Digital Network Control System Online Help for System Release i4.3

Table of Contents

Welcome to the DNCS Online Help for PowerKEY DVB System Release i4.3

Welcome to the Help system for the Digital Network Control System (DNCS) for PowerKEY Digital Video Broadcasting (DVB) System Release (SR) i4.3.

- **Introducing the PowerKEY DVB System** - Learn about the PowerKEY DVB System.
- **About This Version of Help** - Find general information about this version of online help: the version number, the copyright date, the system releases it covers, the terms and conditions of use, the trademarks used, and what's new for System Release (SR) i4.3.
- **Additional Support and Resources** - Obtain other help resources, such as printed guides and technical support.
- **Help for New Users** - Learn about the basic tools that can help you successfully manage a Digital Broadband Delivery System (DBDS).
- **Restarting the DNCS** - Learn the correct order in which to stop and restart critical DNCS processes.
- **Network Setup Overview** - Get an overview of the tasks required to set up a DBDS.
- **Setting Up DBDS Elements** - Learn how to set up the elements used in a standard DBDS.
- **Setting Up Services for Subscribers** - Learn how to set up services for your subscribers.
- **Monitoring Your DBDS** - Learn tasks that can help you monitor your DBDS to ensure it is working properly.
- **Maintaining Your DBDS** - Learn how to keep your DBDS in good working order.
- **Troubleshooting Your DBDS** - Learn how to solve problems when they occur.

Back to Top

Introducing the PowerKEY DVB System
Introducing the PowerKEY DVB System

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

About This Version of Help
About This Version of Help

DNCS Online help version i4.3.0.0 supports PowerKEY DVB SR i4.3. For details about this version of DNCS Online help, see the following topics:

- Help version and copyright information for this help document
- Terms and conditions for use of this version of DNCS Online help
- Trademarks used in this version of DNCS Online help
- What's New for System Release i4.3?

DNCS Help for PowerKEY DVB SR i4.3.

DNCS Online Help Version i4.3.0.0 (UNIX)
Part Number 4038810 Rev A
October 2010

Back to Top

Terms and Conditions

Following are the terms and conditions to which you agree by using the DNCS Help System.

Warning

This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

Acknowledgements

I understand that the information and materials provided in this DNCS Online Help System (the "System") by Scientific-Atlanta, LLC (hereafter "Cisco"), a wholly owned subsidiary of Cisco Systems, Inc., may not always be completely accurate and up-to-date. I agree to use the information provided in the System solely for the purpose of operating my company's Digital Network Control System ("DNCS") and for no other purposes.

Disclaimer

THE SYSTEM IS PROVIDED, “AS IS, WHERE IS, WITH ALL FAULTS.” THERE ARE NO WARRANTIES, WHETHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE SYSTEM OR ANY OF THE INFORMATION PROVIDED THEREIN, INCLUDING BUT NOT LIMITED TO ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SCIENTIFIC-ATLANTA, INC. ASSUMES NO RESPONSIBILITY FOR ERRORS OR OMISSIONS THAT MAY APPEAR IN THE SYSTEM. SCIENTIFIC-ATLANTA, INC. DOES NOT WARRANT THAT THE FUNCTIONS DESCRIBED IN THE SYSTEM WILL MEET THE USER’S REQUIREMENTS OR THAT THE OPERATION OF ANY EQUIPMENT PURSUANT TO THE GUIDELINES SET FORTH IN THE SYSTEM WILL BE UNINTERRUPTED OR ERROR-FREE. SCIENTIFIC-ATLANTA, INC. MAKES NO WARRANTY OF NON-INFRINGEMENT, EXPRESSED OR IMPLIED. THE USER OF THE SYSTEM ACKNOWLEDGES ITS RESPONSIBILITY TO USE ALL REASONABLE METHODS TO PROVE OUT AND THOROUGHLY TEST THE OPERATION OF THE DNCS AND ALL OUTPUTS FROM THE DNCS PRIOR TO ITS USE IN THE USER’S OPERATIONS.

Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL CISCO. OR ITS SUBSIDIARIES BE LIABLE FOR ANY DIRECT, INDIRECT, PUNITIVE, INCIDENTAL, SPECIAL, LOSS OF PROFITS, EXEMPLARY OR CONSEQUENTIAL DAMAGES THAT RESULT FROM THE USE OF, OR INABILITY TO USE, THE SYSTEM OR USE OF ANY INFORMATION OR CONTENT INCLUDED IN THE SYSTEM. THIS LIMITATION APPLIES WHETHER THE ALLEGED LIABILITY IS BASED ON CONTRACT, TORT, WARRANTY, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER BASIS, REGARDLESS OF THE CAUSE OF SUCH DAMAGE AND EVEN IF CISCO HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Indemnification

Upon a request by Cisco, you, on behalf of your company, agree to defend, indemnify, and hold harmless Cisco. and its subsidiaries and other affiliated companies, and their employees, contractors, officers, and directors from all liabilities, claims, and expenses, including attorneys’ fees, that arise from your use or misuse of the System.

Other Terms

Cisco reserves the right to change the System at any time without notice. The System 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 the System employs an invention claimed in any existing or later issued patent.

The information contained in the System is confidential and proprietary information intended for the use of authorized licensee’s of the Cisco DNCS only. If you are not an authorized licensee of the Cisco DNCS, you are hereby notified that any disclosure, use, copying or the taking of any action in reliance on the information provided in the System is strictly prohibited. Information in the System is subject to change without notice. No part of the System may be reproduced or transmitted in any form, by photocopy, microfilm, xerography, or any other means, or incorporated into any information retrieval system, electronic or mechanical, for any purpose, without the express permission of Cisco.

Back to top

Trademarks

The following list provides trademark information for products mentioned in this Help system:

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.

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

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

Back to top

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 System Release (SR) i4.3.

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 a platform-independent 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 ROM 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, CVT triggers, and image carousels available.

See Configure External Download Interface Support for more information.

EMM Carousel Improvements

The rate at which Refresh EMMs are sent out has been increased. The enhancements included in SR i4.3 allow the DNCS to support up to a maximum of 25 set-tops per second (2 million set-tops a day). A Staging Carousel has also been added. In addition, new variables are available to allow system operators to manage EMM bandwidth dynamically between the following contributing sources:

- Refresh EMMs (Renewal EMMs for CA expiration extension)
- Staging EMMs (EMMs sent out on the Staging Carousel [Instant Hit Repeat Subsequent play out])
- Adhoc EMMs (EMMs generated by user operations [ModDhctConfig, AddAuthorization, RemoveAuthorization, and Instant Hit (First Time)])
- PPV EMMs (Event Authorization EMMs refresh just before the event starts)
- Other Conditional Access (CA) messages (Messages related to the CA system, for example, GBAMs)

Improvements have been made to the EMM carousel to address the following issues that were encountered in previous releases:

- The DNCS did not fully utilize the EMM carousel because the distribution cycle was configured in days. For SR i4.3, you can configure the distribution cycle in hours.
- A new Refresh EMM Cycle started only after the configured period of the last cycle ended, even though all set-tops are refreshed.
- Some EMM Packets were dropped because of heavy BOSS activity (for example, ModDhctConfig/DhctInstantHit) taking place at the same time as the refresh cycle.

The following EMM Carousel improvements have been made to address the challenges above and enable the system to:

- Refresh EMMs at a faster rate
- Configure the Refresh EMM cycle in order of hours to increase the distribution cycle rate and to allow for multiple cycles in a day
- Allow users to manage the EMM pipe bandwidth dynamically between the following contributing sources:
    - Refresh EMMs
    - Staging EMMs
    - Adhoc EMMs
    - PPV EMMs
    - Other Conditional Access (CA) messages

See Configuring the EMM Carousel for more information.

Informix 11.1 Support

SR i4.3 provides support for Informix 11.1. This support provides performance improvements for enterprise replication that is 20 to 40% faster than IDS 9.2.x.

