click the **Custom** option and go to step 10.

10 Click in the **Effective Date** field and type the month, day, and year you want the system to start encrypting all content from this service source.

Important: You must type two digits for the month and day, and four digits for the year. When finished, go to step 11.

Example: You would type July 4, 2008, as 07042008. The system inputs the slashes for you and displays 07/04/2008.

11 Click in the **Effective Time** field and type the hour, minute, and second you want the system to start encrypting all content from this service source.

Important: You must type two digits for each value. When finished, go to step 12.

Example: You would type eight o'clock as 080000. The system inputs the colons for you and displays 08:00:00.

Notes:

- Make sure the time you enter is at least 15 minutes into the future.

- You can also represent time in the 24-hour format. For example, 18:30:00 would represent 6:30 p.m.

12 Click **AM/PM** to establish which portion of the day you want the system to start encrypting all content from this service source. When finished, go to step 13.

13 Click **Save**. The system saves the encryption information in the DNCS database and closes the Set Up Security Mode window. The Security Mode List window updates to include the new encryption information.

14 Do you need to set up another security mode for this service source? For example, you may want to allow all of your subscribers to have access to a normally encrypted service (such as HBO) for a limited time (such as a weekend) in an attempt to entice more people to purchase the service.

- If **yes**, repeat steps 7 through 13.

- If **no**, go to step 15.

15 Click **File > Close** to close the Security Mode List window and return to the Source List window.

16 Continue setting up the type of service you would like to provide.

Important: For detailed descriptions of the procedures for these services, refer to the online Help.

- For clear services, continue with the appropriate step of **Set Up a Clear Service**.

- For secure (encrypted) services, continue with the appropriate step of **Set Up a Secure Service**.

- For PPV services, continue with the appropriate step of **Set Up a PPV Service**.

Add an Unlimited Segment

After you encrypt a secure service, you must set up an unlimited segment for that service source. Setting up an unlimited segment for a source instructs the system to continuously send content from that source. This allows authorized subscribers to access the service content at any time.

Time to Complete

Adding an unlimited segment takes approximately 10 minutes to complete.

Performance Impact

Adding an unlimited segment does not impact network performance. You can complete this procedure at any time.

Adding an Unlimited Segment

Complete these steps to set up an unlimited segment for a service source.

Note: This procedure applies only to secure services. It does not apply to clear or PPV services.

1   Is the Source List window open?

- If **yes**, go to step 5.

- If **no**, go to step 2.

2   On the DNCS Administrative Console, click the **DNCS** tab.

3   Click the S**ystem Provisioning** tab.

4   Click **Source**. The Source List window opens.

5   Click once on the row containing the service source for which you are setting up an unlimited segment.

6   Click **File** and select **Segments**. The Segment List (by Source) window opens for the source you selected.

7   Click **File** and select **New**. The Set Up Segment window opens.

8   Click in the **Name** field and type the name you want to use to identify this segment. You can use up to 20 alphanumeric characters.

9   In the Duration field, click the **Unlimited** option, if not already selected. This allows the service content to be available at all times.

Note: Do not complete the **Start Date** and **Start Time** fields. The DNCS automatically selects the current date as the start date, with the start time several minutes in the future.

10 Verify that **Blackout/Spotlight Control** is set to None. If it is not, select None to ensure that this option is disabled.

11 Verify that Fingerprint is set to **None**. If it is not, select **None** to disable this option.

12 In the Digital Copy Rights area, select **Copy One Generation**.

13 In the Macrovision area, select **Disabled**.

14 In the CIT (constrained image trigger) flag area, select **Clear**.

15 Click **Save**. The system saves the segment information in the DNCS database and closes the Set Up Segment window. The Segment List (by Source) window updates to include the new segment information. If you scroll through the list horizontally, you will see a yellow band that indicates when the segment is scheduled to start and stop its duration.

16 Do you need to set up another unlimited segment for this service source? For example, you may want to enable fingerprinting for some of the set-tops. You would need to create another unlimited segment with the fingerprinting option enabled and authorize the set-top with this segment.

- If **yes**, repeat steps 7 through 15.

- If **no**, click **File** and select **Close** to close the Segment List (by Source) window and return to the Source List window. Go to step 17.

17 Click **File** and select **Close** to close the Source List window and return to the DNCS Administrative Console.

18 Continue setting up the type of service you would like to provide.

Important: For detailed descriptions of the procedures for these services, refer to the online Help.

- For clear services, continue with the appropriate step of **Set Up a Clear Service**.

- For secure (encrypted) services, continue with the appropriate step of **Set Up a Secure Service**.

- For PPV services, continue with the appropriate step of **Set Up a PPV Service**.

Add a Service Package

Notes:

- This procedure applies to secure and packages clear services.

- Do not use this procedure for PPV or uinpackaged clear services.

A package consists of one or more services that are available only to specifically authorized subscribers. For example, because secure services are encrypted, the only way for a subscriber to access a secure service is for you to place the service in a package. Then, you can authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable the DHCT to decrypt the secure service.

On the other hand, clear services are sent through the network unencrypted or unscrambled. Therefore, they are available to all of the subscribers in your network and you do not need to add them to packages.

Guidelines

Keep in mind the following important guidelines when you add a service package to the DNCS:

- You must add a secure service to a package. Otherwise, your authorized subscribers will not be able to access it.

- You must add a service package for each channel-based service. Otherwise, your authorized subscribers will not be able to access the service.

- Because clear services are not encrypted, packaging a clear service does not protect it from being accessed (stolen) by unauthorized users.

- The package name that you use must be compatible with the package name rules that your billing system uses. Contact your billing system vendor if you are unsure of their rules for naming packages.

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

Adding a Service Package

Complete these steps to add a new service package to the DNCS.

Note: This procedure applies to secure and packaged clear services. It does not apply to PPV or unpackaged clear services.

1   On the DNCS Administrative Console, click the **DNCS** tab.

2   Click the **System Provisioning** tab.

3   Click **Package**. The Package List window opens.

   Note: By default, the Package List window shows only non-PPV packages (Subscription Only). To view the list of all packages, click the **Show** button and select All Packages.

4   Click **File** and select **New**. The Set Up Package window opens.

5   Click in the Package Name field and type the name you will use to identify this package. You can use up to 20 alphanumeric characters.

   Important: The package name that you enter must be compatible with the package name rules that your billing system uses. However, the default package name should be compatible with your billing system rules. Contact your billing system vendor if you are unsure of their rules for naming packages.

   Notes:

   ▪   The Unlimited option in the Duration field is selected by default. This option allows the subscriber to have unlimited access to the package. Do not change this option without first consulting our technical support. Refer to **Customer Support** in Chapter 16 for detailed information.

   ▪   Do not select the PPV, IPPV, or Allow Event Extension options. The DNCS does not support these options at this time.

6   Click **Save**. The system saves the package information in the DNCS database and closes the Set Up Package window. The Package List window updates to include the new package.

7   Continue setting up the type of service you would like to provide.

   Important: For detailed descriptions of the procedures for these services, refer to the online Help.

   ▪   For clear services, continue with the appropriate step of **Set Up a Clear Service**.

   ▪   For secure (encrypted) services, continue with the appropriate step of **Set Up a Secure Service**.

   ▪   For PPV services, continue with the appropriate step of **Set Up a PPV Service**.

Add a Secure Service to a Package

Note: This procedure applies only to secure services. It does not apply to clear or PPV services.

After you set up an unlimited segment for a secure service, you must add the service segment to a package. A package consists of one or more service segments that are available only to specifically authorized subscribers.

For example, you can offer subscribers different levels of service, such as Basic and Premium. Your Basic service could include nothing but clear services. Because these services are sent to all subscribers in the clear (unencrypted), you do not need to add them to packages.

On the other hand, your Premium service could offer additional services to subscribers who are willing to pay extra for them. You encrypt those additional services to keep them secure from being accessed by anyone who has not paid the extra price for them.

The only way for a subscriber to access secure services is for you to place the secure services in a package, and then authorize the subscriber's DHCT to receive the package. When you authorize the DHCT to receive the package, you enable that DHCT to decrypt the secure services.

Before You Begin

If you need to add a secure service to a new package, you must first add the package to the DNCS. If necessary, go to *Add a Service Package* (on page 97) before you begin this procedure.

Time to Complete

Adding a service package takes approximately 10 minutes.

Performance Impact

Adding a service package does not impact network performance. You can complete this procedure at any time.

Adding a Secure Service to a Package

Complete these steps to add a secure service to a service package.

Note: This procedure applies only to secure services. It does not apply to clear or PPV services.

1   Is the Package List window open?

   ■   If **yes,** go to step 5.

   ■   If **no,** go to step 2.

2   On the DNCS Administrative Console, click the **DNCS** tab.

3   Click the **System Provisioning** tab.

4   Click **Package**. The Package List window opens.

   Note: By the default, the Package List window shows only non-PPV packages (Subscription Only). To view the list of all packages, click the **Show** button and select **All Packages**.

5   Click once on the row containing the package to which you want to add a service segment.

6   Click **File** and select **Provision**. The Package Provisioning window opens for the package you selected.

7   Click **File** and select **Add Segment**. The Segment Selection window opens showing all of the service segments that have been defined on your system.

   Important: Although there is an option to add packages to a package, do not select this option. This version of the DNCS does not support packages within packages.

8   Click to select the service segment you want to add to this package. You can select more than one segment by holding down the Ctrl key as you click on each segment.

9   Click **OK** to close the Segment Selection window. The Package Provisioning window updates to include the service segment(s) you selected for the package.

10 Click **File** and select **Close** to close the Package Provisioning window and return to the Package List window.

11 Do you need to add a service segment to another package?

   ■   If **yes**, repeat steps 5 through 10.

   ■   If **no**, click **File** and select **Close** to close the Package List window and return to the DNCS Administrative Console. When finished, go to step 12.

12 Continue setting up the type of service you would like to provide.

Important: For detailed descriptions of the procedures for these services, refer to the online Help.

- For clear services, continue with the appropriate step of **Set Up a Clear Service**.

- For secure (encrypted) services, continue with the appropriate step of **Set Up a Secure Service**.

- For PPV services, continue with the appropriate step of **Set Up a PPV Service**.

Define Service Sources and Build Sessions

Introduction

After you add a service source to the DNCS database, you must define parameters for the source so that the system knows how to process the service content. When you define a digital service source, you also build a session. Sessions define and allocate the resources that the network uses to deliver service content. When you build a session, you identify the source equipment where the service content originates, such as a D96xx re-multiplexer. You also identify the distribution equipment that places the service content onto the HFC network, such as an SCS/MQAM modulator. It may help to think of a session as a pipeline through the PowerKEY DVB System that is allocated to deliver specific service content.

Important: Refer to *Appendix A, Sources and Services Naming Conventions* (on page 201) before adding and defining service sources.

Before You Begin

Before you define a digital service source, you must have the following information:

- Name of the service source as you defined it when you added the source

- Number of the channel where the service will be displayed

- Service source ID as you defined it when you added the source

- MPEG program number or Elementary Stream Program Identifier from your content service provider

- Amount of bandwidth (in Mbps) to allow for the service (from your content service provider)

- Name of the output distribution equipment that will be receiving the service content from the service source (refer to your network map)

Important: Refer to *Appendix A, Sources and Services Naming Conventions* (on page 201) before defining service sources.

Time to Complete

Defining a digital service source takes approximately 20 minutes to complete.

Performance Impact

Defining a digital service source does not impact network performance. You can complete this procedure at any time.

Defining a Service Source

After you add a digital service source to the DNCS, you must complete these steps to define parameters for that source and build a session for it.

Important: If you are sending the same source content through more than one SCS/MQAM modulator, you must define the source for each modulator using the **Source Definitions** menu option from the **File** menu. For example, if you are sending the same source content through six MQAM modulators, you must define the source six times—once for each SCS/MQAM modulator.
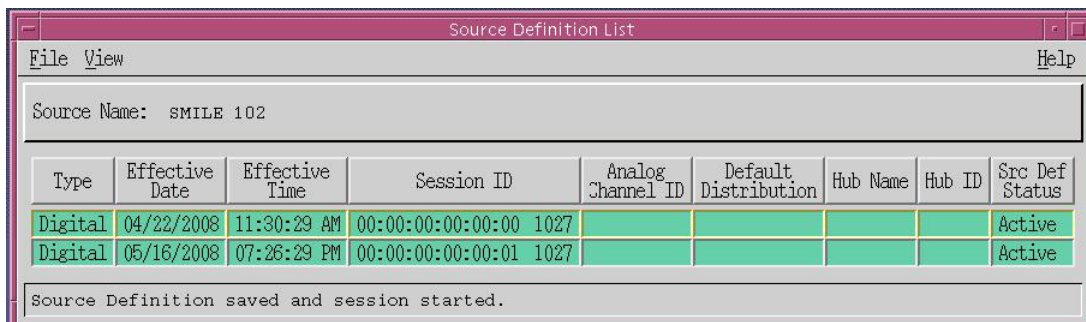
1   Is the Source List window open?

- If **yes**, go to step 5.

- If **no**, go to step 2.

2   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

3   Click **Source**. The Source List window opens.
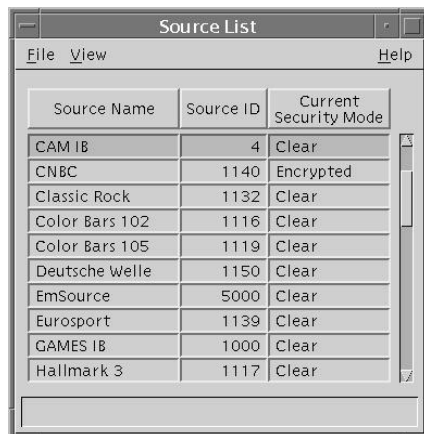
4   Click once on the row containing the service source you need to define.

5   Click **File** then choose **Source Definitions**. The Source Definition List window opens.
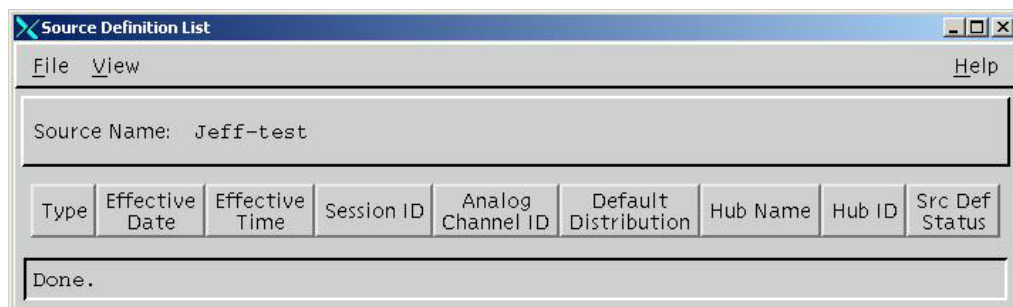
6 If multiple hubs are configured, you must create multiple source definitions for the same source on each hub for different edge devices. The procedure is the same, but you must change the increment of the session ID by 1. In the following example, the first session is 00:00:00:00:00:00 and the second session is 00:00:00:00:00:01.
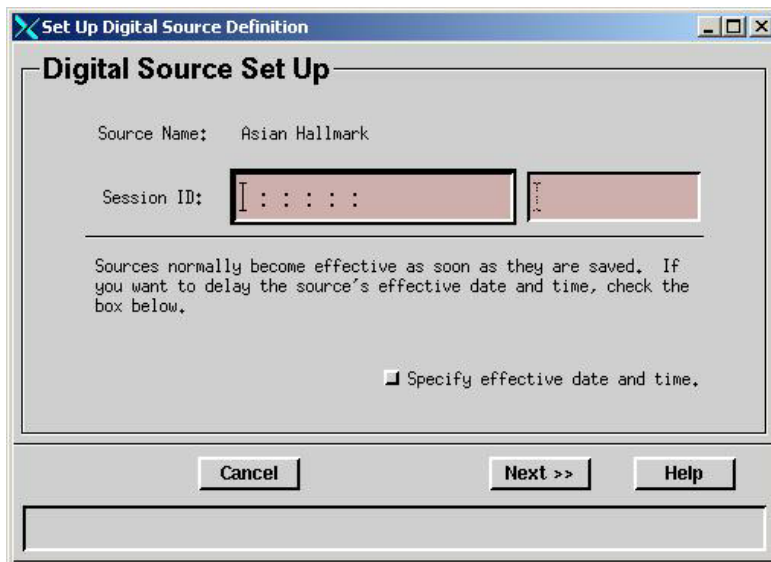
7 On the Source Definition List window, click **File** then choose **New Digital**. The Set Up Digital Source Definition window opens.

8 Click in the **Session ID** field, type the MAC Address and ID of the source in the adjacent box, and then click **Next**. The Define Session window opens.

Notes:

- The session ID will be given as the access criteria in the SI-Server for scrambling.

- When an MQAM modulator is used, select **Broadcast programming**. When a D96xx or a DCM is used, select **SCS-controlled Broadcast**.
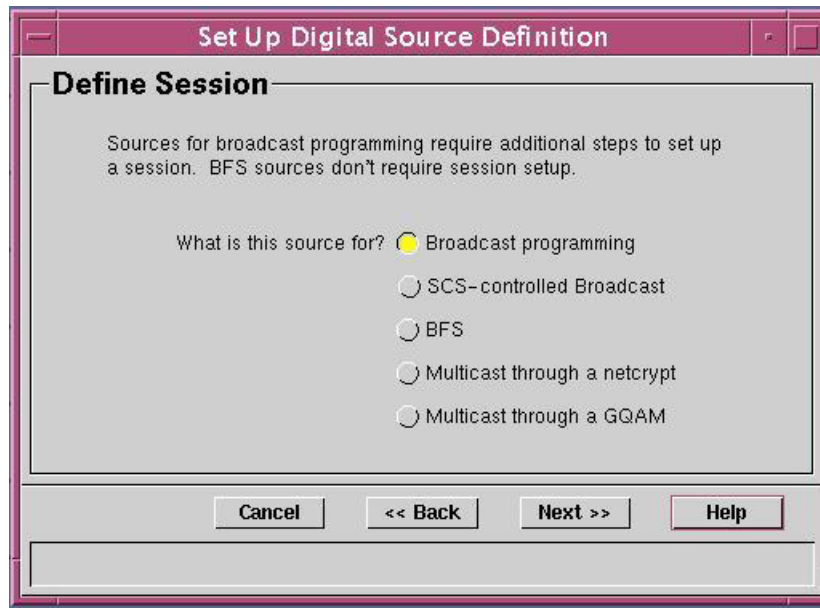
9 Make the appropriate selection for you system (**Broadcast programming** or **SCS-controlled broadcast**), and then click **Next**. The Session Setup window opens.
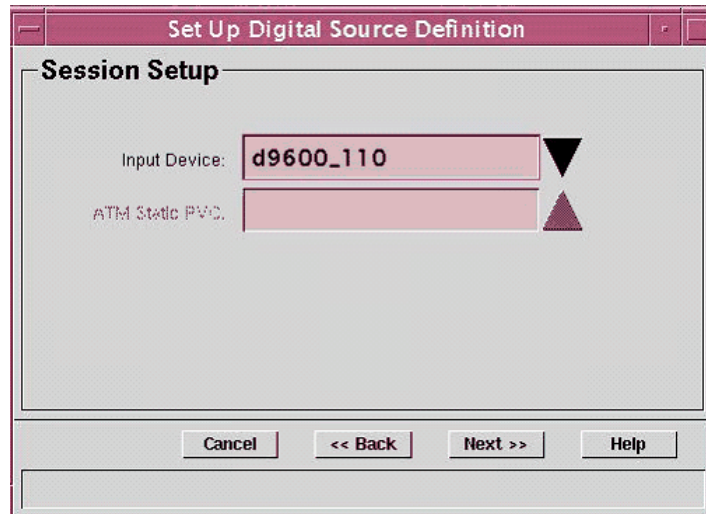
10 Did you select a DCM as the input device in step 9?

- If **yes**, go to step 11.
- If **no,** go step 13.

11 If you selected a DCM as the input device in step 9, a window similar to the following opens.
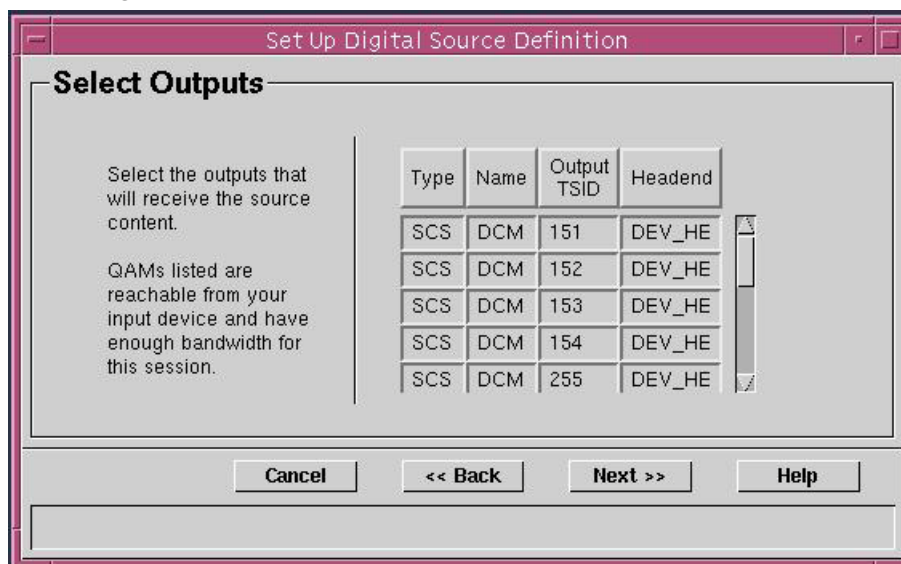
12 Select the appropriate Output TSID, click **Next**, and then go to step 13.

13 Click the **Input Device** arrow and select an input device from the list and click **Next**. The Wrap-up Window opens.
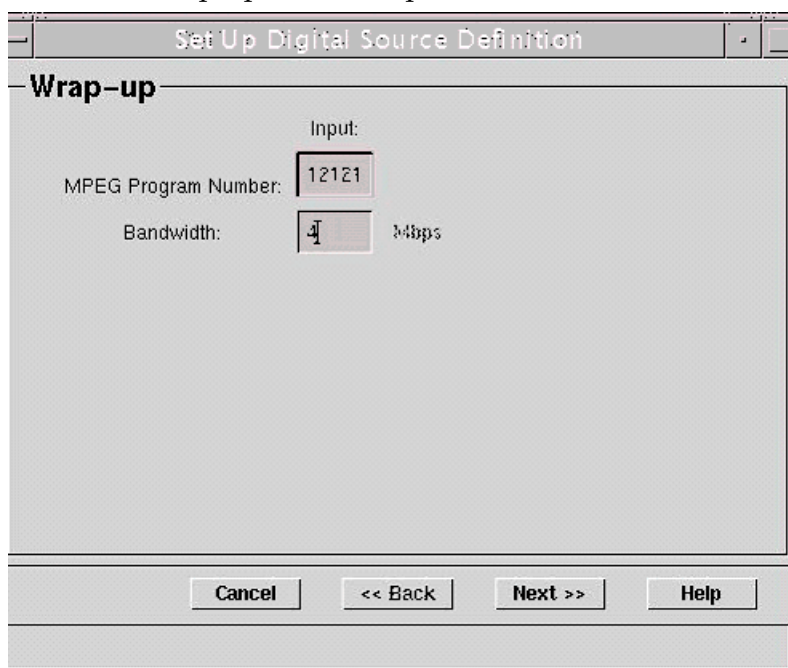
14 Click in the **MPEG Program Number** field, type the MPEG program number for the input device you selected.

15 Click in the **Bandwidth** field, type the bandwidth for the program, and then click **Next**. The Save Source Definition window opens.
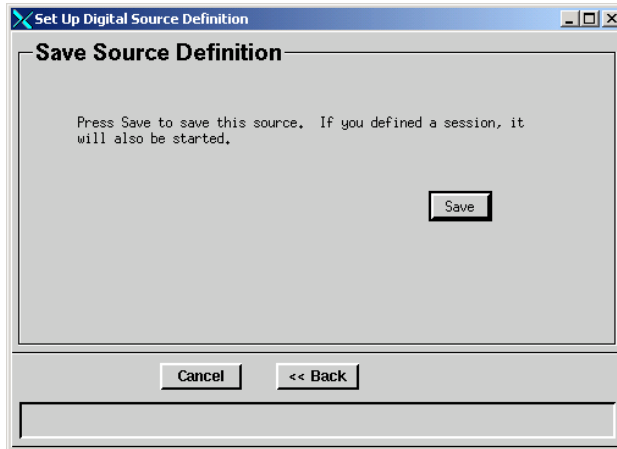
16 Click **Save** to save the source. The system saves the source and starts the session.

Important: SI-Server access criteria must be configured for this source using the same value as the session ID.

Examples:

- If the session ID is 00:00:00:00:00:00 10601, the access criteria in the SI-Server must be 00000000000000002969.

- If the session ID is 00:00:00:00:00:01 10601, the access criteria in the SI-Server must be 00000000000100002969.

Notes:

- When using a D96xx multiplexer or a PCG, session definitions are required only for encrypted channels.

- When you are setting up an encrypted session on the PCG, you must also enable scrambling on the MUX using the SI-Server.

17 Access the Session Filter screen and verify that the sessions were set up correctly.

7

Configuring the PowerKEY DVB System for PPV Services

Introduction

PPV services, like clear broadcasts, are always available to subscribers whenever they tune to a channel carrying the service. The channel displays the service on the subscriber's television. The channel displays a barker that advertises the events that are available for purchase.

There are no control mechanisms or package restrictions that prevent subscribers from accessing the channels where PPV services are offered. Any subscriber can simply tune to a channel that displays the service and order the event. However, the events are considered "secure" because even though the channels are not restricted, the events are only available to subscribers who order them.

This chapter provides steps for creating, modifying, and deleting secure PPV services and events.

In This Chapter

Define PPV Services

This section explains how to create, modify, and delete PPV services.

Before You Begin

Before you can define PPV events for subscribers to purchase, you must define the PPV services that will deliver these events. A **PPV service** is an application that allows subscribers to purchase and view movies, concerts, or sporting events to be viewed at a certain time on a certain channel. A **PPV event** is any program (such as movie, concert, or sporting event) that a subscriber can purchase through a PPV service. If a subscriber has purchased the event that is currently playing on the PPV service, then the PPV service displays that event. If not, then the PPV service displays advertising, interstitials, or some other programming.

As with other services, you must complete the following tasks when defining a PPV service:

- **Add the service source to the DNCS.** This task specifies which digital or analog signal the DBDS will use to deliver the service to subscribers.Refer to *Creating Sources and Setting Up Sessions* (on page 89).

- **Define parameters for the service source.** This task defines the attributes that establish how the system will process service content. Also, this task includes building a session, which defines and allocates the resources that the source will use to deliver the service content. Refer to *Creating Sources and Setting Up Sessions* (on page 89).

- **Encrypt the content coming from the service source.** This task ensures that the content will only be available to authorized subscribers. Refer to *Creating Sources and Setting Up Sessions* (on page 89).

Before you can define PPV services, the service on which a PPV service is built must be registered with the Service Application Manager (SAM). The SAM is a table that identifies available services and their associated applications. Each time the DNCS registers a service with the SAM, the DNCS assigns it a unique service ID. The DNCS automatically registers the service with the SAM when you create the service, so you do not need to register an event's service with the SAM.

The DNCS and AppServer must be configured for PPV. A PPV Barker Service and PPV Event Service must be provisioned before PPV events can be created. The Barker Service provides previews of events that can be purchased and is a Free-to-Air service. An Event Service provides the actual events that subscribers purchase. This service establishes a connection to the DVB service that is streaming the events. A PPV Barker Service advertises events to be purchased and during the GUI-based creation process is linked to the Event Service. The Event Service carries the PPV Service event content.

This section describes the Set Up PPV Service window and explains how to create, modify, and delete PPV services (the applications that deliver PPV events).

Provisioning the PPV Barker Service

In order to provision (create) a PPV Barker Service, you need to create and define a source for a clear broadcast source using the DNCS Source GUI if the system uses MQAM. Then you need to create and build a digital source definition using the DNCS Source GUI. Refer to *Creating Sources and Setting Up Sessions* (on page 89) for specific procedures.

Note: If your system is configured with the barker service as same as the event service, you do not need to provision the Barker service.

Provisioning the PPV Event Use Service

You must register the PPV Event Service with the SAM Service. The process involves creating a PPV Event Use Service on the DNCS/AppServer. The Event Use Service is the DVB service that will be carrying PPV events. Complete these steps to provision PPV Event Use Service for the DNCS.

1   Create and define a source for secure broadcast using the DNCS Source GUI. Refer to *Creating Sources and Setting Up Sessions* (on page 89) for detailed procedures.

2   Encrypt the source to secure it by creating a Security Mode definition using the DNCS Source GUI. For detailed procedures, refer to *Encrypt a Service* (on page 93).

3   Create and build a digital source definition using the DNCS Source GUI. Refer to *Creating Sources and Setting Up Sessions* (on page 89) for detailed procedures.

4   Your next step is to register the source for event service using the SAM Service GUI. Go to *Registering a Source for Event Service Using the SAM Service GUI* (on page 110).

Registering a Source for Event Service Using the SAM Service GUI

You use the Set Up SAM Service window to register a source for event service.

About the Set Up SAM Service Window

The fields on this window are as follows:

- **Service Name**—A name for the service. Lower Case. (Should be the same as the Event_Short_Name (Billing System) and SI_Service_Name [SI Server])

- **Short Description**—Same as Service Name. Lower Case

- **Long Description**—A longer description that provides a more complete definition of the service

- **Application URL**—Should always be "bfs://resapp/watchtv" for RPPV events

- **Logo**—Should always be 255

- **Parameter**:

  - Number—Should be the Source ID on which the PPV Event Use Service is setup

  - Parameter—String (optional) can be a brief description of the PPV event

Registering the Source for Event Service

After you build a PPV Barker and PPV Event Service, register the source with the SAM. Complete these steps to register the source for event service.

1   On the DNCS Administrative Console, select the **Application Interface Modules** tab. The Application Interface Modules tab appears in front of the other tabs.

2   Click **SAM Service**. The SAM Service List window opens.

3   From the **File** menu, click **New**. The Set Up SAM Service window opens.

4   On the **Set Up SAM Service** window, complete all the following required fields:

- Service Name (Lower Case)
- Short Description (Lower Case)
- Long Description
- Application URL
- Logo
- Parameter: Number
- Parameter: String (optional)

Note: Make sure that the Service Name and Short Description are the same as Event_Short_Name (Billing System) and SI_Service_Name (SI Server).

5   Click **Save**. The SAM register the event service.

6   Your next step is to set up PPV service. Go to *Creating a PPV Service* (on page 115).

Understanding the Set Up PPV Service Window

Use the Set Up PPV Service window to create or modify PPV services.

The fields on this window are as follows:

- **Service Name**—A unique name for the service. This field is case sensitive.

  Note: Service names are typically provided by the billing system and should be the same as the Event_Short_Name (Billing System) and the SI_Service Name (SI-Server).

- **Short Description**—A useful descriptive short name, such as IPPV1 and IPPV2 for subscribers when they tune to the channel where this PPV service resides. This field is case sensitive.

- **Long Description**—A longer description that provides a more complete definition of the service. This is for your benefit only. Subscribers never see the information entered here.

- **Logo Index**—Should always be set to "0" (zero).

- **Default Order Telephone Number**—Specifies the phone number for subscribers to call to order a reservation pay-per-view (RPPV) event advertised by this service.

- **Default Cost** (Optional)—Sets the default cost for events on the service if no cost is specified for the event.

- **Default Order Start Interval** (Optional)—Not available at this time.

- **Event Use Service**—The service that will be seen on this PPV service when PPV events are purchased. Click the arrow to display a list of all services available, and then select the appropriate service from the list.

■ **Subscription Service** (Optional)—Not available at this time.

■ **Interstitial Service** (Optional)—Not available at this time.

Creating a PPV Service

After you have built the services, the next step is to create a service that advertises and sells the events: a PPV service.