Additional Support and Resources

Additional Support and Resources

The following additional resources are also available to help you:

- Technical support from our service engineers or customer service representatives
- Printed resources, which can be ordered or viewed from the Internet

---

Contact Us

If you have questions about this product, use the following table to call the technical support or customer service center in your area. Follow the menu options to speak with a service engineer or customer service representative.

Region	Assistance Centers	Telephone and Fax Numbers
United States	Cisco® Services Atlanta, Georgia	Technical Support for *Digital Broadband Delivery System* products only, call: Toll- free 1-866-787-3866 Local 770-236-2200 Fax 770-236-2488
		Technical Support for all products *other than* Digital Broadband Delivery System, call Toll- free 1-800-722-2009 Local 678-277-1120 Fax 770-236-5748
		Customer service questions: Toll-free 1-800-722-2009 Local 678-277-1120 Fax

		770-236-5748
Europe	European Technical Assistance Center (EuTAC), Belgium	Product Information: 32-56-445-444 Technical Support: 32-56-445-197 or 32-56-445-155 Fax 32-56-445-061
Asia-Pacific	Hong Kong, China	Technical Support 011-852-2588-4745 Fax 011-852-2588-3139
Australia	Sydney, Australia	Technical Support 011-61-2-8446-5394 Fax 011-61-2-8446-8015
Japan	Tokyo, Japan	Telephone 011-81-3-5322-2067 Fax 011-81-3-5322-1311

Back to top

Printed Resources

Visit our website (https://www.sciatl.com/subscriberextranet/techpubs) to view additional publications about our products.

You need a user name and password to access this website. If you do not have a user name and password, go to https://www.scientificatlanta.com/dsnexplorer/register.htm to complete and submit a registration form.

Note: You may need to install a PDF reader, such as Adobe Acrobat Reader, on your system to view these publications.

Back to top

Help for New Users
Help for New Users

These topics can help you find information quickly and learn the basics about the Digital Network Control System (DNCS) and how it can help you manager your Digital Broadband Delivery System (DBDS):

- **Help Tips for New Users**
- **DNCS Overview**
- **DNCS Status Bar**
- **DNCS Management Tools**

Back to Top

Tips for New Users

Help Tips for New Users

These tips can help you find information quickly:

Navigation Tips

Quick Paths

Print Help Topics

Search Tips

Ways to Find Information

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

- Use any of the following methods to find information you need in the DNCS Help:
    - Click the topic in the **Contents** list at left.
    - Click the **Index** tab at left and type in a keyword.
    - Click the **Search** tab at left and type in a keyword.
    - Click the **Glossary** tab at left and search through an alphabetical listing for definitions of terms used throughout this Help system.

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

- In many cases, you can press the **Enter** key on your keyboard and have the same effect as clicking **OK** or **Save** in a window.
- To open a window for an existing item, the procedures in this Help system advise you to click once on the item name, and then click **File > Open**. If you prefer, in many instances you can simply double-click on the item name to open the window.
- To return to a help topic you have previously visited, click **Go > Back** on your browser toolbar.
- 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 Internet browser and then re-open it.

Back to top

Quick Paths

At the beginning of many procedures in this Help system is a Quick Path for getting to a specific 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 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.

Back to top

Using the Search Feature

Follow these steps to use the Search feature.

1. In the left pane, click the **Search** tab and enter one or more key words in the **Search** field.
2. Click **List Topics** or press **Enter**. Help searches all topics containing the word or words you entered and displays the results of the search by listing topics containing the word or words in the list below.
3. Use one of the following methods to display a topic that appears in the list:
   - Click twice on any topic in the list.
   - Click on a topic and then click **Display**.

Tips for Searching DNCS Online Help

Entering a word or phrase in the Search tab and clicking Find explores the content of topics and finds all occurrences of the word or phrase. This method can help you find a topic (if you know its title), or every instance of a concept or feature in the system.

Use the following tips to refine your searches:

- Searches are not case-sensitive, so you can type your search in uppercase or lowercase characters.
- You may search for any combination of letters (a-z) and numbers (0-9).
- To search for an exact phrase, group the elements of your search using double quotes to set apart each element. For example, to search for information about the window Set Up BFS Host, enter **"Set Up BFS Host"** in the search field. This ensures that the system looks for this exact phrase. On the other hand, entering **Set Up BFS Host** in the search field, causes the system to look for topics that contain any of these four words.

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 activate that area (frame).
2. Click **File > Print Frame** on your browser toolbar.

Back to top

What Is a DNCS?

A Digital Network Control System (DNCS) is a UNIX workstation that is typically installed in a headend or, occasionally, a hub, and is connected to a Digital Broadband Delivery System (DBDS). The DNCS provides information about each element in a DBDS and allows elements to communicate with each other. By communicating with these elements, the DNCS allows operators to provide subscribers with many types of digital cable services.

Back to top

Using a DNCS

For the DNCS software to recognize and communicate with other DBDS elements, operators complete specific tasks from the following two DNCS user interfaces. These interfaces also allow operators to define, manage, and monitor most elements and services of a DBDS:

- DNCS Administrative Console Status interface
- DNCS Administrative Console interface

Back to top

Basic DNCS Tools
Status Tools

DNCS Administrative Console Status Window
The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.

For more information, click on either the **DNCS** or **AppServer** section in the following illustration.

Back to top

DNCS Status
The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- *Running* — the DNCS software package is present and in operation
- *Inactive* — the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

Back to top

SARA Server Status
The **AppServer** section of the Administrative Console Status window indicates whether or not the SARA Server is in operation based on the following conditions:

- *Running* — the SARA Server software package is present and in operation
- *Inactive* — the SARA Server software package is present, but not in operation
- *Not Responding* — the SARA Server does not respond when the DNCS tries to communicate with it
- *Not Installed* — a SARA Server host is defined in the host table, but the SARA Server software package is not present; usually indicates that you are not using the SARA Server, but the application server of another vendor

- *Blank* — no SARA Server host is defined in the host table, and the SARA Server software package is not present; usually indicates that you are not using the SARA Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the SARA Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major SARA Server processes.

CAUTION: Do not attempt to start or stop an AppServer process manually unless our technical representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers. Contact technical support.

The SARA Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server** (DHCT Configuration Server) - Sends the SetPIN transactions to the DHCT.
- **ppvfileserver** (Pay-per-view File Server) - Generates PPV files for SARA and places those files on the Broadcast File Server.
- **ppvServer** (Pay-per-view Server) - Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.

Note: Other processes that show in the AppServer Control window are not used in the international system.

For more information on the SARA Server, refer to *Configuring the PowerKEY DVB System for System Release i4.3.* To obtain this guide, refer to **Printed Resources**.

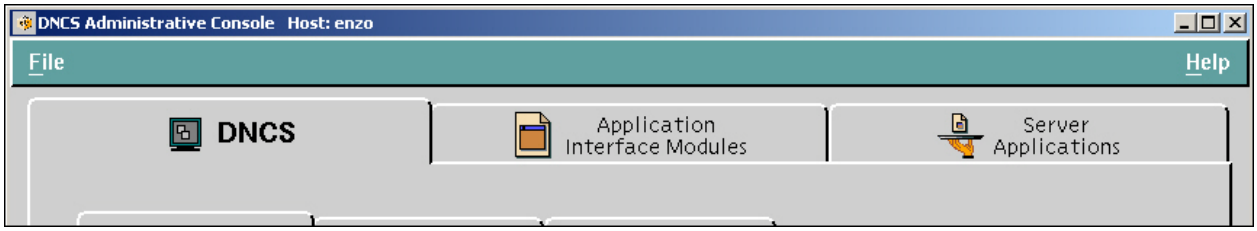
Back to top

Management Tools

DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.

For more information, click on a specific tab in the following illustration.