1 On the DNCS Administrative Console, select the **Server Applications** tab. The Server Applications tab moves to the forefront, similar to the following example.
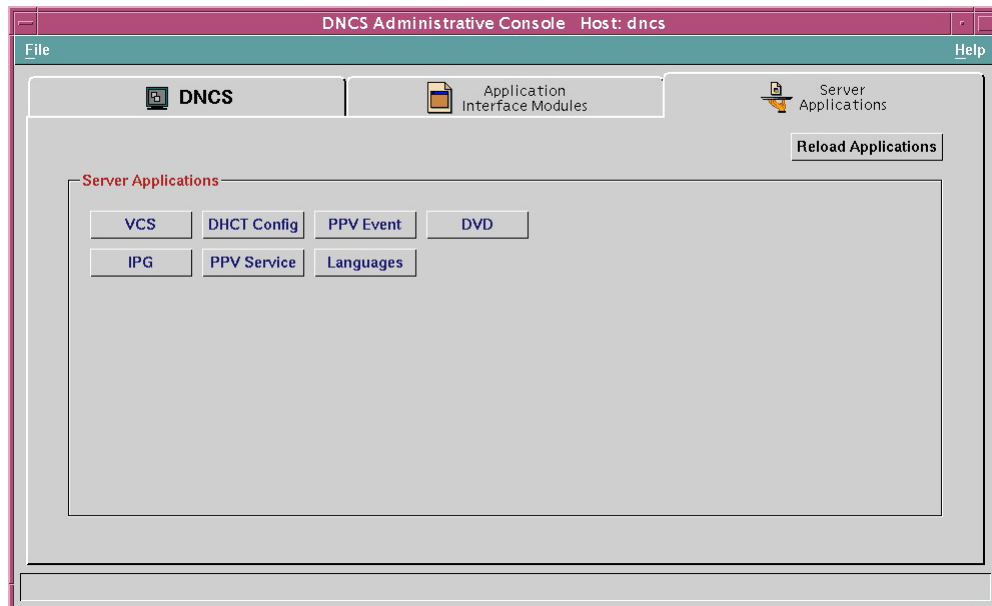
2 Click **PPV Service**. The PPV Service List window opens, similar to the following example.

3   From the **File** menu, click **New**. The Set Up PPV Service window opens, similar to the following example.

4   On the **Set Up PPV Service** window, complete all of the following required fields. Optional fields are labeled.

- Service Name
- Short Description
- Long Description
- Logo Index (Optional)
- Default Order Telephone Number
- Default Cost (Optional)
- Default Order Start Interval (Optional)
- Event Use Service
- Subscription Service (Optional)
- Interstitial Service (Optional)

Notes:

- See *Understanding the Set Up PPV Service Window* (on page 112) for descriptions of these fields.
- Be sure to make a note of the values in the Short Description field and the Event Use Service field. You will need these values when you set up this PPV service on the EPG in the SI-Server billing system.

5 Click **Save**. The Application Server creates a PPV service for the source and automatically does the following:

- Registers the service with the SAM

- Assigns a URL of ippv to the service

- Creates an unlimited segment from the service, which you can view in the Segment List

Note: At this point, you have created both the PPV service and the Event Use service, and you have linked the two services to each other.
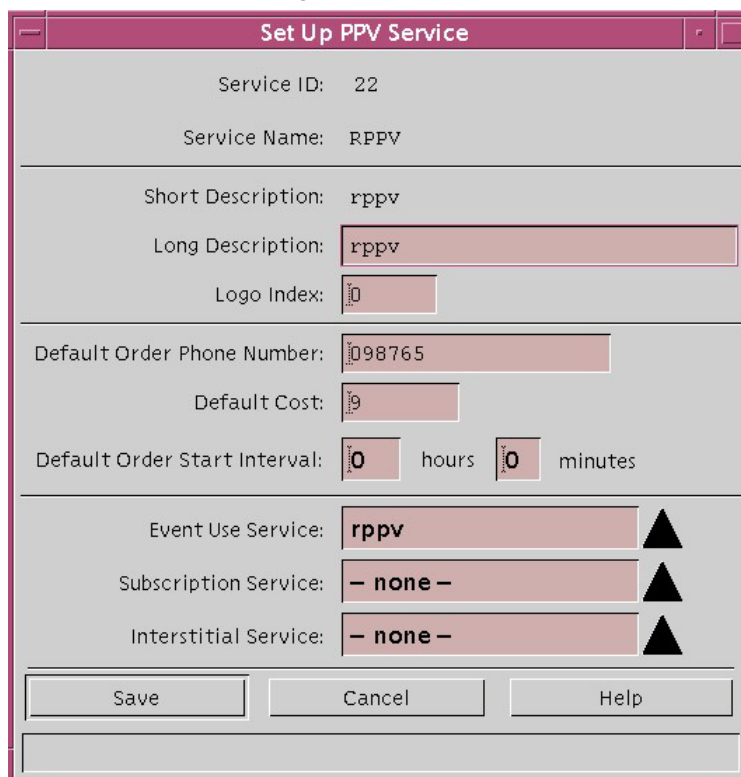
6 Do you want to add another PPV service?

- If **yes**, go back to step 3 and add the next service.

- If **no**, go to step 7.

7 Your next step is to configure the SI-Server for the PPV services (barker and events). Configure the SI tables using the documentation provided with the SI-Server.

Modifying PPV Services

1 On the PPV Service List window, highlight the row of the desired service, similar to the following example.
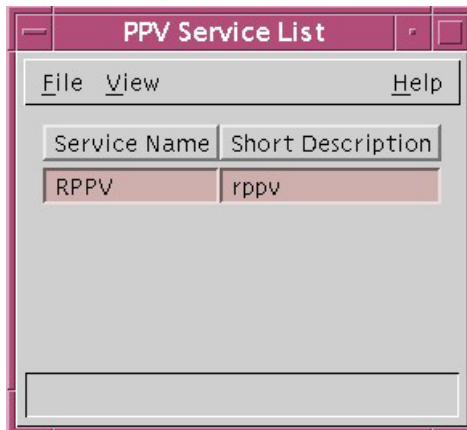
2   Click the **File** menu and select **Open**. The Set Up PPV Service window opens, similar to the following example.

3   Make necessary changes in the fields, and click **Save**.

Deleting a PPV Service

Important: The system will not allow you to delete a service if events also use the service.

1   Select the service you want to delete in the PPV Service list window.

2   Click the **File** menu and select **Delete**. A Question window opens, prompting you to confirm that you want to delete the current item.

3   Click **Yes** to confirm that you want to delete the PPV service.

Understanding PPV Events

This section describes how to define the following types of events as defined by the billing system:

- **RPPV event**-Subscribers can purchase a PPV event by placing a telephone call/SMS. A cable service representative (or an automated service) may order the event for the subscriber.

- **IPPV event**-Subscribers can purchase an IPPV event by using the DHCT remote control.

Generating PPV Events

Typically, the billing system defines PPV events automatically. However, a solid understanding of how the billing system defines PPV events makes it easier for you to correct any errors that may occur.

Configuring the Application Server for PPV

1   Log on to Application Server as **dncs** user.

2   Create a file named ".netrc" in the /export/home/dncs directory.

3   Add the following in the .netrc file and **Save**.

- Name of the machine <si server name>

- Login information (si server username having ftp permission>

- Password <password for the user>

4   Change the permission of the .netrc file to **Read Only** using the "chmod 400 .netrc" command.

Configuring the SI-Server for PPV

1   Create the PPV BAT for each PPV service and import each BAT to all the SCS/MUX devices. For detailed instructions, refer the *SI-Server Complete SI Solution User Manual* (part number V599525_V00).

2   Configure the EPG automatic import and export task. For detailed instructions, refer the *SI-Server Complete SI Solution User Manual* (part number V599525_V00).

3   Configure SI table for PPV service. For detailed instructions, refer the *SI-Server Complete SI Solution User Manual* (part number V599525_V00).

Configuring the Billing System for PPV

The billing system generates PPV events as follows:

1   The billing system sends event definition to the Application Server.

2   The Application Server processes the definition and sends it to the DNCS for packaging.

3   The DNCS creates a package for the event and assigns the package an EID.

8

Configuring the Broadcast File System

Introduction

The Broadcast File System (BFS) provides a mechanism for standardized downloads of applications, games, images, and other data formats required by applications. The objective of using BFS is to allow the transfer of broadcast data to the target platform such as a set-top. Broadcast data can be any sort of data object desired by an application on the target platform including binary files such as applications or images, games, text files, or other formats. The BFS will take these data objects and broadcast the data on a broadband carousel to the target platform. The *carousel* is simply an elementary data stream that is continually playing out these data objects over and over. The target platform will be able to extract the desired data object from the broadband carousel and perform operations on the data object as defined by the software application

This chapter provides steps for configuring the BFS to support applications on set-tops.

In This Chapter

Set Up the BFS In-Band Source

To send in-band data to the DNCS, you must set up a corresponding source. For setting up a video source, you can use the Source user interface on the DNCS. To send out-of-band data in band, you must set up the source using the BFS Admin user interface.

To set up the BFS in-band source, complete the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Application Interface Modules** tab.

2 Click **BFS Admin**. The BFS Admin Sites window opens.

3 Is there only one site in the headend?

- If **yes**, go to step 5.

- If **no**, go to step 4.

4 If there is more than one site in the headend, select **File** and **All Sites**. The BFS Admin user interface for all sites opens. Go to step 6.

5 If there is only one site in the headend, select the available site. The BFS Admin user interface for that site opens. Go to step 6.

6 Click **Sources**. A list of the available sources opens.

7   Select **File** and **New**. The Set Up BFS Source window opens.

8   In the **Source Name** field, enter the name of the game or GoDB application. For example, enter **Games**.

9   In the **Source ID** field enter **202**.

10   For **Source Type**, select BFS.

11   For the **Transport Type,** select **ASI In-band**.

12   For the **Data Rate**, enter **1 Mbps** (the default value).

13   For **Block Size**, enter **1024** bytes.

14   From the **Available Hosts** column, select a host and move it to the Selected Hosts column.

15   Click **Save**.

16   Repeat steps 7 through 15 for each new in-band source you need to set up.

Set Up the BFS Out-of-Band Source

To send out-of-band data to the DNCS, you must establish an OOB carousel by setting up an out-of-band source.

To set up the BFS out-of-band source, complete the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Application Interface Modules** tab.
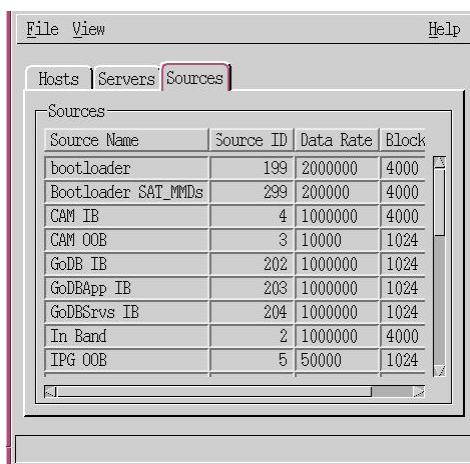
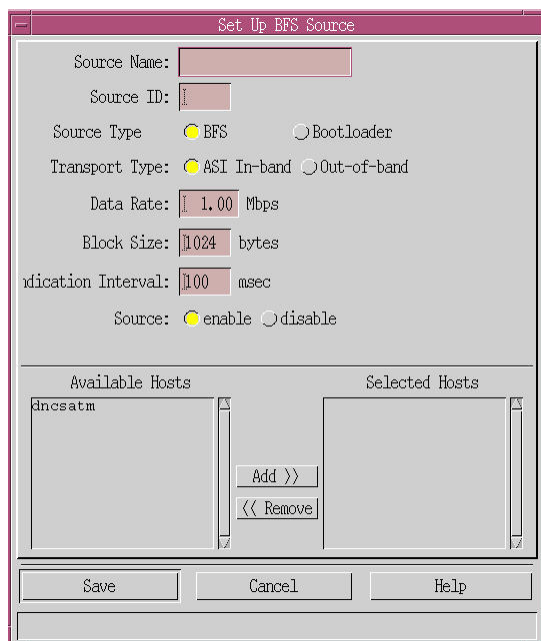

2 Click **BFS Admin**. The BFS Admin Sites window opens.

3 Is there only one site in the headend?

   ■ If **yes**, go to step 5.

   ■ If **no**, go to step 4.

4 If there is more than one site in the headend, select **File** and **All Sites**. The BFS Admin user interface for all sites opens. Go to step 6.

5 If there is only one site in the headend, select the available site. The BFS Admin user interface for that site opens. Go to step 6.

6 Click **Sources**. A list of the available sources opens.

7 Select **File** and **New**. The Set Up BFS Source window opens.

8 In the **Source Name** field, enter the name of the game or GoDB application. For example, enter **Games OOB**.

9 In the **Source ID** field enter **201**.

10 For the **Transport Type**, select **ASI Out-of-band**.

11 For the **Data Rate**, enter **0.01 Mbps**.

12 From the **Available Hosts** column, select a host and move it to the Selected Hosts column.

13 Click **Save**.

14 Repeat steps 7 through 13 for each out-of-band source you want to set up.

Set Up the BFS Server

To play out the carousels continuously in the DNCS, you must set up a BFS server. To set up a BFS server, complete the following steps.

1   On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Application Interface Modules** tab.

2   Click **BFS Admin**. The BFS Admin Sites window opens.
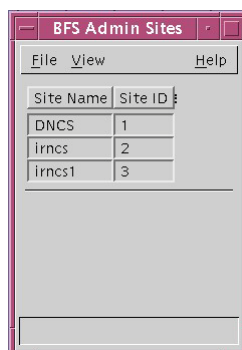
3   Is there only one site in the headend?

■   If **yes**, go to step 5.

■   If **no**, go to step 4.

4 If there is more than one site in the headend, select **File** and **All Sites**. The BFS Admin user interface for all sites opens. Go to step 6.

5 If there is only one site in the headend, select the available site. The BFS Admin user interface for that site opens. Go to step 6.
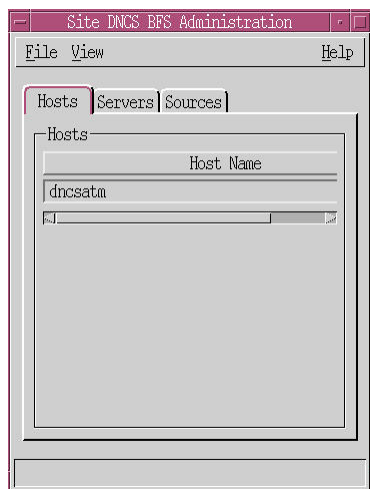
6 Click **Servers**. A list of the available servers opens.
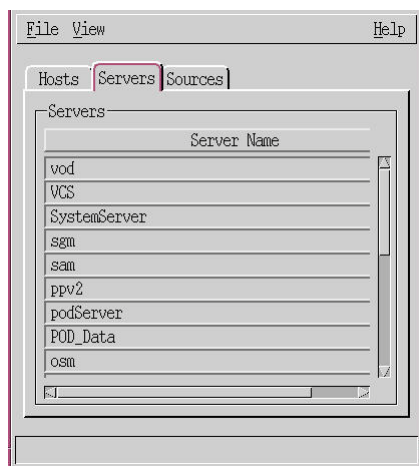
7 Select **File** and **New**. The Authorize BFS Server window opens.
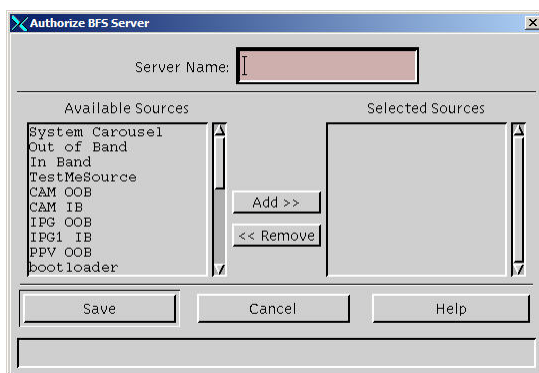
8 In the **Server Name** field, enter **Games**.

9 From the **Available Sources** column, select a source and move it to the Selected Sources column.

10 Click **Save**.

Configure PAT Entries

To configure the PAT entries, complete the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Application Interface Modules** tab.

2 Click **BFS Admin**. The BFS Admin Sites window opens.
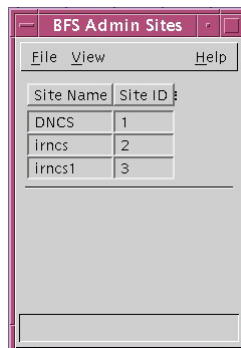
3 Is there only one site in the headend?

- If **yes**, go to step 5.

- If **no**, go to step 4.

4   If there is more than one site in the headend, select **File** and **All Sites**. The BFS Admin user interface for all sites opens. Go to step 6.

5   If there is only one site in the headend, select the available site. The BFS Admin user interface for that site opens. Go to step 6.
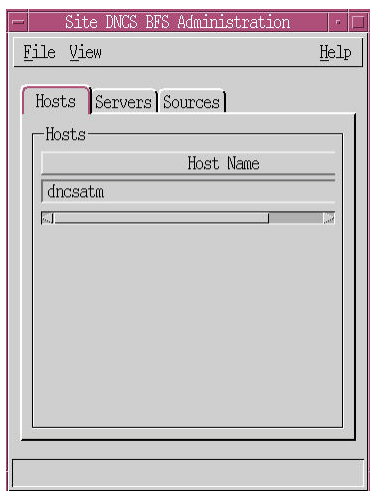
6   Click the **Hosts** tab.

7 Double-click **dncsatm**. The Set Up BFS Host window opens.

8 Click **PAT Configuration**. The Inband Data PAT window opens.

9 If there is an entry created for the ASI in-band source ID, select the entry and click **Delete Entry**. Otherwise, proceed to step 10.

10 Click **New Entry**. The BIG PAT Setup window opens.

11 In the **Session MAC Address** field, enter **00:00:00:00:00:00**.

12 In the **Session Number** field, enter **202**.

13 In the **Program Number** field, enter **2002**.

14 In the **PMT PID** field, enter **304**.

15 Click **Save**.

Configure the Multiple Download Setup

For the Satellite/MMDS network, you will use a different BFS session. For this configuration, you should configure a new BFS source and session in the headend for the bootloader.

To configure multiple download setup, complete the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Application Interface Modules** tab.
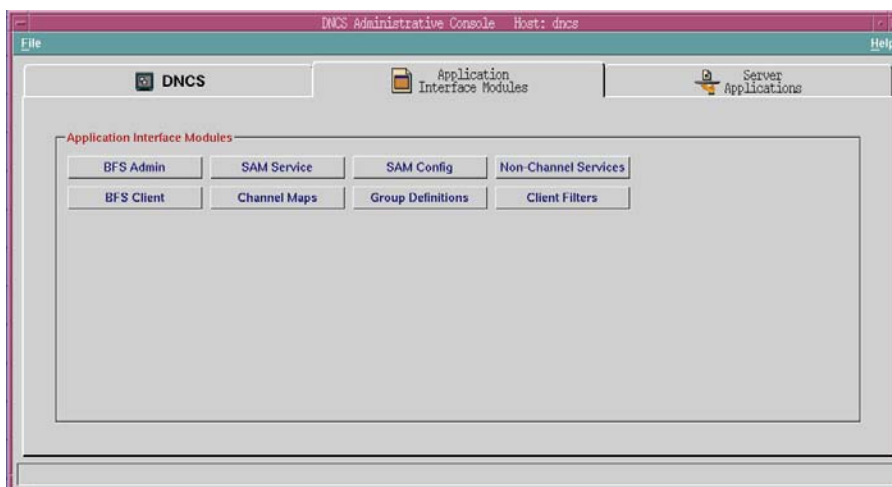
2 Click **BFS Admin**. The BFS Admin Sites window opens.
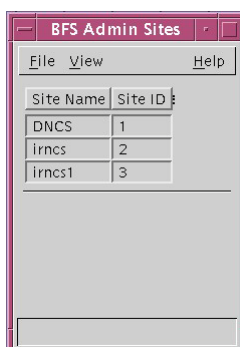
3 Select the site you want to use and click **File** and **Select**. The Site DNCS BFS Administration window opens.
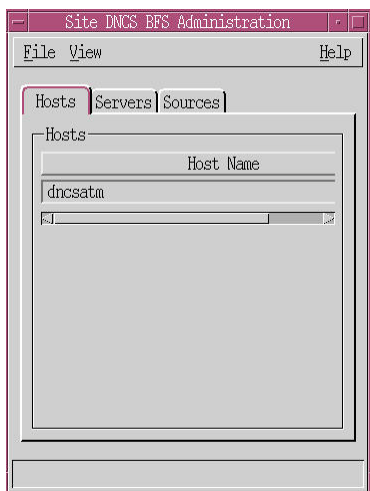
4 Click **Sources**. A list of the available sources opens.

5   Select **File** and **New**. The Set Up BFS Source window opens.

6   Complete the fields on the Set UP BFS Source window as follows:

■   In the **Source Name** field, enter the name of the bootloader. For example, enter **Bootloader_for_Sat**.

■   In the **Source ID** field enter **203**.

■   For the **Source Type**, enter **Bootloader**.

■   For the **Transport Type,** select **ASI In-band**.

■   For the **Data Rate**, enter **0.20** Mbps.

■   For the **Block Size**, enter **4000** bytes.

■   For the **Indication Interval**, enter **100** msec.

■   For **Source**, click **Enable**.

■   From the **Available Hosts** column, select **dncsatm**.

7   Click **Save**.

8 Click **Servers**. A list of the available servers opens.
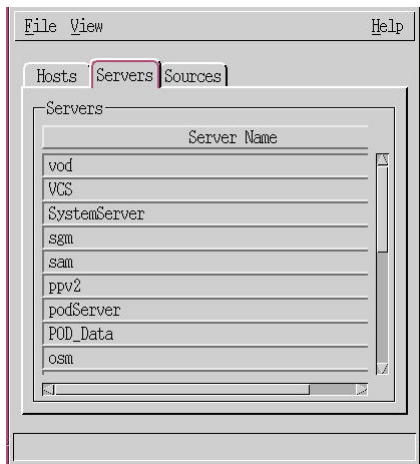
9 Double-click on the bootloader server. The Authorize BFS Server window opens.
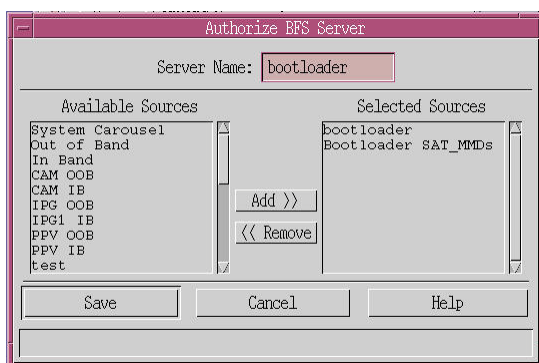
10 From the list of available sources, click the source you created for the bootloader (Bootloader_for_Sat in our example), and click **Add** to move it to the Selected Sources column.

11 Click **Save**.

12 Click **Hosts** and select **dncsatm**.

13 Click **File** and **Open**. The Set Up BFS Host window opens.

14 Click **PAT Configuration**. The Inband Data PAT window opens.

15 Do any of the numbers listed in the Session Number column match the source ID that you added in step 6?

■ If **yes**, select that row and click **Open**. The BIG PAT Setup window opens. Go to step 16.

■ If **no**, go to step 18.

16 Complete the fields as follows:

■ For **Program Number**, enter **200**.

■ For **PMT PID**, enter **304**.

17 Click **Save**.

18 Click **New Entry**, and complete the fields as follows:

- For **Session Number**, enter the source ID you entered in step 6.

- For the **Program Number**, enter **2001**.

- For the **PMT PID**, enter **304**.

19 Click **Save**.

20 Make sure the session details that correspond to the new bootloader source you built are available in the active state as shown in this graphic.

9

Authorizing Features for Set-Tops

Introduction

Feature authorization (also known as named entitlement) allows you to enable or disable specific set-top features from the DNCS. For example, you can enable or disable the games feature for a set-top from the DNCS.

The Named Entitlements feature serves the following purposes:

- Defines the mapping between a named feature, such as DVR, and an EID

- Provides a mechanism for a client application to determine whether the set-top has been authorized for the feature

- Enables an application to refer to a feature by a well-known entitlement name and by a system-specific EID

This chapter provides procedures for configuring feature authorization.

In This Chapter

Creating Named Entitlements

Named entitlements enable you to refer to a feature by a well-known name as well as by a system-specific EID. You can easily identify the feature when it has an easily recognized name.

To create named entitlements, complete the following steps.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

2 Click **Package**. The Package List window opens.

3 Click **File** and **Manage Feature**. The Named Entitlement List opens.
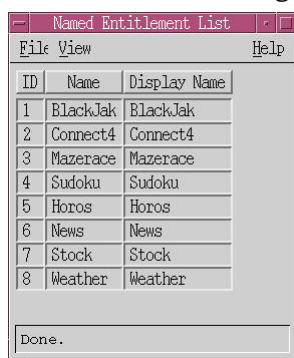
4 Click **File** and **New**. The Set Up Named Entitlement window opens.
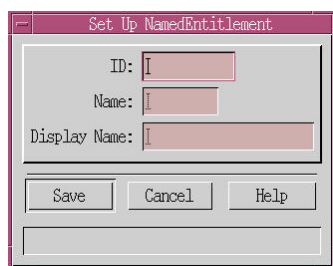
5 Enter values for the ID, Name, and Display Name fields. The ID must be numeric and up to 10 characters.

Note: The feature name should be exactly the same name as the feature. For example, for a game of BlackJak, the feature name should be BlackJak.

6 Click **Save** to add the named entitlement.

Editing Named Entitlements

To edit the display name for a named entitlement, complete the following steps.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

2 Click **Package**. The Package List window opens.

3 Click **File** and **Manage Feature**. The Named Entitlement List window opens.
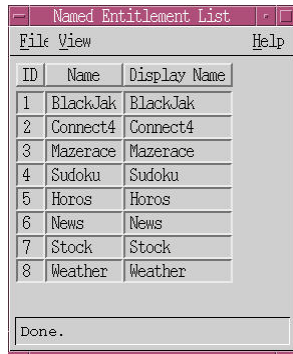
4 Select the entitlement you want to edit and click **File** and **Open**. The Set Up Named Entitlement window opens.
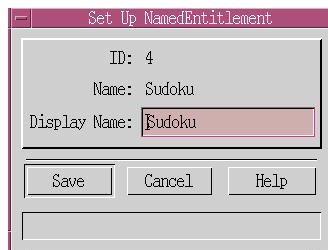
5 In the **Display Name** field, enter the new name for the entitlement.

6 Click **Save** to save your changes.

Deleting a Named Entitlement

To delete a named entitlement, complete the following steps.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

2 Click **Package**. The Package List window opens.

3 Click **File** and **Manage Feature**. The Named Entitlement List opens.
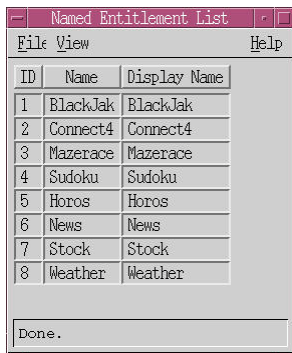
4 Select the entitlement you want to delete and click **File** and **Delete**. The system prompts you whether you want to delete the entitlement.

5 Click **Yes** to delete the named entitlement.

Assigning Named Entitlement Features

To assign named entitlement features to packages, complete the following steps.

1   From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

2   Click **Package**. The Package List window opens.

3   Select a package from the list for which you want to assign the feature and click **File** and **Assign Feature**. The Assign Feature window opens.
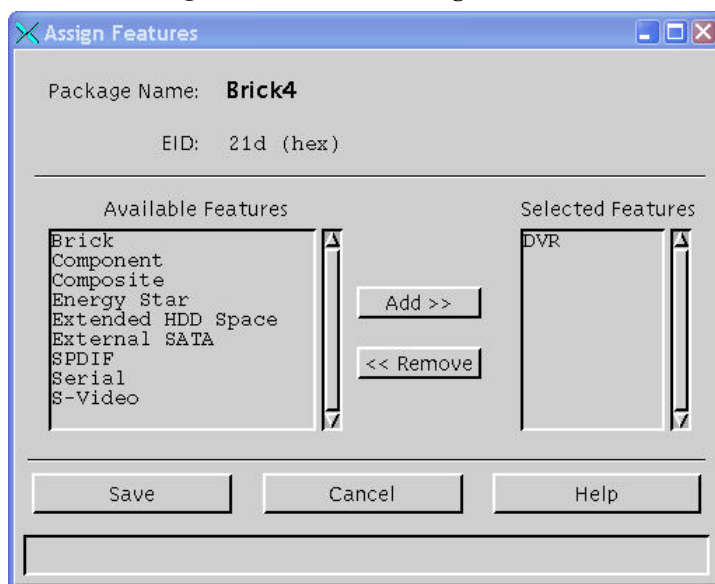
4   From the Available Features list, select one or more features you want to add to this package and click **Add**. These features are moved to the Selected Features list.

5   Click **Save** to assign these features to this package.

Removing Assigned Features from Packages

To remove an assigned feature from a package, complete the following steps.

1 From the DNCS Administrative Console, click the **DNCS** tab, and then click the **System Provisioning** tab.

2 Click **Package**. The Package List window opens.

3 Select a package from the list for which you want to assign the feature and click **File** and **Assign Feature**. The Assign Feature window opens.
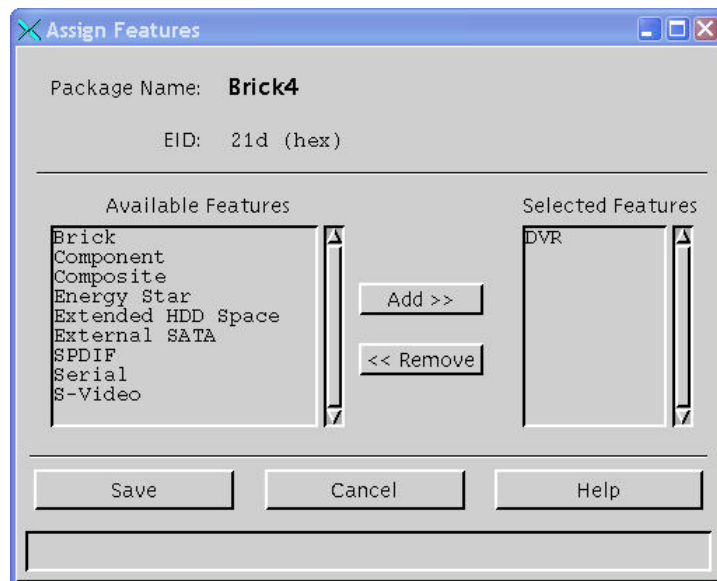
4 From the Available Features list, select one or more of the named entitlements shown in the Available Features list that you want to unassign for the package and click **Remove**.

Note: Before deleting the package, all the associated features should be removed from the package.

5 Click **Save** to removes these features from this package.

Extracting EIDs and Associated Source IDs

You can use the eutdump utility to extract the EIDs and associated source IDs from the system to help you debug the system. You can use this utility to identify what package contains the source and to check whether the system is sending the entitlement unit table (EUT) correctly.

Run the eutdump utility with the "eut" file as the input. Type the following command to run the utility:

/dvs/dncs/bin/eutdump /dvs/dvsFiles/CAM/eut

From the output, you can determine the following:

- Section type ' Named Entitlement will have all the details of the package which has a named entitlement association.

- An EID with the name of the named entitlement will be present in the Section type

- If the Named entitlement feature is disabled, eutdump output will not contain "Named Entitlement" section type.

10

Configuring Multiple Bootloader Carousels

Introduction

The Broadcast File System (BFS) has been enhanced to support more than one bootloader carousel. With multiple bootloader carousels, the BFS can send set-top module software version images using more than one carousel. This enhancement allows operators to reduce download times by splitting a set of images among multiple carousels and to design the data rate based on the DHCT type and network bandwidth availability.

In This Chapter

Setting Up a New Carousel

Default carousels are configured during the installation process. If you want to add a new bootloader carousel or multiple carousels, complete the following steps.

Important: The maximum rate for a carousel is 1 Mbps. If you are setting up multiple carousels, keep these points in mind:

■ The cumulative data rate for all out-of-band (OOB) bootloader carousels should not exceed 1 Mbps.

■ You should strive to keep the number of carousels to a minimum. Only add additional carousels if they provide a significant advantage to the download process.