Back to top

DNCS Tab

DNCS Tab

The **DNCS** tab on the DNCS Administrative Console provides access to certain functions that DNCS software directly controls. These functions are separated into four sub-tabs:

- System Provisioning
- Network Element Provisioning
- Home Element Provisioning
- Utilities

Back to top

System Provisioning Sub-Tab

System Provisioning Sub-Tab

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab

The **System Provisioning** sub-tab on the DNCS tab is divided into six functional sections:

- Service Provisioning
- RF Spectrum Management
- Sites
- System Management
- Addressable Message

Note: The international system does not use the EAS feature, which is accessed from the buttons in the **EAS message** area of the tab.

Back to top

Service Provisioning

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab

The **Service Provisioning** section of the System Provisioning sub-tab has three buttons that allow you to set up aspects of different kinds of services as described in the following table.

This button...	Allows you to perform these tasks...
Source	• Add, modify, or delete analog and digital service sources. • Encrypt or un-encrypt service sources. • Add, modify, or delete analog and digital service source definitions. • Add, modify, or delete segments for individual sources. • View segments of all sources.
Package	• Add, modify, or delete service packages. • Create packages within packages.
ATM PVC	The international system does not use this feature.

Back to top

RF Spectrum Management

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab

The **RF Spectrum Management** section of the System Provisioning sub-tab contains the Bandwidth Allocation button, which allows you to perform the following tasks:

- Add, modify, or delete upper and lower frequency allocations for various service types (analog, digital, and so forth)
- View QAM sessions, frequency allocations, and transport stream IDs

Back to top

Sites

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab

The **Sites** section of the System Provisioning sub-tab contains the RNCS Sites button that allows you to perform the following tasks:

- View an RNCS site summary
- Add, save, or delete RNCS sites
- Add, save, or delete RNCS headends

- Add or delete billing references

System Management

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab

The **System Management** section of the System Provisioning sub-tab has four buttons that allow you to manage various aspects of the DBDS as described in the following table.

This button...	Allows you to perform these tasks...
DNCS System	• Set up DHCT session signalling parameters • Set up Network session signalling parameters • Establish whether or not the system is compliant with Open Cable standards. **Note:** The international system does not use Advanced Parameters or Channel Plan settings.
UN-Config	• Initiate UN-Config for a single DHCT. • Initiate UN-Config for a DHCT type. • Reboot a single DHCT. **Note:** For assistance in using this feature, refer to *Downloading New Client Application Platform Software Installation Instructions*. To obtain a copy of this document, see **Printed Resources**.
User Access	Add, modify, or delete users with differing levels of access to the DNCS. **Note:** For assistance in using this feature, refer to *Guidelines for System Security Passwords*. To obtain a copy of this document, see **Printed Resources**.
DHCT Mgr	• Establish the DHCT registration mode: Administrative Gateway or Open. • Establish the method by which IP addresses are assigned to DHCTs: Dynamic, Override, or Static. • Establish how often UN-Config messages are sent to DHCTs in the system. **Note:** For assistance in using this feature, refer to *Explorer Digital Home Communications Terminal Staging Guide*. To obtain a copy of this document, see **Printed Resources**.
DST	The international system does not use DST settings.

Back to top

Addressable Message

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab

The **Addressable Message** section of the System Provisioning sub-tab contains the Messaging button that allows you to perform the following tasks:

- View active messages
- Create, open, or retire Messages
- Create, open, or delete message groups from the Available Groups list
- Create, open, or delete message configurations from the Configuration list
- Edit and delete message parameters from the Parameter list

Network Element Provisioning

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab

The **Network Element Provisioning** sub-tab on the DNCS tab has several buttons that allow you to set up hardware elements in your system (excluding DHCTs) as described in the following table.

This button...	Allows you to perform these tasks...
Headend	Add, modify, or delete a headend.
Node Set	The international system does not use node sets.
Service Group	The international system does not use service groups.
Hub	Add, modify, or delete a hub.
QPSK/CMTS/OIT	Add an OIT bridge. **Note:** The international system does not use QPSK or CMTS bridges.
BIG	The international system does not use Broadband Integrated Gateways (BIGs).
QAM	• Add, modify, or delete an MQAM modulator. • Reset an MQAM modulator. **Note:** The international system does not use QAM or GQAM modulators.
MPEG Source	Add, modify, or delete an MPEG source.

VASP	Add, modify, or delete a VASP entry. Verify your VASP Configuration.
STA	The international system does not use a synchronous optical network (SONET)-to-ASI interface.
SONET	The international system does not use SONET.
UpConverter	The international system does not use UpConverters.
SCS	• Set up PCG/SCS pairs. • Add an SCS element. • Modify SCS ports. • Modify SCS modeling parameters. • Delete an SCS element.
PCG	• Set up PCG/SCS pairs. • Add, modify, or delete a PCG.
Table-Based QAM	The international system does not use table-based QAM modulators.
SMDG	The international system does not use stat mux dejitter groups (SMDGs).

Back to top

Home Element Provisioning Sub-Tab

Quick Path:
DNCS Administrative Console > DNCS tab > Home Element Provisioning tab

The **Home Element Provisioning** sub-tab on the DNCS tab allows you to manage the devices deployed within a subscriber's home.

Back to top

DHCT Provisioning

The **DHCT Provisioning** area has five buttons that allow you to work with the DHCTs in your system as described in the following table. You may find the *Downloading New Client Application Platform Software Installation Instructions* useful for more information on using this part of the DNCS.

Important: Except for testing purposes, you should set up (stage) the DHCTs in your system as described in the *Explorer Digital Home Communications Terminal Staging Guide*.

See **Printed Resources** for information on obtaining these guides.

This button...	Allows you to perform these tasks...
Type	• View a list of the DHCT types contained in your DNCS database, along with the revision level and OUI for each. • Add, modify, or delete a DHCT type. • Associate software TOC files with or unassociate them from specific types of DHCTs.
DHCT	• Add, modify, or delete an individual DHCT. • Send service or system information to an individual DHCT within a few minutes. • Assign service packages to an individual DHCT. • Enable an individual DHCT to display secure analog, and PPV services.
Boot Page	The international system does not use this feature.
OS	The international system does not use this feature.
Image	• Load the DHCT resource file (settop.res) into the DNCS database. • Record the current set of image files on your system. • Load image files onto the BFS. • Create a test group of DHCTs. • Set up and download client software to DHCTs on your system that use the CVT method. • Force an immediate download of client software to DHCTs that use the CVT method.

Back to top

CableCARD Provisioning

The international system does not use CableCARD modules.

Back to top

Utilities Sub-Tab

Utilities Sub-Tab

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab

The **Utilities** sub-tab on the DNCS tab allows you to perform a variety of useful tasks as described in the following table.

This button...	Allows you to perform these tasks...
Tracing	Set the tracing level for each DNCS process so that you can define how much debugging information is displayed in the dncsLog file for each process.  **Important:** Unless you are using tracing for a specific reason, we recommend that you leave all of your DNCS tracing levels to set to the default, 0 (zero). Contact our technical support if you need help setting your DNCS tracing levels.
Logging	Access the Logging utility to fine-tune log levels for processes and their libraries. For more information, see Logging Utility.
Session List	Control sessions and resources within the network. For more information, see Session List.
Reports	Run various reports to see how the system is functioning. For more information, see the *Report Writer Version 4.3 for DNCS and ISDS User Guide*. To obtain this guide, see **Printed Resources**.  **Note:** The international system does not use all of the reports this feature provides.
GUI Servers	• See the location of a particular web user interface (UI) server file. • Modify the web UI application name, server name, and server port. • View the status of a web UI server (for example, *active*). If the server does not respond to a system request for its status, the display indicates a status of *unknown*. • Stop or restart a web UI server. For more information, see UI Server Manager.
Performance Monitoring	Display system performance data in a graphical format, such as a line chart. For more information, see Performance Monitoring.
xterm	Open an xterm window to perform troubleshooting activities.