1 From the DNCS Administrative Console, click the **Application Interface Modules** tab.

2 Click **BFS Admin**. The BFS Admin Sites window opens.

3 Click **File** and then select **All Sites**. The Site AllSites BFS Administration window opens.

4 On the Site AllSites BFS Administration window, click the **Sources** tab. The Sources tab moves to the forefront.

5 Click **File** and then select **New**. The Set Up BFS Source window opens.

6 In the Set Up BFS Source window, fill in the fields according to your naming convention making sure that the Source Type is set to **Bootloader** and the **Transport Type** is set to **ASI In-Band.**

7 Click **Save**. The new source is added to the Site AllSites BFS Administration window on the RF Sources tab.

8 On the Site AllSites BFS Administration window, click the **Servers** tab. The Servers tab moves to the forefront.

9 Click **File** and then select **New**. The Authorize BFS Server window opens.

10 Fill in the **Server Name** in the Server Name field.

11 From the Available Sources column, select the new source that you created in steps 5 and 6 of this procedure.

12 Add the new source to the Selected Sources field.

13 Click **Save**. The new server appears in the Server Name list on the Site AllSites BFS Administration window.

14 Do you need to add multiple carousels?

   – If **yes**, repeat steps 5 through 13.

   – If **no**, close the BFS Administration AllSites window.

15 The new carousel will now appear in the Carousel area on the Set Up DHCT Download window from the DHCT Downloads tab on the Image List window.

11 Chapter 11

Monitoring the System Remotely

Introduction

To get the attention of the system operator quickly whenever any of the DNCS processes stop, a remote machine attached to the DNCS can generate a noise (or alarm) that allows the operator to detect the condition.

Requirements

The remote alarm configuration requires the following:

- A remote machine that has a sound card installed.

- Internet Explorer must be installed on the remote machine.

- The IP address for the remote machine must have access to web services. This access must be configured in the following file: /usr/local/apache/conf/httpd.conf

- The Apache server and Tomcat must be running in DNCS.

- The Apache server must run with the updated configuration. After updating the httpd.conf file, you must restart the Apache server.

This chapter provides the information you need for configuring your system so that you can monitor it from a remote machine.

In This Chapter

Configuring the DNCS for Remote Monitoring

To use the remote alarm feature of the DNCS, the following environment variable must added to the .profile file using this command:

export DNCSINIT_IPADDR=[*IP address of DNCS***]**

Allowing Access to a Remote Machine

To allow access to a remote machine, complete the following steps.

1 Use an editor such as vi to open the httpd.conf file.

2 Search for the following string in the file: "<Location/>".

3 Add the following line within the "Location" section:

Allow from <ip-address of the remote machine>

Example: Allow from 64.103.160.155

Restarting the Apache Server

The Apache server must run with the updated configuration. After updating the httpd.conf file, you must restart the Apache server.

To restart the Apache server, you must run the following commands in the order shown:

svcadm disable svc:/network/http:apache2

svcadm enable svc:/network/http:apache2

Viewing System Alarms

To view alarms, complete the following steps:

1 Start the Apache server.

2 Start the DNCS.

3 Enter the following URL on the remote machine to display a web page of any inactive processes and to see a log of the status for each process:

http://[IP address of the DNCS]:8045/alarm/dncsStatus.html

12 Chapter 12

Configuring State Administration of Radio, Film, and Television (SARFT)

Introduction

SR i4.2.2 supports SARFT. SARFT is a Chinese government regulatory authority and stands for State Administration of Radio, Film, and TV. SARFT has access to all Cable companies and runs periodic tests to see if the cable providers are complying with the regulatory requirements. SR i4.2.2 allows the DNCS to generate the SARFT report for the configured number of days.

In This Chapter

Enabling SARFT

Complete the following steps to enable the SARFT feature on the DNCS.

1   Log in to the DNCS as dncs user.

2   Open an xterm window.

3   Enter the following command:

updatehctOperlog.sh

4   At the prompt for enabling caching, enter **1**.

5   At the prompt, enter the number or days to cache. For example, enter **30**. The system will generate a report showing 30 days of information. Wait for the report to complete. The report process could take up to an hour.

Note: If you need to change the number of days to cache the information, repeat steps 1 through 5 and enter the number of days you want to cache the information.

6   At the end of the report generation process, the system asks for the DNCS password for adding the Crontab entry for the SARFT report generation schedule. Enter **dncs** for the password.

Enabling External Access to the SARFT Report

To enable external access to the SARFT report, complete the following steps.

1   Open an xterm window on the DNCS.

2   Type **su** and enter the root password.

3   Enter the following command:

/etc/apache2

4   Enter the following command to stop the httpd process:

svcadm disable svc:/network/http:apache2

5   Enter the following command to find the location of the http configuration file:

vi httpd.conf

6   Go to the location indicated in step 5 and enter the following command:

Allow from [IP address of the external machine]

Example: Allow from 192.168.100.1

7   Save the changes and exit the http.conf file.

8   Start httpd using the following command:

svcadm enable svc:/network/http:apache2

Accessing the SARFT Report from an External System

If the feature is enabled, you can access the SARFT report from an external system using the following access link on the external system:

http://[IP address of the DNCS]:[http_port]/casbuffer

SARFT Files and Directories

To help you manage your SARFT reports, the following directory structure and file format are used for SARFT reports:

- All SARFT related files are located in this directory:
  /dvs/dncs/SARFT_DATA_DOCS

- The SARFT reports template can be configured using the following file:
  sarft_cfg.xml

- All the reports's XSD are available under the SARFT directory for reference.

- Backups of reports are stored in this directory:
  /dvs/dncs/SARFT_DATA_DOCS/backup

  Note: Reports that are older than the number of days you configured your system to cache them are stored in this backup directory.

Report Backup Process

The system backs up reports using the following process.

1 The SARFT feature is enabled with caching. For example, the feature is enabled on 04/01/2009 and you choose 30 days for caching (caching is also known as OPER_DAYS).

2 A cron entry setting will run the SARFT report every day at the specified time (00:00 hrs). For this example, at 00:00 hours on 04/02/09 the following reports are generated:

- ICCardReport
- ProductListReport
- EntitlementReport
- StaticsReport

3 Generated XML files are kept in the following directory with a **20090401** prefix:

   /dvs/dncs/SARFT_DATA_DOCS.XML Files

4 This same process continues daily until the feature is disabled. When the 31st day occurs (05/01/2009 in our example), the /dvs/dncs/SARFT_DATA_DOCS directory will contain reports from 04/01/2009 to 04/30/2009. After the report for 05/01/2009 is generated, the report files for 04/01/2009 are moved to the backup directory. The entitlement report and the ICCard report for 04/02/2009 are generated again to hold the data from the database for generating the SARFT report.

13

Chapter 13

Configuring the System for Satellite and Terrestrial Support

Introduction

To configure your system for satellite and terrestrial support, you must complete the following tasks:

- Enable Satellite and MMDS Feature. For more information see *Enable PowerKEY DVB Features and Licenses* (on page 17).

- Enable Network Binding Feature. For more information see *Enable PowerKEY DVB Features and Licenses* (on page 17).

- Configure Satellite Hubs. For more information see *Configure the Satellite Hub* (on page 164).

- Stage Satellite Set-Tops. For more information see *Stage Satellite Set-Tops* (on page 166).

- Model a Satellite Transport. For more information see *Model a Satellite Transport* (on page 169)

- Provision a Cable SCS and MPEG Source for Satellite and Terrestrial Transport. For more information see *Provision a Cable SCS and MPEG Source for Satellite and Terrestrial Transport* (on page 172).

In This Chapter

Configure the Satellite Hub

To configure the satellite hub, complete the following steps.

1 From the DNCS administrative console, check the status of the DNCS to ensure that all processes are running.

2 On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.
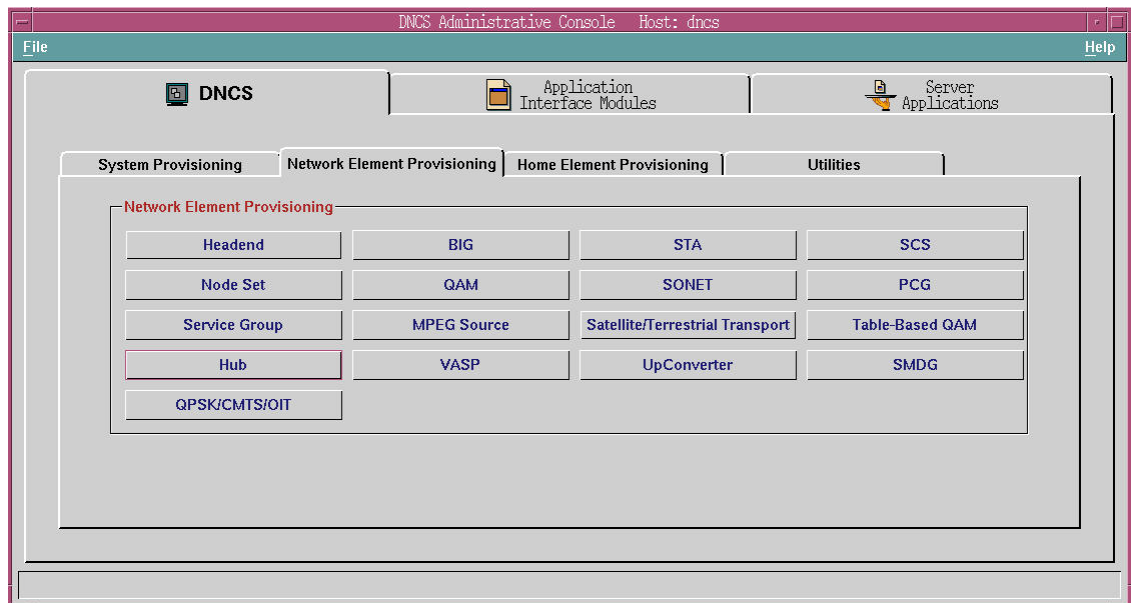
3 Make sure the Satellite/Terrestrial Transport option is enabled as indicated by the Satellite/Terrestrial Transport button appearing as shown in step 2.

4 Click **Hub**. The Hub Summary screen opens.

5 Make sure the network binding option is enabled as indicated by the N/W Binding Pkg column in the screen for step 3.

6 Click **Add Hub**. The screen populates with a new row for the hub you are adding.

7 In the **Hub Name** field, enter the name for the satellite hub you are adding.

8 From the **Transport Type** drop-down list, select **Satellite**.

9 Is the Network Binding option enabled?

- If **yes**, go to step 10.

- If **no**, go to step 11.

10 From the **N/W Binding Pkg** drop-down list, select a package from the list to be associated with this hub.

11 Click **Save** to save the hub details.

12 Repeat steps 6 through 11 for each hub you want to configure for satellite.

Stage Satellite Set-Tops

To stage satellite set-tops, complete the following steps.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Home Element Provisioning** tab.

3 Click **DHCT**. The DHCT Provisioning window opens.
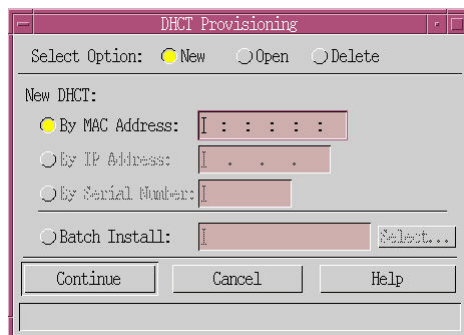
4 Click **New**.

5 Click **Batch Install** and then click **Select**. The Batch Data Directory Selection window opens.
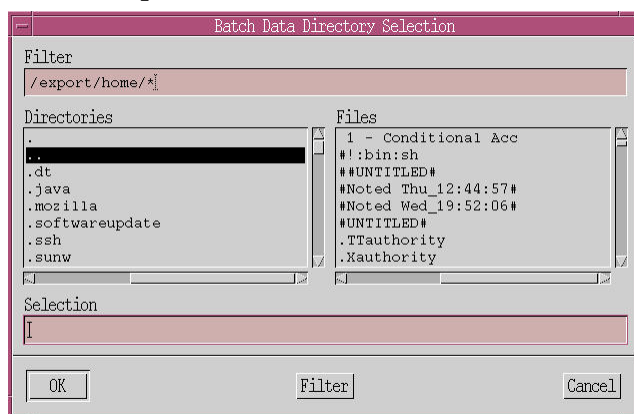
6 Select the directory that contains the TOC file and click **OK**. The Batch Install field populates with the directory path for the TOC files.

7 Click **Continue**. The Batch Install Progress window opens. This window shows a breakdown of the data to be loaded during a batch installation.
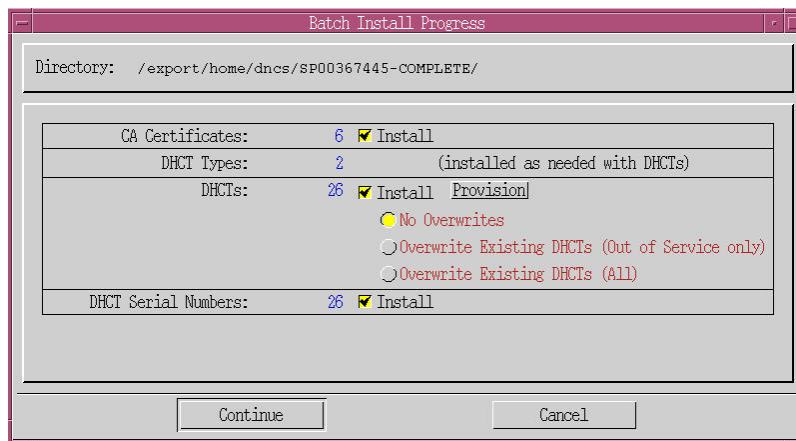
8 Click **Provision** to apply the provision template to all set-tops. The Set Up DHCT window opens.
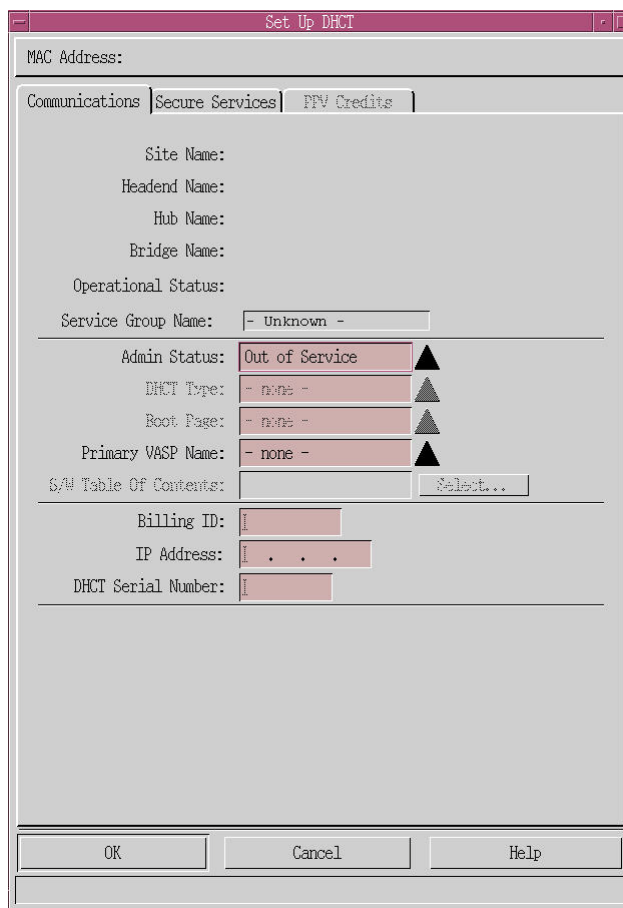
9 Select the **Communications** tab.