Back to top

Opening an xterm Window

An xterm window gives you enter UNIX commands to manipulate, view, and edit various program files within the DNCS operating system.

Complete these steps to open an xterm window on the DNCS workstation.

1. On the DNCS Administrative Console, click the **Utilities** tab.
2. Click **xterm**. An xterm window opens and displays a user prompt.

Back to top

Application Interface Modules Tab

Quick Path:
DNCS Administrative Console > DNCS tab > Application Interface tab

The **Application Interface Modules** tab on the DNCS Administrative Console provides an interface between the server applications and the DHCTs as described in the following table.

This button...	Allows you to perform these tasks...
BFS Admin	Modify BFS servers, sources, and hosts. **Important:** Unless we direct you to do so, do not modify BFS servers, sources, or hosts. Modifying these elements without our assistance may cause the system to become unstable.
BFS Client	The international system does not use this feature.
SAM Service	Register services with the SAM when setting up PPV services.
Channel Maps	The international system does not use this feature.
SAM Config	The international system does not use this feature.
Group Definitions	The international system does not use this feature.
Non-Channel Services	The international system does not use this feature.
Client Filters	The international system does not use this feature.

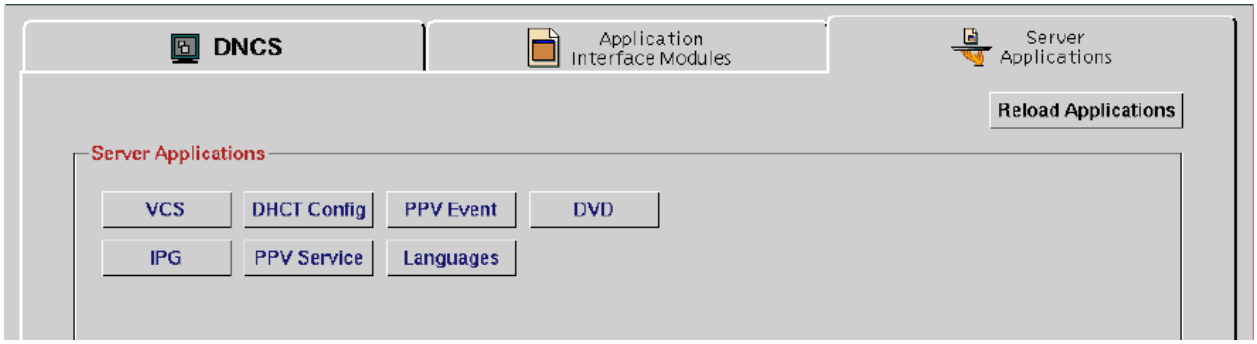
Back to top

Server Applications Tab

Quick Path:
DNCS Administrative Console > DNCS tab > Server Applications tab

The **Server Applications** tab on the DNCS Administrative Console provides access to applications that reside on the SARA Server so that you can configure services associated with SARA applications. The options that appear on this tab vary depending on the applications available on your system. The following illustration provides some examples of options you might see on this tab. Refer to the *Configuring the PowerKEY DVB System For System Release i4.3* for more information. To obtain this guide, refer to **Printed Resources**.

Note: The international system does not use the features provided by the VCS, EPG, Languages, or DVD buttons.



Back to top

Setting Up Your Network
Network Setup Overview

Setting Up Your Network
The first step in managing the elements in your network is to set up the DNCS software so that it recognizes and can communicate with those elements. You do this by entering information about each element into the DNCS database.

In most cases, we set up your network hardware and services in the DNCS for you. However, if you need to set up your network yourself, you can use these procedures. You can also use these procedures if you need to add elements to an existing network.

Note: When we first install your system, we configure the routes that are needed for all of the network elements to communicate with each other. However, if you add new network elements, new routes will need to be configured. In this case, we encourage you to have a service agreement or other means available for having these routes configured by qualified personnel.

Back to top

Before You Begin
Before you set up your network in the DNCS, you must do the following:

- Make sure that all the hardware to be managed by the DNCS is physically installed in your system
- Have your network map readily available. If you cannot locate your network map(s), contact technical support.

Back to top

Set Up Your Network
Important

- Unless noted otherwise, the steps listed below can be used for any type of system, standard or custom.
- If you are setting up your network for the first time, you must complete ALL of these procedures in the order listed.

Complete these procedures to set up your network elements:

1. Get your network map; you will refer to it frequently throughout this process.
2. If your system uses a SARA server, set up the SARA server.
3. Set up the SI-Server using the ROSA Element Manager.

   Note: Refer to the following manuals for instructions using ROSA Element Manager. To obtain a copy of either manual, see Printed Resources.

   - *SI-Server Complete SI Solution User Manual*
   - *ROSA Network Management System User's Guide*
4. Set up the following logical elements in your system by adding them to your network:

- Headends
- Hubs
- OIT bridges

5. Set up the following elements that process system data for your system:
   - Set up the Direct ASI link.
   - VASP entries
6. Set up the following elements according to your system configuration:
   - Sites using PowerKEY technology, MQAM Content elements
   - Sites using SimulCrypt technology, PCG/SCG pairs
7. Set up the DHCTs in your network.

   Note: As part of this process, you will set up channel maps for the services and, if needed, bouquet allocation tables (BATs).
8. Set up your services (clear, secure, PPV, and so on).
9. Record any changes you made to your network on your network map.

Back to top

Network Map

Network Maps

When we install a network, we prepare customized network maps (sometimes called "spider diagrams") that provide detailed information about the equipment layout of the site. After your equipment was installed, the installer should have given your system administrator a Network Planning Package. One of the items in that package is a copy of your network map.

Depending on your system, you may have several maps for your network. Keep your network map(s) readily available when you are using the DNCS to manage your network. If you cannot locate your network map(s), contact technical support.

Note: If you are setting up your DBDS network yourself, you must create your own network map(s).

Naming and Numbering Scheme

Updating Network Maps

Back to top

Naming and Numbering Scheme

Important: Each name must be unique for each piece of equipment within your system.

When you look at your network map, you will notice that each hardware element is labeled with a unique IP address, MAC address, and name. You may also see individual transport streams identified.

Note that there is a pattern to the naming and numbering scheme for these elements. The pattern may be as simple as numbering the individual elements, such as MQAM 1, MQAM 2, and so on. Conversely, the pattern may be more specific by identifying the function or location of each element, such as VODQAM.

When you make additions or changes to your network, we strongly recommend that you use a naming and numbering scheme that follows the scheme used in your network map. Doing so will make it easier for you to identify where individual elements are located within your network, as well as what specific data is coming from and going to those elements. Additionally, you will be less likely to duplicate element names within your system, which can cause numerous data transport errors.

Back to top

Updating Network Maps

Whenever you make a change to your network, update your network map. This will allow you to troubleshoot your system more effectively and efficiently, should the need arise.

Back to top

Set Up Network Elements

Setting Up Network Elements

Refer to the following topics for assistance in setting up elements used in a typical DBDS.

- **SARA Server** (if used)
- **SI-Server and D96xx Re-Multiplexers**
- **Headends**
- **Hubs**
- **OIT Bridge** (one per system)
- **Direct ASI Link**
- **VASP Entry**
- Choose either of the following, depending on your system configuration:
  - For sites that do not use SimulCrypt technology, set up **MQAM Content Modulators**.
  - For sites using SimulCrypt technology, set up **PCG/SCS Pairs**.
- **DHCTs**

Back to Top

SARA Server

Online Help is not available for our Resident Application (SARA) server. If you have questions about the SARA server, refer to *Configuring the PowerKEY DVB System For System Release i4.3*. To obtain a copy of this document, see **Printed Resources**.