10 From the **Admin Status** drop-down list, select **In Service One Way**.

11 Select the **Secure Services** tab. Any entry on this screen causes the PowerKEY staging EMMs to be created for each set-top in the batch. Any package that is selected will be applied to all set-tops in the batch and authorize them for the package.
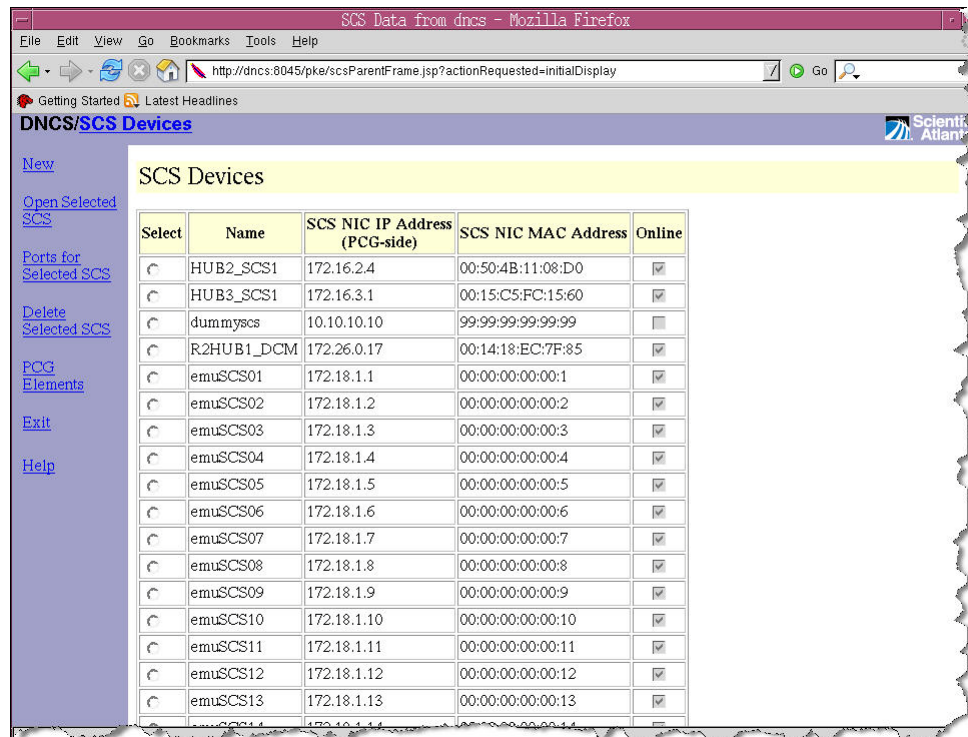
12 Make sure that both DMS Enable and DIS Enable are selected.

13 Click **OK**. The Batch Install Progress window opens.

14 Click **Continue**. The Batch Installation process loads the set-top data and public keys into the DNCS database. This process may take a few minutes.

Model a Satellite Transport

To model a satellite transport, you must provision a cable Simulcrypt Synchronizer (SCS) if one is not already available. Complete the following steps to model a satellite transport.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Network Element Provisioning** tab.

3 Click **SCS**. The SCS Devices window opens.

4 Click **New**. The New SCS Device window opens.

5 In the **Name** field, enter the name for the SCS.

6 In the **IP Address** field, enter the IP address for the SCS device.

7 In the **MAC Address** field, enter the MAC address of the SCS device.

8 In the **ID** field, enter the ID of the device.

9 Click the check box for the **Online** field to make the SCS active.

10 Select the PCG from the **Primary PCG** drop-down menu.

11 Select the Headend from the **Headend** drop-down menu.

12 In the **Max Sessions** field, enter the maximum number of sessions this device is allowed to build.

13 Click **Save**.

14 After the SCS saved successfully, select the SCS and click **Ports** to view the ports for the selected SCS option.

15 Select a port from the SCS Devices screen and click **Ports for Selected SCS**.

16 Click **Add Input Port** and complete the screen.

17 Click **Add Output Port** and complete the screen.

18 Click **Exit** to return to the administrative console.

19 Create an MPEG source for this SCS port. See *Set Up MPEG Sources* (on page 39) for details.

20 Make sure the MPEG source for the SCS appears in the list of sources.

21 From the **Network Element Provisioning** tab, click **Satellite/Terrestrial Transport**. The Satellite Transport Parameters window opens.

22 Click **Add New** to add a row to the screen.

23 Complete the fields as follows:

- **TS ID**. Enter the ID for the transport stream.

- **Download Frequency**. Enter the frequency to use for the download.

- **Symbol Rate**. Enter enter the symbol rate

- **Polarization**. From the drop-down list, select the polarization method.

- **Modulation**. From the drop-down list, select the modulation type.

- **Hub ID**. From the drop-down list, select the Hub ID.

- **Cable TS ID**. Enter the ID for the cable transport stream.

  Important: The TS ID for the satellite transport must be unique for the DNCS and not conflict with the TS IDs of either QAM or SCS devices.

- **Home TS**. Check this box if it is the home transport stream.

24 Click **Save**.

Provision a Cable SCS and MPEG Source for Satellite and Terrestrial Transport

For each satellite and terrestrial transport, you must provision a cable Simulcrypt Synchronizer (SCS) and MPEG source. Complete the following steps to provision the sources.

1   On the DNCS Administrative Console, click the **DNCS** tab.

2   Click the **Network Element Provisioning** tab.

3   Click **Satellite/Terrestrial Transport**. The Satellite Transport Parameters window opens.

4   Click **Add New** to add a row to the screen.

5   Complete the fields as follows:

- **TS ID**. Enter the ID for the satellite transport stream.

    Important: The TS ID for the satellite transport must be unique across the DNCS and it should not be the same as any TS ID of either the QAM or SCS devices that are configured.

- **Download Frequency**. Enter the frequency to use for the satellite download.

- **Symbol Rate**. Enter enter the symbol rate for the satellite transport in symbols per second.

- **Polarization**. From the drop-down list, select the polarization method.

- **Modulation**. From the drop-down list, select the modulation type.

- **Hub ID**. From the drop-down list, select the satellite hub ID.

- **Cable TS ID**. Enter the ID for the cable transport stream modeled using the SCS identified earlier.

    Important: The TS ID for the MMDS transport must be unique for the DNCS and not conflict with the TS IDs of either QAM or SCS devices.

- **Home TS**. Check this box if it is the home transport stream. You must check this box if the UNConfigIndication for the satellite hub needs to carry satellite tuning parameters.

6   Click **Save**.

14

Messaging

Introduction

The Messaging feature for the PowerKEY DVB System allows you to communicate with your subscribers using messages that can be targeted to your subscribers' DHCTs. These messages can carry information relating to various topics, including, but not limited to:

- Accounting alerts

- Service outages

- Promotional offers

- Emergency alerts

Messages can be addressed according to, but not limited to, the following scenarios:

- Specific DHCTs

- A group of DHCTs

- All DHCTs

- All DHCTs in a hub

- All DHCTs belonging to a site

This chapter provides procedures for configuring the Messaging feature on your PowerKEY DVB DNCS.

Important: Messages will be activated and sent primarily from the billing system. Refer to your Billing Operation Support System (BOSS) documentation and your Business Applications Support System (BASS) documentation for additional procedures for configuring messaging on the billing system.

In This Chapter

Configure Messaging

This section describes the various user interfaces relating to the Messaging feature, and explains how to use these interfaces to create, modify, and delete messages on your PowerKEY DVB System.

Important: The procedures described in this section are performed using the various DNCS Messaging user interface screens. Refer to your BOSS and your BASS documentation for additional procedures for configuring messages on the billing system.

Create a Message Configuration

1   On the DNCS Administrative Console, choose the **System Provisioning** tab. A window similar to the following window opens.
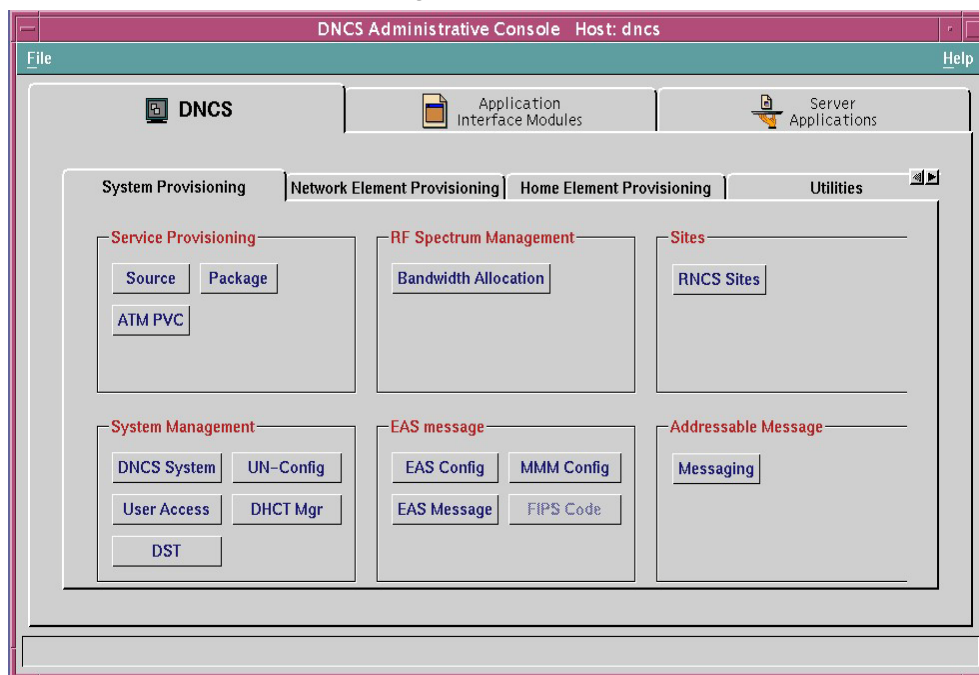
2   Click **Messaging**. The Message List window opens.
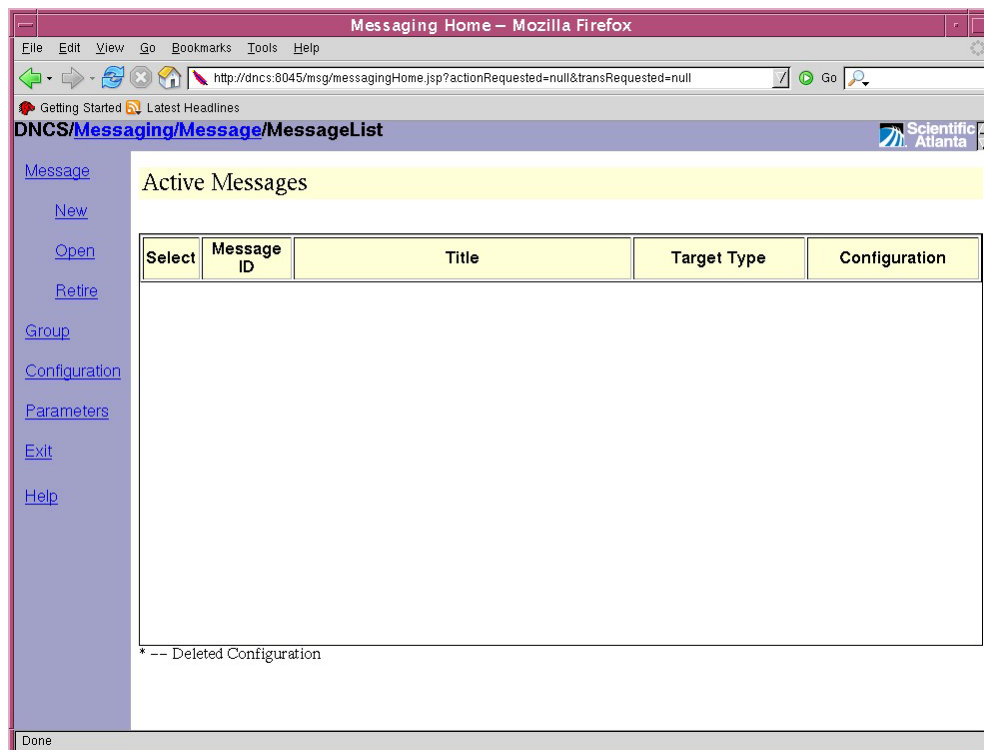
3 Select **Configuration** then choose **New** . The Create New Configuration window opens with **Urgency*** selected.

Important: The Urgency*, Message Time*, and Force Tune* parameters are mandatory settings.

4   Type the configuration name in the Configuration Name field.

5   Select the message priority from the Priority drop-down list.

Note: You can select Normal, Emergency, or Alert.

6   Select who can clear the message from the Cleared By drop-down list.

Note: You can select User, DHCT, or System Only.

7   Click **Message Time*** and type the following settings into the respective fields:

a   Duration (in seconds): The length of time that the message will appear on the on the TV screen

b   Delay Between Repeats (in seconds): The length of time before the message will reappear on the TV screen

c   Number of Repeats: The number of times the message will repeat prior to the expiration time

d   Expiration Time (in minutes): The length of time that the message will remain in the system

8   Click **Force Tune*** and provide the following information in the respective fields:

a   Force Tune: Enables or disables force tuning. Select **NONE** to disable force tuning. Select **Service Id** to enable force tuning.

b   Service Id: If you selected Service Id in the Force Tune field, enter the Service Id to which the set-top will tune when the message is received

    c   Power On: Enables the set-top to power on or to remain powered off (in standby mode) when the message is received

    d   Lock Channel: Allows the set-top to tune to the force tuned channel if a Service Id is selected

    e   Trigger Key: If enabled, allows users to trigger the force tune by pressing a designated key on the remote control

    f   Audio PID: When force tuning is enabled, configure this field to determine which audio format should be available for the user

9   Click **Led Alert** and configure the set-top LED blinking rate (cycles/second, duration (seconds), and period (seconds).

10 Click **Display** and use the options available to configure how the message will display on the TV screen.

11 Click **Save** to save the configuration.

Create Message Groups

1   From the Message List window select **Group** and then choose **New**. The Create New Group window opens.

2   Type the group name in the Group Name field.

3   Type the MAC Address of the DHCT in the MAC Address field and then click **Add** to add the MAC address to the Associated DHCTs field.

4   To add more MAC addresses, repeat step 3 until you have entered all the required MAC addresses.

Note: To remove a MAC address from the Associated DHCTs field, highlight the MAC address and then click **Remove**.

5   Click **Save** to save the new group.

Configure Messaging Parameters

1   From the Message List window, select **Parameters**. The Parameter List window opens displaying available message parameters.
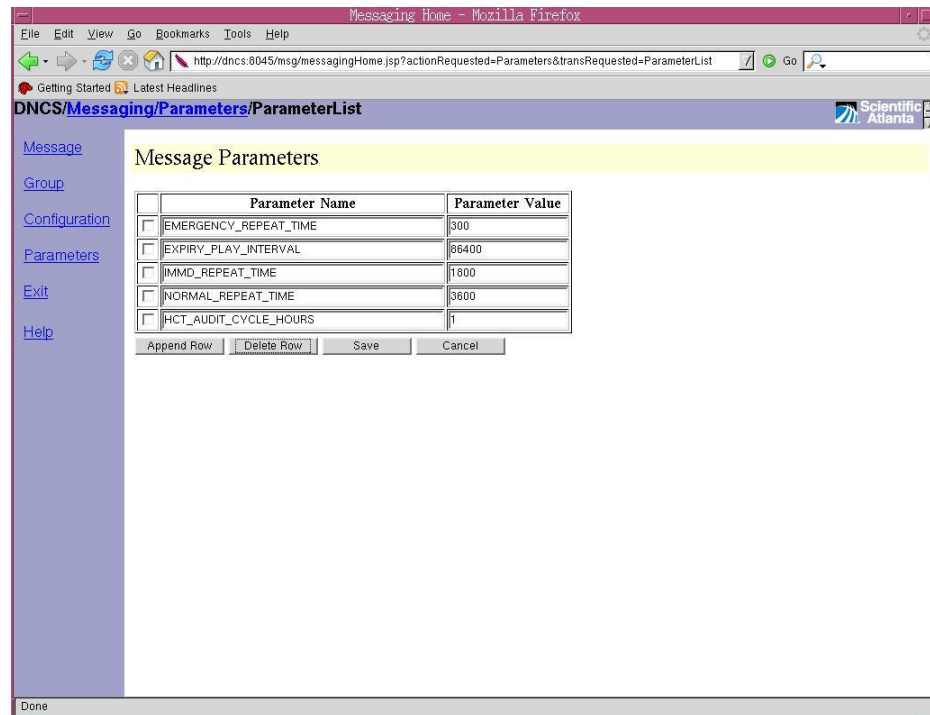
2   The value corresponding to the **EMERGENCY_REPEAT_TIME** parameter determines the repeat interval (in seconds) for Emergency messages.

3   The value corresponding to the **EXPIRY_PLAY_INTERVAL** parameter determines the duration (in seconds) for which retired messages will be played out for non-expiring messages.

4   The value corresponding to the **IMMD_REPEAT_TIME** parameter determines the repeat interval (in seconds) of Alert messages.

5   The value corresponding to the **NORMAL_REPEAT_TIM**E parameter determines the repeat interval (in seconds) of Normal messages.

6   The value corresponding to the **HCT_AUDIT_CYCLE_HOURS** parameter determines the duration (in hours) between which the group association messages will be sent periodically.

Create and Send Messages

1   From the Message List window, select **Message** and then choose **New**. The Create New Message window opens.

2 In the **Target** section, choose on of the following options:

- To send the message to a specific MAC address or to a list of MAC addresses, select **MAC ADDRESS** from the Send To drop-down list, enter the MAC address, and then click **Add** to add the MAC address to the target list. Repeat for additional MAC addresses.