Set Up the SI-Server, the D96xx Re-Multiplexers, and the DCM

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

Back to top

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

Complete these steps to configure the SI-Server and the D96xx re-multiplexers.

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*

   Note: To obtain copies of either document, see **Printed Resources**.

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 on configuring the D96xx re-multiplexers. To obtain a copy of this document, go to **Printed Resources**.

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.

   Note: Refer to this step after you configure Direct ASI and the OIT bridges.

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.

Back to top

Logical Elements

Adding a Headend

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Headend > File > New

The first logical element you must set up in your network is a headend. You can add an unlimited number of headends to the DNCS.

A headend is a logical element that represents a group of MQAM modulators that provide services to a particular group of DHCTs.

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Add a Headend

Complete these steps to add a headend to your network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Headend**. The Headend List window opens.
4. Click **File > New**. The Set Up Headend window opens.

5. Click in the **Headend Name** field and type the name you will use to identify this headend (for example, **HE1**). 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 **Save**. The system saves the headend information in the DNCS database and closes the Set Up Headend window. The Headend List updates to include the new headend.

7. Add the new headend to your network map.

8. Do you need to add another headend?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **File > Close** to close the Headend List window and return to the DNCS Administrative Console. Go to **Adding a Hub**.

Back to top

Hubs

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub

After you add a headend to the DNCS database, you must assign at least one hub to that headend. You can have an unlimited number of hubs per headend. 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 disabled and network binding disabled
- Distributed DNCS disabled and network binding enabled
- Distributed DNCS enabled and network binding disabled
- Distributed DNCS enabled and network binding enabled

Choose your system configuration and then follow the procedure for that configuration for creating, modifying, or deleting a hub.

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

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 set-top will display an "unauthorized" barker and will not boot. 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 it is associated with. Then the package can be deleted.

Back to top

Configuration 1: Distributed DNCS Disabled and Network Binding Disabled

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub

Creating New Hubs

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub List window opens.
4. From the Hub List window, select **File** and choose **New**. The Set Up Hub window opens.
5. Click the **Headend Name** arrow and select a headend name from the list.
6. 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.

7. Click in the **Network ID** field and type a unique Network ID for the hub.

   Important: The suggested Network ID is 48059 (0xBBBB hex).

   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.

8. 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.

9. 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.

10. Add the new hub to your network map.

11. Do you need to add another hub?
    - If **yes**, repeat steps 4 through 9.
    - If **no**, click **Exit** to close the Hub List window.

12. Are you are setting up your network for the first time?
    - If **yes**, your next step is to set up an OIT Bridge. Go to **Adding an OIT Bridge**.
    - If **no**, continue making any other changes that you need to make to your network.

Back to top

Modifying a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Make Changes] > Save > OK

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

- Hub name
- Network ID

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**.

1. On 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**.

8. Click **OK**. The Hub List window updates to include the new hub information. DHCTs receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a DHCT causes it to apply updates immediately.

9. Update your network map to reflect these changes.

10. Do you need to modify another hub?
    - If **yes**, repeat steps 4 through 8.
    - If **no**, click **File** and select **Close** to close the Hub List window.

11. 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.

Back to top

Deleting a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Select Hub] > Delete Selected Hub > OK

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.

1. Are there any node sets associated with this hub?
    - If **yes**, delete those node sets first. Go to **Deleting a Node Set**. When finished, return to this procedure.
    - If **no**, go to step 2.

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

3. Click the **Network Element Provisioning** tab.

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

5. Click the **Select** button next to the hub that you want to delete.

6. Click **Delete Selected Hub**. A confirmation message opens.

7. Click **OK**. The message closes. The system removes the hub information from the DNCS database and from the Hub Summary window.

8. Delete the hub from your network map.

9. Do you need to delete another hub?
   - If **yes**, repeat steps 1 through 8.
   - If **no**, click **Exit** to close the Hub Summary window.

10. Continue making any other changes that you need to make to your network.

Back to top

Configuration 2: Distributed DNCS Disabled and Network Binding Enabled

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub

Creating New Hubs

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub List window opens.
4. Click **File > New**. The Set Up Hub window opens.
5. Click the **Headend Name** arrow and select a headend name from the list.
6. 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.

7. Click in the **Network ID** field and type a unique Network ID for the hub.

   Important: The suggested Network ID is 48059 (0xBBBB hex).

   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.

8. 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.

9. 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.

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

10. Add the new hub to your network map.

11. Do you need to add another hub?
    - If **yes**, repeat steps 4 through 10.
    - If **no**, click **Exit** to close the Hub List window.

12. Are you are setting up your network for the first time?
    - If **yes**, your next step is to set up an OIT Bridge. Go to **Adding an OIT Bridge**.
    - If **no**, continue making any other changes that you need to make to your network.

Back to top

Modifying a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Make Changes] > Save > OK

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**.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. 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 modify.
5. Click **File** and choose **Open**. The Set Up Hub window opens for the hub you selected.
6. 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.

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

Results:

- The Hub List window updates to include the new hub information.
- DHCTs receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a DHCT causes it to apply updates immediately.

8. Update your network map to reflect these changes.

9. Do you need to modify another hub?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **File** and select **Close** to close the Hub List window.

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.

Back to top

Deleting a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Select Hub] > Delete Selected Hub > OK

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.

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to **Deleting a Node Set**. When finished, return to this procedure.
   - If **no**, go to step 2.

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

3. Click the **Network Element Provisioning** tab.

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

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

6. Click **File** and then choose **Delete Selected Hub**. A confirmation message opens.

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

8. Delete the hub from your network map.

9. Do you need to delete another hub?
   - If **yes**, repeat steps 1 through 8.
   - If **no**, click **Exit** to close the Hub List window.

10. Continue making any other changes that you need to make to your network.

Back to top

Configuration 3: Distributed DNCS Enabled and Network Binding Disabled

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub

Creating New Hubs

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub Summary window opens.
4. Click **Add Hub**. An empty row is added to the user interface.
5. Enter the correct **Hub Name** and **Network ID** in the blank fields.
6. Select the headend for this hub.

7. 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.

8. Add the new hub to your network map.

9. Do you need to add another hub?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **Exit** to close the Hub Summary window.

10. Are you are setting up your network for the first time?
    - If **yes**, your next step is to set up an OIT Bridge. Go to **Adding an OIT Bridge**.
    - If **no**, continue making any other changes that you need to make to your network.

Back to top

Modifying a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Make Changes] > Save > OK

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

- Hub name
- Network ID

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**.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub Summary window opens.
4. Click the **Select** button next to the row containing the hub you want to modify.
5. Click **File** and choose **Open**. The Set Up Hub window opens for the hub you selected
6. 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.

7. When you finish making changes, click **Save**.
8. Click **OK**. The Hub Summary window updates to include the new hub information. DHCTs receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a DHCT causes it to apply updates immediately.
9. Update your network map to reflect these changes.
10. Do you need to modify another hub?
    - If **yes**, repeat steps 4 through 8.
    - If **no**, click **File** and select **Close** to close the Hub List window.
11. 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.

Back to top

Deleting a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Select Hub] > Delete Selected Hub > OK

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.

1. Are there any node sets associated with this hub?
   - If **yes**, delete those node sets first. Go to **Deleting a Node Set**. When finished, return to this procedure.
   - If **no**, go to step 2.

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

3. Click the **Network Element Provisioning** tab.

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

5. Click the **Select** button next to the hub that you want to delete.

6. Click **Delete Selected Hub**. A confirmation message opens.

7. Click **OK**. The confirmation message closes. The system removes the hub information from the DNCS database and from the Hub Summary window.

8. Delete the hub from your network map.

9. Do you need to delete another hub?
   - If **yes**, repeat steps 1 through 8.
   - If **no**, click **Exit** to close the Hub Summary window.

10. Continue making any other changes that you need to make to your network.

Back to top

Configuration 4: Distributed DNCS Enabled and Network Binding Enabled

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub

Creating New Hubs

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

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

3. 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.

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

5. 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.

6. Select the headend for this hub.

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

8. Add the new hub to your network map.

9. Do you need to add another hub?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **Exit** to close the Hub Summary window.

10. Are you are setting up your network for the first time?
    - If **yes**, your next step is to set up an OIT Bridge. Go to **Adding an OIT Bridge**.
    - If **no**, continue making any other changes that you need to make to your network.

Back to top

Modifying a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Make Changes] > Save > OK

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

- Hub name
- Network ID
- 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**.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. 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.

4. Click the **Select** button next to the row containing the hub you want to modify.

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**.

   Notes:

   - The Hub List window updates to include the new hub information.
   - DHCTs receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a DHCT causes it to apply updates immediately.

7. Update your network map to reflect these changes.

8. Do you need to modify another hub?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **File** and select **Close** to close the Hub List window.

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.

Back to top

Deleting a Hub

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub > [Select Hub] > Delete Selected Hub > OK

You may want to delete a hub because you are no longer 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. Go to **Deleting a Node Set**. When finished, return to this procedure.
   - If **no**, go to step 2.

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

3. Click the **Network Element Provisioning** tab.

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

5. Click the **Select** button next to the hub that you want to delete.

6. Click the link **Delete Selected Hub**. A confirmation message opens.

7. Click **OK**. The confirmation message closes. The system removes the hub information from the DNCS database and from the Hub Summary window.

8. Delete the hub from your network map.

9. Do you need to delete another hub?
   - If **yes**, repeat steps 1 through 8.
   - If **no**, click **Exit** to close the Hub Summary window.

10. Continue making any other changes that you need to make to your network.

Back to top

Adding an OIT Bridge

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QPSK/CMTS/OIT > File > New > CMTS/OIT

After you add a hub to a headend, you must add at least one Out-of-Band/InBand Translator (OIT) bridge to that hub if the hub provides services to broadcast-only DHCTs. (Broadcast-only DHCTs have no QPSK tuner.)

An OIT bridge provides OIT data to D96xx re-multiplexers, including the Home D96xx Re-Multiplexer. OIT data is encapsulated into MPEG transport streams that are written to an ASI card on the DNCS. The OIT data stream shares the Direct ASI card with the Home Transport and OSM streams. The OIT data for broadcast-only DHCTs consists of Entitlement Management Messages (EMMs), Global Broadcast Authentication Messages (GBAMs), UNPassthru and UNConfig messages.

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

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Procedure

Complete these steps to add an OIT bridge set to your network.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QPSK/CMTS/OIT**. The QPSK/CMTS/OIT List window opens.

4. Click **File > New > CMTS/OIT**. The Set Up CMTS/OIT Bridge window opens.

Important:

- All bridges on the RNCS must be virtual IP addresses (including the first one).
- 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. Go to Configuring Virtual IP Addresses.

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

5. Click the **Hub** arrow and select the hub associated with this OIT bridge.

6. Click in the **Bridge Name** field and type the name you will use to identify this node set (for example, **HE1_Hub1_OIT1**). You can use up to 20 alphanumeric characters.

Note: Be sure to use a name that contains no spaces and that is consistent with the naming scheme used on your network map.

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

8. In the **IP Address** field, enter the IP address of the local host. We recommend that you use the following address: 127.0.0.1.

9. Click the **DCM** arrow and select **Mixed DOCSIS/DAVIC**.

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 opens.

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

- 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.

- 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.

- 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.

- 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).
- In the **PID** column, click in the **Messaging** field and type the hexadecimal PID value for the Messaging stream. Allowable values=0x20-0x25.
- In the **Dncs ASI Pid** column, click in the **EMM** field and type the hexadecimal PID value for the PowerKEY EMM stream.
- 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.
- In the **Dncs ASI Pid** column, click in the **System Messages** field and type the hexadecimal PID value for the System Messages stream.
- In the **Dncs ASI Pid** column, click in the **CAT** field and type the hexadecimal PID value for the CAT stream. Allowable values=0x20-0x25.
- In the **Dncs ASI Pid** column, click in the **Messaging** field and type the hexadecimal PID value for the Messaging stream. Allowable values=0x20-0x25.
- 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.
- 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.
- 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.
- 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.
- In the **Max Data Rate** column, click in the **Messaging** field and type the maximum data rate for this stream in Mbps. Allowable values=0.01 – 1.0 Mbps.

13. Click **OK** The Set up CMTS/OIT Bridge window closes and the OIT bridge is listed in the QPSK/CMTS/OIT List window.

14. Click **File > Close** to close the QPSK/CMTS/OIT List window and return to the DNCS Administrative Console. Go to step 15.

15. Are you setting up your network for the first time?
    - If **yes**, your next step is to set up the elements that process system data for your network by setting up a Direct ASI Link. Go to **Direct ASI Overview**.
    - If **no**, continue making any other changes that you need to make to your network.

Back to top

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.
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

12.

- 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

12.

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 virtual IP addresses.

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 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 (based on availability) 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:

<ip address><tab space><hostname>

Notes:

1.
- The <ip address> 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**).
- An example row would be:
10.78.192.01 dncsv1

9. Plumb the virtual interface using the following command

1. **Ifconfig plumb <virutual Interface>**
2. **Example:**

Ifconfig plumb ce1:1

10. 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

11. Repeat this entire procedure for each RNCS.

Direct ASI, MPEG Sources, and MQAM Modulators

Direct ASI Overview

The Direct ASI feature delivers data directly from the DNCS to the MQAM modulators and SCS using an ASI link. This section provides an overview of the procedures for setting up Direct ASI for the first time.

Note: Our engineers configure your DNCS to support Direct ASI when they upgrade your system. Because our engineers perform these tasks for you, you should not need to configure your DNCS for Direct ASI. However, the procedures given here can help you understand how a DNCS is configured to support Direct ASI. This knowledge may be helpful in monitoring and managing your DBDS.

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Process Overview

To set up the Direct ASI feature, you must complete the following steps. For step-by-step instructions for a particular task, click on that task.

1. Add an MPEG Home Transport source for the ASI card.

   Notes:

   - You must create a source for the Home D96xx Re-Multiplexer, which receives data input from the Direct ASI output on the PowerKEY DVB system.
   - At this point you can also create MPEG sources for the D96xx Re-Multiplexers in your system.

0. Add a Home Transport MQAM modulator to the DNCS.

   Note: At this point you can also create elements for the other MQAM modulators in your system.

3. Configure Direct ASI cards.
4. Confirm Direct ASI mode.
5. Set up Home Transport MPEG sessions.

Back to top

Add MPEG Sources

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > File > New

After you add an OIT bridge, add MPEG sources to the DNCS. Each MPEG source represents a D96xx Re-multiplexer. You must create an MPEG source for every D96xx Re-multiplexer in the system, including the D69xx that you have identified as the "Home D96xx Re-multiplexer." The Home D96xx Re-multiplexer receives BFS data input from the Direct ASI output.

Back to top

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, contact technical support. You must also have the following information, which should be noted on your network map:

- Name of the headend containing the ASI card
- A name that will identify each MPEG source as one that is used for the ASI card (We recommend that you use the name HT_ASI.)
- The IP address for D96XX (from your system administrator)
- Physical (MAC) address for the D96xx that is being used for scrambling
- Number identifying the output port on the MPEG source that is logically connected to the input port on the D96xx
- Number identifying the transport stream going from the MPEG source to the MQAM modulator/SCS

Back to top

Process Overview

To add an MPEG source to the D96xx Re-Multiplexer, complete the following tasks.

1. Set up the basic parameters for the MPEG Source.
2. Set up the connection from the MPEG source to the D96xx Re-Multiplexer.

Back to top

Setting Up MPEG Source Parameters

The first step in adding an MPEG source is to set up the basic parameters for the MUX as described in the following steps.