- To send the message to a set-top group, select **GROUP** from the Send To drop-down list, select the Group Name from the Group Name drop-down list, and then click **Add** to add the Group name to the target list.

- To send the message to a specific Hub, select **HUB** from the Send To drop-down list, select the Hub Name from the Hub List, and then click **Add** to add the Hub to the target list. Repeat for additional Hubs.

- To send the message to a specific Site, select **SITE** from the Send To drop-down list, select a Site from the Site List, and then click **Add** to add the Site to the target list. Repeat for additional Sites.

- To send the message System wide (broadcast to all DHCTs in the system), select SYSTEM WIDE from the Send To drop-down list.

3 In the **Message Type** section, select the configuration from the Configuration drop down menu, and then select the audio type and content.

4 In the **Message Activation** section, select and/or enter the following information:

- To display the message immediately on the TV screen (without delay), select **None** from the Delay drop-down list.

- To display the message at a later time on the TV screen, select **Relative**, **Absolute UTC**, or **Absolute Local** from the Delay drop-down list, and then enter the Delay in Minutes and Activation Time.

5 In the **Message Content** section, select and/or enter the following:

a Select the Content Type from the drop-down list. The options are **None**, **Black Screen**, **HTML**, **URL**, or **Text** based on how you want the message content and format to appear on the TV screen.

b Select the **Language**. For example, for English, select ENG.

c In the **Message Title** field, enter the title of the message.

d In the **Message** field, enter the Message content.

e Click **Add** to add the message to the message list.

f Repeat steps b and e for multiple messages.

g Click **Send** to send the message based on the parameters you selected previously.

Delete a Group

1 From the Message List window, select **Group**. The Available Groups window opens displaying existing Group names.

2 Select the Group Name(s) that you want to delete and click **Delete** from the left menu under Group.

3 A confirmation window opens. Click **OK** to proceed.

Delete a Configuration

1 From the Message List window, select **Configuration**. The Available Configuration window opens displaying available configurations.

2 Select the Configuration Name(s) that you want to delete and click **Delete** from the left menu under Configuration.

3 A confirmation window opens. Click **OK** to proceed.

Retire Messages

1 From the Active Messages window, select a message from the message list and click **Retire**. The Retire Message window opens.
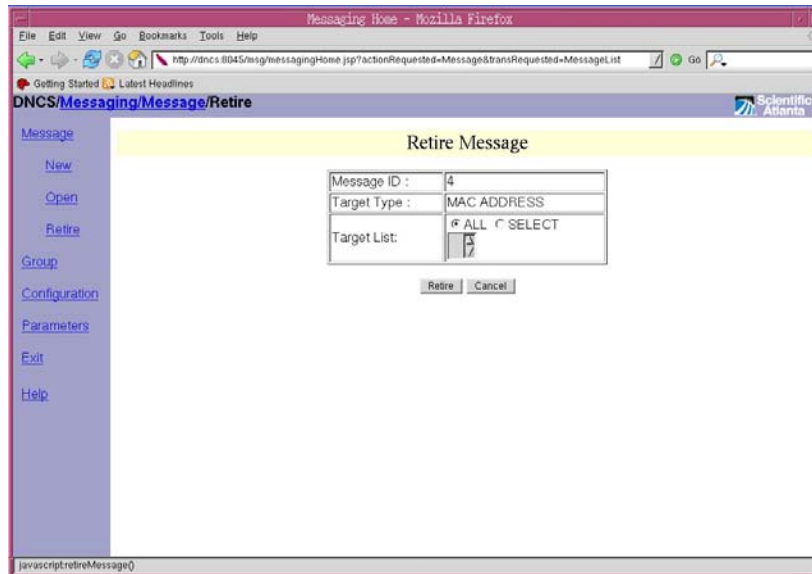
2 Choose one of the following options, and then go to step 3:

- To retire all messages in the Target List, click **ALL**.

- To select specific messages from the Target List, click **SELECT**.

3 Click the **Retire** button located under the table. The selected messages are retired.

15 Chapter 15

Troubleshooting

Introduction

This chapter provides procedures that allow you to manage and monitor your system components. Included in this chapter are instructions for enabling logging and tracing on the DNCS, enabling tracing on the Application Server and viewing the log files, and rebooting set-tops from the DNCS. Use the procedures in this chapter to manage, monitor, and troubleshoot your system.

In This Chapter

Enable Logging on the DNCS

Introduction

From the Logging Summary window, you can select the type of information the DNCS records about critical processes (and their libraries). When the DNCS records this information, it stores the information in the following locations:

■ Collective information about all processes is stored in dncsLog in /var/log/dncsLog.

■ Information about individual processes is stored in /dvs/dncs/tmp/[name of process.*]. The file name of the log for an individual process is the name of the process followed by a 3-digit counter. For example, the file name for the qamManager log might be qamManager.000.

The Logging utility is most useful when you are experiencing problems and want to capture information that can help you resolve the problem. After you adjust the logging level for a specific site and process, you can open the DNCS log in /var/log/dncsLog and view the data that the DNCS has recorded. Or open the log for an individual process in /dvs/dncs/tmp/[name of process.*].

Important: For additional details about the Logging feature, refer to the *DNCS Online Help for System Release i4.3 (Unix Version)* (part number 4038810).

Setting Logging on the DNCS

Adjust Logging Levels on the DNCS

Complete the following steps to select logging levels for processes running on the DNCS.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Utilities** tab.

3 Click **Logging**. The Logging Summary for Host window opens and displays the processes of the DNCS host as the default.
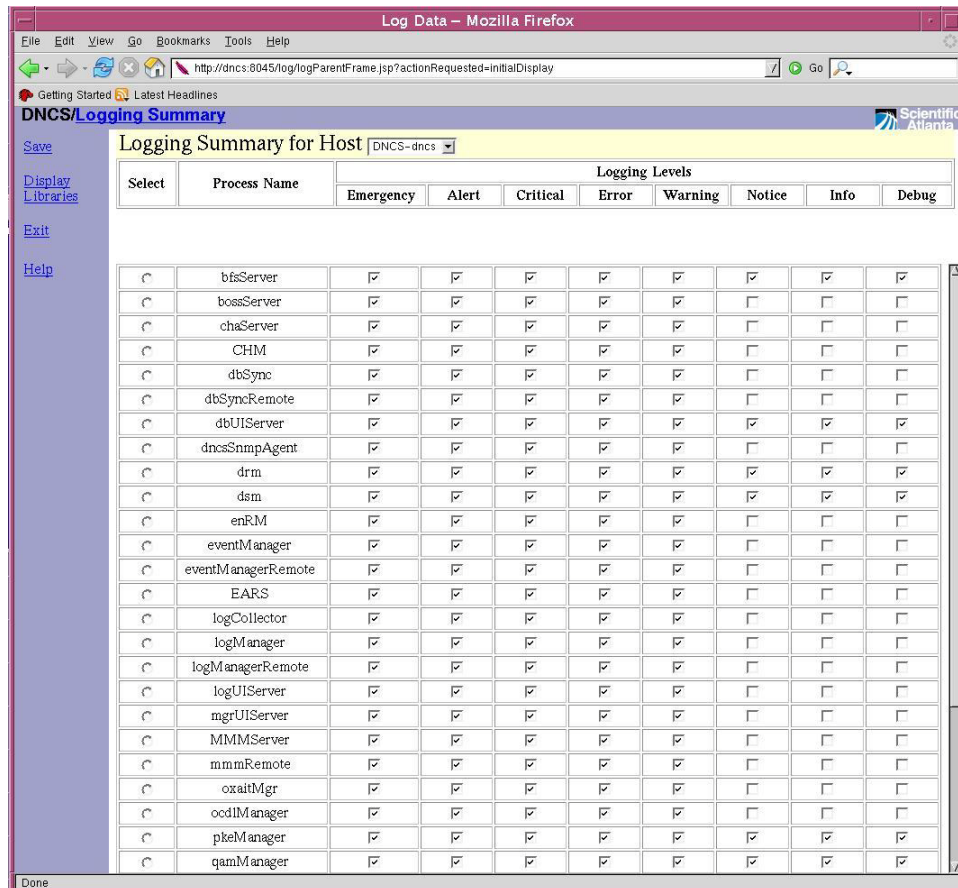
4 For each process whose logging level you want to change, click in the appropriate check box of the Logging Levels area of the window, and select the level you want the system to apply.

5 Click **Save**. The system displays a message to let you know the save was completed.

6 Click **OK**.

7 Click **Exit** to close the Logging Summary window and view the logging data in /var/log/dncsLog. Or look at data for an individual process in /dvs/dncs/tmp/[name of process.*].

Adjust the Logging Levels of Libraries

Complete the following steps to select logging levels for the libraries of specific processes.

1 On the DNCS Administrative Console, click the **DNCS** tab.

2 Click the **Utilities** tab.

3   Click **Logging**. The Logging Summary for Host window opens and displays the processes of the DNCS host as the default.
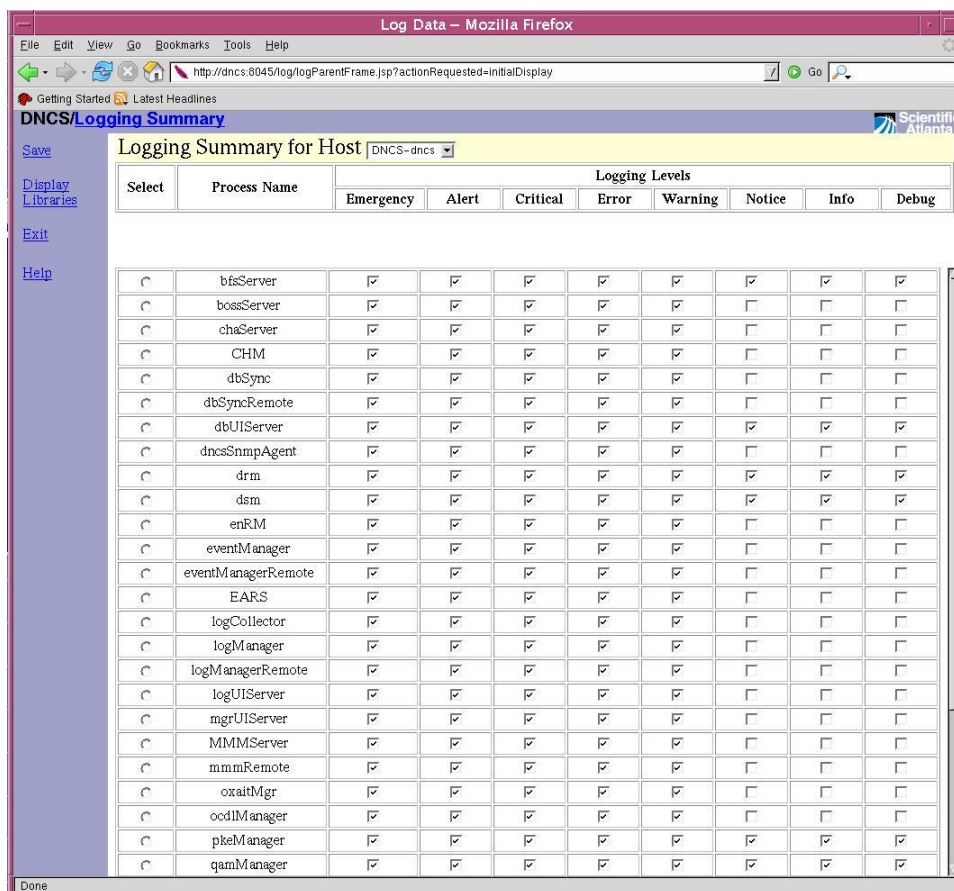
4   Click the option button in the **Select** column next to the process whose libraries you want to log.

5   Click **Display Libraries**. The Libraries for the process you selected in the previous step are listed beneath the Logging Summary list.

6 For each library whose logging level you want to change, click in the appropriate check box of the Logging Levels area of the window, and select the level you want the system to apply.

7 Click **Save**. The system displays a message to let you know the save was completed.

8 Click **OK**.

9 Click **Exit** to close the Logging Summary window. You can now open an xterm window and view the logging data in /var/log/dncsLog. Or look at data for an individual process in /dvs/dncs/tmp/[name of process.*].

Enable Tracing on the DNCS

Introduction

The DNCS includes a tracing function, which tracks the flow of information through the DNCS processes. In order to capture this information to a log file, you must enable tracing on the DNCS.

You can choose to trace varying information with varying degrees of detail. You do this through the use of trace levels. Trace levels let you specify how much information you want to include in the log file. The following table provides valid trace levels.

Trace Level	Definition
0	Reports only errors. This level is always turned on by default whenever tracing is enabled.
1	Reports errors and debug information.
2	Reports errors, debug information, and flow information.

Important: For additional details about the Tracing feature, refer to the *DNCS Online Help for System Release i4.3 (Unix Version)* (part number 4038810).

Enabling Tracing on the DNCS

Complete the following steps to enable tracing on the DNCS.

1   On the DNCS Administrative Console, select the **Utilities** tab and then click **Tracing**. The DNCS Tracing Management window opens.
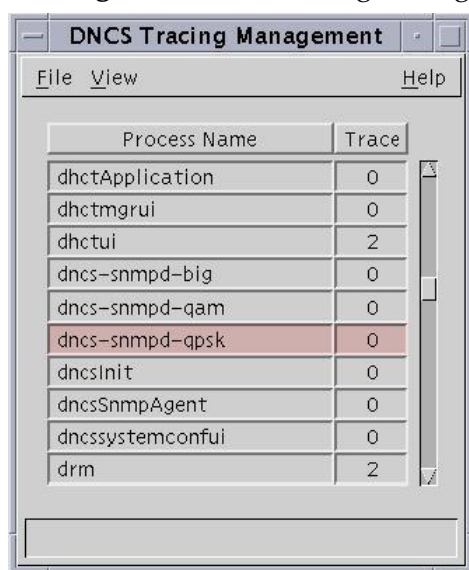
2 From the DNCS Tracing Management window, highlight a process from the list, select **File** and then click **Open**. The Set Up Tracing window opens.

3 From the Set Up Tracing window, choose the tracing level that you want to apply to the selected process.

4 When you have completed choosing all tracing levels, click **Save** to save your settings and close the Set Up Tracing window.

Enable Tracing on the Application Server

Introduction

The Application Server includes a tracing function, which tracks the flow of information through Application Server processes. In order to capture this information to a log file, you must enable tracing on the Application Server. Cisco Services may request that you enable tracing so you can capture this information for diagnostic purposes.

This section provides procedures to enable and disable the tracing function and to specify the level of detail that you want to include in the log file.

Understanding Trace Levels

You can choose to trace varying information with varying degrees of detail. You do this through the use of **trace levels**. Trace levels let you specify how much information you want to include in the log file. The following table provides valid trace levels.

Trace Level	Definition
0	Reports only errors. This level is always turned on by default whenever tracing is enabled.
1	Reports errors and debug information.
2	Reports errors, debug information, and flow information.

The trace.cfg File

The Application Server contains a file called /dvs/appserv/tmp/trace.cfg. This file contains commands that let you specify the following options:

■ Whether to enable or disable tracing for a specific process

■ The amount of detail that you want to capture to a log file

■ In order to enable or disable tracing or to change the trace levels for a process, you must edit the trace.cfg file

After you make changes to the trace.cfg file, you can run the /dvs/appserv/bin/tools/showTracing utility to put the changes into effect. If you do not run the showTracing utility, any changes that you made to the trace.cfg file may not take effect immediately. It is not necessary to restart any Application Server processes for changes to take effect.

Syntax For The trace.cfg File

You must enter the trace.cfg entries using the following syntax:

tracename programcontext tracelevel

The following table explains each component of the trace.cfg entry. Use the components to build entries for the trace.cfg file.

Part	Description
tracename	Identifies the subset of code within an executable file that you want to trace. The **tracename** component can be the trace name that was registered in the executable code, or it can be the library file name without the lib and .* extensions.
	The tracename component is optional. You can include tracename to turn on tracing for a given subset of code, such as a library. If it is omitted, tracing is turned on in all contexts for the tracename.
programcontext	Identifies the process that you want to trace. The **programcontext** component can be the name of the executable file or the trace name that was registered in the executable code.
tracelevel	Identifies the level of detail that you want to capture for this process.

Examples:

- _ipgui 2—The programcontext is _ipgui, and the tracelevel is 2. This entry starts a level 2 trace on the _ipgui process.

- gui _ipgui 1—The tracename is gui, the programcontext is _ipgui, and the tracelevel is 1. This entry starts a level 1 trace on code labeled gui in the _ipgui process. (This code may be in the gui library.)

- All _ipgui 1—The tracename is all, the programcontext is _ipgui, and the tracelevel is 1. This entry starts a level 1 trace on all code in the _ipgui process.

Enabling the Tracing Function on the Application Server

In order to enable or disable tracing for an Application Server process, you must edit the /dvs/appserv/tmp/trace.cfg file. Each line in this file represents a trace command for an Application Server process.

Lines that begin with a pound sign (#) are comments. The tracing function ignores these lines. Therefore, in order to disable tracing, you can simply add a pound sign to the beginning of the corresponding line.

Also, some of these comment lines may contain trace commands that have been disabled. To enable tracing, you can simply remove the pound sign from the beginning of those lines.

Complete these steps to enable the tracing function for an Application Server process.

1   In an xterm window on the Application Server, type **cd /dvs/appserv/tmp** and press **Enter**. The /dvs/appserv/tmp directory becomes the working directory.

2   Type **vi trace.cfg** and press **Enter**. The trace.cfg file opens.

3   Does the file contain any comment lines that correspond with the tracing function you want to enable?

   ■   If **yes**, remove the **#** from the beginning of that line and go to step 5.

   ■   If **no**, go to step 4.

4   Use the arrow keys to scroll to the bottom of the file and add the appropriate entry for the tracing function you want to enable.

   Note: See *The trace.cfg File* section (on page 188) for more information on writing trace.cfg entries.

5   Type **:wq** to save and close the file.

6   Type **dvs/appserv/bin/tools/showTracing** to put the changes into effect.

   Important: If you do not perform this step, the changes that you made will not be put into effect.

Disabling the Tracing Function on the Application Server

Complete these steps to disable the tracing function for an Application Server process.

1   In an xterm window on the Application Server, type **cd /dvs/appserv/tmp** and press **Enter**. The /dvs/appserv/tmp directory becomes the working directory.

2   Type **vi trace.cfg** and press **Enter**. The trace.cfg file opens.

3   Find the entry that corresponds with the tracing function you want to disable.

4   Place the cursor at the beginning of the line you want to disable and type #.

   Note: It is a good idea to comment out the entry instead of deleting it. By doing so, you can easily enable the command later if necessary. To comment out an entry, add a # to the beginning of the line containing the entry.

5   Type **:wq** to save and close the file.

6   Type dvs/appserv/bin/tools/showTracing to put the changes into effect.

View the Log Files on the Application Server

Introduction

The Application Server captures various kinds of trace information to various log files. Those log files are stored in two directories: /var/log/dncsLog and /dvs/appserv/tmp. The log files contain the following information:

- The files in /var/log/dncsLog only contain error message and process start/stop messages. The Application Server automatically deletes these log files after three days.

- The files in /dvs/appserv/tmp contain all of the process output that is captured. The Application Server automatically deletes these log files after seven days.

The Logger Utility

The Application Server includes a utility called Logger that manages the size, name, and placement of the log files in the/dvs/appserv/tmp directory. Logger stores these files for 7 days. Logger creates a new log file for each traced process every day or when the previous log file reaches a pre-determined size. When Logger creates a new log file, it closes the old file and compresses it using the gzip utility. A compressed file is renamed to include a .gz extension.

Viewing the Log File

To view the data in a zipped log file, type **gzip –dc goqam.gz** and press **Enter**. In this command, goqam is the name of the file you want to view. When you enter this command, the Application Server creates an unzipped file without the .gz extension.

For example, to view the data in vcServer.101.gz, type **gzip –dc vcServer.101.gz** and press **Enter**. The Application Server creates an unzipped file called vcServer.101.

Log File Naming Conventions

Log files for individual processes are stored in the /dvs/appserv/tmp directory. These files are named after the process that they traced, and the filename contains a three-character extension. For example, **ppvfileserver.201** contains trace information for the ppvfileserver process.

The first character of the three-character extension identifies the day of the week that the information was captured as follows:

Character	Day of the Week
0	Sunday
1	Monday
2	Tuesday
3	Wednesday
4	Thursday
5	Friday
6	Saturday

The second and third characters number the files that were created for a specific process during a specific day, beginning with 00 and going through 99.

Examples:

- The **vcServer.400** file contains the first section of trace information for last Thursday for the vcServer process.

- The **bfsRemote.003** file contains the fourth section of trace information for last Sunday for the bfsRemote process.

If any processes are running multiple instances, such as the ipgServer, the log files will be named after the programContext instead the programName. For example, **ipgServer-eng.201** contains the second section of trace information for last Tuesday for the ipgServer-eng process.

Reboot a DHCT

Introduction

Occasionally, for troubleshooting or monitoring purposes, you may need to reboot a DHCT from the DNCS. You can reboot a DHCT from the DNCS using one of the following methods:

- DHCTs of a specific model number

- An individual DHCT

Select from the following procedures according to your system requirements and current needs.

Rebooting DHCTs of a Specific Model Number

Follow these instructions to reboot DHCTs of a specific model number.

1   If necessary, open an xterm window on the DNCS.

2   Type **IIH -b -M[model number]** and then press **Enter**.

   Note: Substitute the model number of DHCT for [model number].

   Example: IIH -b -M3375

   Result: A confirmation message, similar to the following, appears:

   **saManager is running
   DHCTs with DHCT model=[model number] will be Rebooted
   # MAC addresses will be involved.
   Do you want to continue (Y/N)?**

3   Type **y** and then press **Enter**. The system reboots the specified DHCTs.

Rebooting an Individual DHCT

Follow these instructions to reboot an individual DHCT.

1   If necessary, open an xterm window on the DNCS.

2   Type **IIH -b [DHCT MAC address]** and then press **Enter**. The system reboots the specified DHCT.

Notes:

■   Substitute the MAC address of the DHCT for [DHCT MAC address].

■   The MAC address can be formatted with or without colons (:).

Examples:

■   **IIH -b 00:02:DE:A6:45:92**

■   **IIH -b 0002DEA64592**

Reset the PIN on a DHCT

Complete the procedure in this section to reset the PIN on a DHCT.

Important: This procedure applies to resetting the DHCT PIN from the DNCS. You can also reset the DHCT PIN from the billing system.

1 Is your system configured with the Application Server?

- If **yes**, go to step 2.

- If **no**, go to step 7.

2 In the DNCS Administrative Console, click the **Server Applications** tab.

3 Click **DHCT Config**. The DHCT Configure Prompt window opens.

4 In the DHCT Configuration Prompt window, click **Addressable**. The Set Up Addressable DHCT Configuration window opens.

5 In the DHCT MAC Address field, enter the **MAC Address** of the DHCT.

6 Select the PIN Entry tab and enter the **Blocking PIN** and the **Purchase PIN** in the appropriate fields. Then, go to step 11.

7 In the DNCS Administrative Console, click the **Home Element Provisioning** tab.

   Note: Make sure that the variable PKDVB_APPSERV_NOT_PRESENT is set to **1** (one) in the /export/home/dncs/ .profile file.

8 Click **DHCT**. The DHCT Provisioning window opens.

9 Select the **By MAC Address** option, enter the **MAC Address** of the DHCT, and then click **Continue**. The DHCT Setup window opens.

10 In the DHCT Setup window, enter the **PIN** in the Set PIN field.

11 Click **Send** to send the new PIN to the DHCT.

16

Customer Information

If You Have Questions

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

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

A

Sources and Services Naming Conventions

This appendix contains the naming conventions for sources and services in the PowerKEY DVB System.

In This Appendix

TSID Numbering Conventions

TSID Numbering Suggestions

Use the following suggestions for TSID numbering:

- MPEG Source Output TSIDs: 01 to 99

- MQAM Input TSIDs: 01 to 99

- MQAM Output TSIDs = MQAM Input TSIDs + 100

- Output TSID Range: 101 to 199

- D96xx Output TSID = MQAM output TSID

- NIT (DVB SI) TSIDs = MQAM output TSIDs

DVB Service ID Numbering Conventions

DVB Service ID Numbering Suggestions

Sources provisioned in the DNCS should be thought of as being DVB services. DVB services are identified by triple ONID, TSID, and Source (Service) IDs. Use the following suggestions for DVB Service ID numbering:

- The ONID is the Network ID provisioned in the hub.

- The TSID is the output RF TSID provisioned in the MQAM.

- The Source (Service) ID is a five digit number where the first 3 digits are the TSID and the last 2 digits are a unique service number for the TSID. TSIDs range from 101 to 199. Service numbers range from 01-99.

  Example: Service ID = XXXYY where XXX is the TSID ID and YY is the Service number.

DVB Service ID Examples

The following list illustrates DVB Service ID examples.

- DVB service = CNN

- DNCS Hub Network ID = 48059 0xBBBB

- MQAM output TSID = 101

- MQAM input TSID = 1

- MPEG Source output TSID = 1

- First service for TSID = 101

- DVB ONID = 48059

- DVB TSID = 101

- Service ID = 10101

- DNCS Source ID = 10101

Note: The DVB Service IDs on your system may vary.

Glossary

App Server

> See Application Server.

Application Server

> A server that executes applications that are required to provide digital services to subscribers. The Application Server comes with the following set of standard applications:
>
> - DHCT Configuration
>
> - Pay-Per-View event and Service setup

BFS

> Broadcast File System. The primary interface (means of communication) between the AppServer and the DHCTs that are connected to the network.

CF session

> Continuous Feed Session. Defines and allocates resources that the network uses to deliver a particular service to subscribers. A CF Session will remain intact until the DNCS operator manually tears it down.

Channel

> A signal space of a specified bandwidth. The 8 MHz band space used for the video, audio, and game data carriers. Also used to identify the service provided on a particular channel.
>
> - For digital audio, the 3 MHz band space for one QPR carrier.

Channel Map

> A set of channels that specific subscribers are authorized to receive through their DHCTs.

Channel Mapping

> Placing an available television channel signal to appear at any desired channel marking on a customer's HCT.

Comment out

To add a # (pound sign) to the beginning of a line in a configuration file. The Application Server ignores any lines that begin with a #.

DBDS (Digital Broadcast Delivery System)

Name for the our system of delivering digital signals on a two-way path to the cable subscriber's home television. This system would include all hardware and signaling paths from the satellite signal interfaces to the cable converter box in the subscriber's home.

DHCT (Digital Home Communications Terminal)

Device that connects a subscriber's television to the DBDS, allowing the subscriber to receive broadband services. The DHCT provides services to subscribers by tuning to the appropriate digital channel, decompressing the video and audio streams, decrypting them if necessary, generating an analog output signal to carry the video and audio content, and then sending it to the television. The type of data carried on each data channel is as follows:

– From the FDC, the DHCT receives system messages, as well as tuning and management data.

– The DHCT uses the reverse data channel to send data relating to billing, performance monitoring, email, event purchases, and the Internet upstream to QPSK demodulators.

Direct ASI

Direct ASI allows you to send BFS data directly from the DNCS to your BFS QAM modulator. Direct ASI simplifies your network by eliminating the need for a BFS BIG or for ATM permanent virtual circuits (PVCs). If you are using an RCS you can send BFS data directly from an RNCS/LIONN at a remote site to the FS QAM modulator at the remote site.

DNCS (Digital Network Control System)

The computer workstation that defines, organizes, monitors, and controls the components, features, and applications supported by the DBDS. The DNCS provides DHCTs with broadcast services that are displayed on subscribers' televisions throughout a cable network. The DNCS works with the Ethernet router providing data throughout the DBDS. The DNCS uses multi-mode fiber to transfer data through the ATM switch to the router. Data is sent in ATM cells over PVCs.

DVB

- Short for Digital Video Broadcasting Project (DVB), DVB is an industry-led consortium of more than 260 broadcasters, manufacturers, network operators, and regulatory bodies and others in over 35 countries committed to designing global standards for the global delivery of digital television and data services.

- DVB is also the name used to describe the various European systems for television, radio and data broadcasting in all areas of the world outside of North America.

ECM

Entitlement Control Message. System-wide information that "unlocks" an encrypted service by transmitting control words. Each ECM is unique for each service. An ECM enables cryptographic partitioning so that different Entitlement Agents (EAs) can selectively grant access to their own services.

Element

Term used to refer to DBDS devices, groups of devices, and software components that must be provisioned from the DNCS.

EPG (Interactive Program Guide)

A program listing and schedule that is displayed on the television screen.

Explorer

Our trademarked name for the Digital Home Communications Terminal. Also known in the CATV industry as a set-top box.

GQAM

gigabit quadrature amplitude modulation. A QAM that provides up to sixteen 6 MHz outputs while occupying only one unit of rack space. *See also* QAM, MQAM.

headend

The location of the network elements that processes the signal by receiving and preparing the source signals and making them ready for the transport network. *See also* network elements.

HFC

hybrid fiber coax. Consists of fiber optic transmission systems extending from a hub to HFC nodes, and a coax bus network extending from the HFC nodes to the DHCTs within the subscriber's home.

interstitial

Programming that appears on PPV channels between events, such as general programming or an advertisement.

LED

light-emitting diode. Semiconductor device that converts electrical energy into light. Status lights on hardware devices are typically LEDs.

Logger

A utility on the Application Server that manages the size, name, and placement of the log files

in the/dvs/appserv/tmp directory

MAC address

Media Access Control address. A unique physical address embedded into a network device. Similar to a serial number.

modulator

Sends control and authorization information from the DNCS to the DHCT.

MPEG

Moving Picture Experts Group. An international video compression standards-setting group working under the supervision of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). MPEG's mission is to develop standards for compressed full-motion video, still image, audio and other associated information.

MPEG-2

Intended for higher quality video-on-demand applications and runs at data rates between 4 and 9 Mbps.

MQAM

Multiple Quadrature Amplitude Modulation. A QAM that provides up to four 6 MHz outputs while occupying only one unit of rack space. *See also* QAM, GQAM.

MSO

multiple system operator. A cable company that operates more than one cable system.

network elements

Devices typically located at the headend, which include satellite receivers (IRT, IRD), Real-Time Encoder (RTE), BIG, QAM modulator, DNCS, and the application server. *Also known as* system components.

NVOD (Near Video-On-Demand)

A technique used in cable services using several channels to transmit a feature film with staggered start times.

PowerKEY® Conditional Access system

Our registered trademark name for the hardware and software encryption and decryption of digital signal. Uses secret key, public key, and private key data to secure the digital signal.

PPV

pay-per-view. Service for which subscribers are charged a user fee for individual program events.

PPV barker

A screen that the DHCT displays appears to advertise an event or let a subscriber order a PPV event.

PPV window

A period of time during which a PPV action occurs. The period of time that a window is present often determines when the PPV service displays a specific type of advertisement or purchase option.

provision

The process of preparing a device or service so that the DNCS recognizes the device, which allows the device to operate properly.

QAM

quadrature amplitude modulation. A frequency modulation technique primarily used for program audio and video. QAM supports data rates from 38 to 50 Mbps.

RMA

Return material authorization.

RPPV

Reservation pay-per-view. Requires the subscriber to use the telephone to reserve a PPV event.

SAM

Service Application Manager. Associates a specific service with an application that defines the medium to be used for that service, such as the World Wide Web. The SAM maintains the application in a specific directory to be used when needed by the DHCTs.

SARA

SA Resident Application. The set of operating programs that is "permanently" loaded into the DHCT. These programs are immediately available to the subscriber upon activation of the DHCT.

Session

See *CF session*.

source

In the DBDS, a source is the actual program or data that is made available to the DHCT as a service to the subscriber. Sources can include: MPEG-2 digital broadcast services that are non-secure, non-encrypted, audio/video programs; Internet connections from an Internet service provider (ISP); Digital PPVs that are secure, encrypted, digital MPEG-2 programs; Digital music services; Analog programs that are modulated in the traditional format or converted into MPEG-2 format.

SR

System Release. Our software release package for components of the DBDS.

staging

The process of loading the necessary software and security information into the Explorer DHCT prior to deployment in subscriber's homes.

TED

Transaction Encryption Device. Provides Conditional Access control for the PowerKEY software within the DNCS and works directly with the DNCS to maintain security throughout the network.

Tracing

The process of tracking the flow of data messages between the Application Server and other network elements.

VCR

videocassette recorder.

VOD

video-on-demand. The ability of a subscriber to select a program event and watch it within moments of selection. VOD allows pausing and rewinding of the event.