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

4. Click **File > New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.
5. Click the **Headend Name** arrow and select the headend associated with the D96xx Re-Multiplexer.
6. Click in the **MPEG Source Name** field and type the name of this MPEG source (for example, **MUX_101)**. You can use up to 20 alphanumeric characters.
7. Click the **Device Type** arrow and select **MUX** as the type of MPEG source you are adding.

Note: If MUX does not appear in the list of device types, click in the **Device Type** field and enter **MUX**.

8. Click in the **IP Address** field and type the IP address for the Home D96xx Re-Multiplexer. Be careful to properly place the dots (**.**) between numbers.

Note: You can locate this IP address from the front panel LCD on the Home D96xx Re-Multiplexer.

9. Click in the **Physical Address** field and type the MAC address for the Ethernet port on the Home D96xx Re-Multiplexer that is being used to receive ASI data from the ASI card on the DNCS.

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.

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

11. Your next step is to set up the connection from the MPEG source to the MQAM/SCS. Go to **Setting Up MPEG Source Connections**.

Back to top

Setting Up MPEG Source Connections

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

1. On the Set Up MPEG source window, click the **Connectivity** tab. The Connectivity window opens.

Note: Because no devices are connected yet, the illustration field is 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** 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) in the Port Number field.

4. Click in the **Transport Stream ID** field and type a number to represent the transport stream going from this MPEG source to the MQAM modulator/SCS. This number must correspond with the ASI input (usually on your network map) on the associated MQAM modulator/SCS. See **Source and Service Naming Conventions** for the correct naming and numbering conventions.

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

5. Click the **Transport Protocol** arrow and select **ASI** as the type of output that feeds the MQAM modulator/SCS.

6. Click **OK**. 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 MQAM modulator/SCS that the Re-Multiplexer connects to, the system will automatically complete the Connect To fields on this window.

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

8. Click **Save**. 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. Add the new MPEG source to your network map.

10. Your next step is to add the MQAM modulator/SCS that will be receiving data from this MUX. Choose either of the following depending on your system configuration:

- For sites that do not use SimulCrypt technology, go to **Add an MQAM Modulator**.
- For sites using SimulCrypt technology, go to **Set Up PCG/SCS Pairs**.

Back to top

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 MQAM Modulators

Add an MQAM Modulator

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > File > New > MQAM

After you have added an MPEG source to the DNCS and if you are using MQAM modulators to receive source data, add MQAM modulators to the DNCS. When adding MQAM modulators to your system, you will add an MQAM modulator to receive Home Transport data from the Home D96xx Re-multiplexer. The Home Transport MQAM Modulator modulates the data onto an RF carrier, and then sends it downstream on the inband data path to all DHCTs in the headend. Do not change the transport frequency established for this MQAM modulator.
Under normal operating conditions, the Home Transport Frequency should not be changed. Changing the frequency can cause the QAM frequency to be modified in the Set Up QAM window on the DNCS; but it will not be updated in the DNCS database. As a result, the set-top begins to search for the correct frequency and possibly locks on to an incorrect frequency.
Workaround: Should the home transport frequency be changed, disable the bootloader session in the BFS Admin console, tear down the OSM session (199), change the home transport frequency, and then enable the bootloader session in the BFS Admin console. For assistance, contact technical support.

Important: Each headend in your network must have a Home Transport MQAM modulator associated with an ASI card on the DNCS. Otherwise, some DHCTs in your network will not receive BFS data from that headend.

Note: If your system uses a PCG, go to **Add a PCG**.

Back to top

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, contact technical support. 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)
- Subnet mask for the MQAM modulator (from your system administrator)
- MAC address for the MQAM modulator (click for information on locating the MAC address)
- Numbers identifying the two transport streams going from the MQAM modulator out to the hubs in your system
- Type of modulation and symbol rate standard the MQAM modulator uses, such as ITU J.83 Annex A
- Frequency of the channels being used to send data from the MQAM modulator to the hubs on your system
- Numbers identifying the input ports on this MQAM modulator that are physically connected to the associated MPEG source
- Name of the headend containing the MPEG source for the MQAM modulator
- Type of MPEG source devices being used to send data to this MQAM modulator (for example, ASI)
- Name of the associated MPEG sources
- Numbers identifying the output ports of the associated MPEG sources that are physically connected to the input ports 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.

Back to top

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add an MQAM modulator to the DNCS, you must complete the following tasks in order.

1. Set up the MQAM modulator basic parameters.
2. Set up the MQAM modulator connection to the MPEG source.
3. Activate the MQAM modulator.

Back to top

Setting Up MQAM Modulator Basic Parameters

The first step in adding an MQAM modulator is to set up the MQAM modulator basic parameters. Complete these steps to set up the basic parameters for a MQAM modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click **File > New > MQAM**. The Set Up MQAM window opens with the Basic Parameters tab in the forefront.
5. Click the **Headend Name** arrow and select the headend in which this Home Transport MQAM modulator resides.
6. Click in the **QAM Name** field and type the name you will use to identify this Home Transport MQAM modulator (for example, **HE1HTMQAM**). 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.

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

8. Click the **Modulation Type** arrow, and select the type of modulation standard this modulator uses. For example, if this is a 256 MQAM modulator that uses ITU A modulation, you should select ITU J.83 Annex B (8 MHz).

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

10. 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.

11. If your system uses a default gateway, click in the **Default Gateway** field and enter the IP address of your default gateway.

Note: Using a default gateway speeds up the reconnection process that occurs after a Home Transport MQAM modulator is rebooted.

12. You do not need to enter ASI INPUT Transport Stream IDs. The system sets up these values automatically when the corresponding transport stream IDs are set up in the MPEG sources and the connections are later established on the Connectivity tab.

13. For each RF output, complete these fields:
    - Click the **Modulation** arrow and select the type of modulation this Home Transport MQAM modulator uses. For example, if this modulator uses 256 QAM, you should select 256-QAM.
    - Click in the **Transport Stream ID** field and type a unique number to identify the transport stream going from this Home Transport MQAM modulator out to the hubs on your system. You can use up to 5 numeric characters.

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

- Click in the **Channel Center Frequency (MHz)** field and type the frequency of the channel you will use to send data from this Home Transport MQAM modulator to the hubs on your system. We recommend that you enter a value in 8 MHz increments from 108 to 858.

14. Under normal operating conditions, the following options are disabled. However, under some circumstances, such as the examples listed here, enabling these options is helpful:
    - Enable the **Continuous Wave Mode** option to produce an unmodulated RF carrier that is useful in taking measurements. Enabling this option is useful when performing testing.
    - Enable the **Mute RF** option to turn off the RF output for a port. Enabling this option is helpful when installing the modulator.
    - Enable the **Disabled** option to prevent the DNCS from setting up any additional sessions on an RF output port. (Existing sessions are not affected and continue to function as expected.) Enabling this option may be helpful when performing plant maintenance or in the rare event that a port fails.

15. Do not change the setting for the symbol rate setting.

Important: The symbol rate for transport streams carrying data from the Home D96xx Re-Multiplexer must remain at 6.900 Ms/s.

16. Is the **Spectral Inversion** setting enabled?
    - If **yes**, clear the selection and continue with the next step.
    - If **no**, continue with the next step.

Important: The recommended Spectral Inversion setting is *disabled*.

17. Click **Apply**. The system saves the information you have entered thus far into the DNCS database and enables the Port to Hubs button and the Connectivity tab.

18. Click the **Port to Hubs** button for the first transport stream. The RF Output Port window opens and the Basic Parameters area of this window shows the data that you entered for key RF output fields. The Associate Hubs area shows the hubs that are available to receive content data from this Home Transport MQAM modulator.

19. Define which hubs will receive Home Transport data from a transport stream as follows:
    - To send data from this MQAM modulator to only specific hubs in the headend, select the hub name in the **Available Hubs** field, and then click **Add**. The hub name moves into the Selected Hubs field. Repeat this step for each hub you want to receive data from this Home Transport MQAM modulator.
    - To send data from this Home Transport MQAM modulator to all hubs in the headend, make sure no hubs appear in the Selected Hubs field.

Note: To remove a hub from the Selected Hubs field, select the hub name, and then click **Remove**. The hub name moves into the Available Hubs field.

20. Click **Save**. The system saves this information into the DNCS database and closes the RF Output Port window.

21. To define the hubs that will receive Home Transport data from the second transport stream on the Home Transport MQAM modulator, click the second **Port to Hubs** button and repeat steps 19 and 20.

> **Important:** Do *not* change information in the Advanced Parameters tab without first consulting technical support. Changing this data without direction from technical support can degrade system performance. You should not need to use the Advanced Parameters tab because the system automatically configures these settings for you. These settings tell a modulator which version of software to use.

22. Because the system automatically sets up advanced parameters, you do not need to complete any fields on the Advanced Parameters tab. Your next step is to set up the connections between the MQAM modulator and the MPEG source on the DNCS. Go to **Setting Up MQAM Modulator Connections**.

Back to top

Setting Up MQAM Modulator Connections

After you set up the basic parameters for a MQAM modulator, complete these steps to set up the connections between the MQAM modulator and the MPEG source.

1. On the Set Up QAM window, click the **Connectivity** tab. The Connectivity window opens with an illustration of the devices already connected to this MQAM modulator.
2. If not already selected, click to select **Input Port 1** option in the **QAM Name** area.
3. In the **Connect To** area, click the **Headend Name** arrow and select the headend in which the device that feeds this MQAM resides.
4. Click the **Device Type** arrow and select **MUX**.
5. Continue defining connections to the MUX by completing the following tasks.
   - 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.
   - Click the **Port Number** arrow and type **1**.
6. Click to select **Input Port 2** option in the **QAM Name** area and repeat steps 4 and 5 to set up the second input port.
7. Click **Apply**. The system saves this information into the DNCS database.
8. Your next step is to activate this MQAM modulator. Go to **Activating an MQAM Modulator**.

Back to top

Activating a MQAM Modulator

After you set up the connections between the MQAM modulator and the device that feeds it, complete these steps to activate the MQAM modulator.

Note: You can activate a 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 window opens.
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**. 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 modulator. The MQAM modulator is listed two times in the window to show its two output streams.
5. Add the new MQAM modulator to your network map.
6. If this MQAM modulator is the Home Transport MQAM modulator, go to **Configure the Direct ASI Cards**.
7. Do you need to add another MQAM modulator?
   - If **yes**, go back to **Setting Up MQAM Modulator Basic Parameters**.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console. Continue making any other changes that you need to make to your network.

Back to top

Locate the MAC Address of an MQAM Modulator

You can look at the sticker on the side of the MQAM modulator to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator in question.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

Back to top

Reset an MQAM Modulator

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [Select an MQAM modulator] > File > Reset

Important: Do not attempt to modify or delete a Home Transport MQAM modulator without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to the Home Transport MQAM modulator. For assistance, contact technical support.

Resetting an MQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

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

2. When the QAM List window opens, click to select the MQAM modulator that you want to reboot.

   Notes:
   - Each MQAM modulator is listed two times (once for each of the modulator's two RF output channels), but select only the first occurrence.

3. Click **File** and then select **Reset.** The Question window appears with the question, **Are you sure you want to reset QAM modulator 'name of modulator'?**

4. Click **Yes**. The QAM List window displays the following message: **The reset request has been received by QAM modulator 'name of modulator.'**

Back to top

Configure the Direct ASI Cards

Quick Path:
DNCS Administrative Console > Applications Interface Modules tab > BFS Admin > Hosts tab

The PowerKEY DVB System uses Direct ASI input to an ASI card installed in the DNCS to transmit ASI data streams from the DNCS directly to re-multiplexers using an ASI link. This page provides instructions for configuring Direct ASI cards to deliver BFS data to the Home D96xx Re-multiplexer. The Home D96xx receives data input from the Direct ASI output on the PowerKEY DVB System.

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Configuring the Direct ASI Cards

Complete these steps to configure the Direct ASI cards to deliver data to the Home D96xx Re-multiplexer.

1. From the DNCS Administrative Console, click the **Applications Interface Modules** tab.
2. Click **BFS Admin**. The BFS Admin Sites window opens.
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.
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**, and then go to step 9.
9. Does the transport stream (TS) ID shown in the Transport Stream ID field match the Home SCS/MQAM TS ID 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 that corresponds to the MQAM/SCS device output. The value for this field will be the value of the output TSID found on the SCS ports page. For additional details, see Setting Up SCS Ports Modeling Parameters.

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 opens.

16. In the BFS Administration window, double-click the **bootloader** source. A Set Up BFS Source window opens, and displays information about the bootloader source.

17. Verify the following information for the bootloader source:
    - If the Source is not enabled, select **enable**.
    - If **dncsatm** is not listed in the Selected Hosts field, move it from the Available Hosts field to the Selected Hosts field.

18. 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.

19. In the Site DNCS BFS Administration window, click **File** then select **Close** to close the window.

20. Continue setting up the Direct ASI feature by ensuring that the DNCS is in Direct ASI mode. Go to **Confirm Direct ASI Mode**.

Back to top

Confirm Direct ASI Mode

Quick Path:
DNCS Administrative Console > Applications Interface Modules tab > BFS Admin > Hosts tab > dncsatm

The PowerKEY DVB System uses Direct ASI. This section provides a procedure for confirming that the Direct ASI mode is enabled on your system. It also includes instructions for enabling Direct ASI mode if necessary.

Back to top

Confirming Direct ASI Mode

Complete these steps to confirm that your system is in Direct ASI mode, and to enable Direct ASI mode if necessary.

1. From the DNCS Administrative Console, click the **Applications Interface Modules** tab.

2. Click **BFS Admin**. The Site DNCS BFS Administration window opens with the Servers tab in the forefront.
3. From the Site DNCS BFS Administration window, click the **Hosts** tab.
4. Double-click **dncsatm** in the Host Name field. The Set Up BFS Host window opens.
5. Are the selections in the Set Up BFS Host window dimmed?
   - If **yes**, go to step 6.
   - If **no**, you must enter the correct parameters. For the correct parameters, go to step 5 of **Configure the Direct ASI Cards**. When you have finished entering the correct parameters, continue with step 8 of this procedure.
6. From the Set Up BFS Host window, select **ASI**. The system switches to Direct ASI mode. Go to **Configure the Direct ASI Cards**.
7. Do not select PAT Configuration. This configuration is for expert diagnostic support only.
8. Click **Save**. The system saves your settings.
9. Your next step is to tear down (delete) and rebuild the Home Transport sessions. Go to **Set Up Home Transport Sessions**.

Back to top

Obtain BFS MPEG Program Numbers

Quick Path:
DNCS Administrative Console > Utilities tab > Session List > Session Filter > Broadcast File System > Display Server Sessions > Session Data Summary

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.

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. 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 **Set Up Services**.

Set Up Home Transport Sessions

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select the MQAM] Display QAM Sessions

After you switch to Direct ASI mode, you must set up Home Transport sessions by tearing down (deleting) BFS sessions and building Home Transport sessions. This page provides a procedure for tearing down and rebuilding sessions on the DNCS.

Back to top

Setting Up Home Transport Sessions

Complete these steps to set up Home Transport sessions by tearing down BFS sessions and Home Transport sessions.

1. In the DNCS Administrative Console Status window, click the DNCS **Control**. The DNCS Control window opens and shows the status of major system processes.
2. From the DNCS Administrative Console, select the **DNCS** tab.
3. Select the **Utilities** tab.
4. Click **Session List**. The Session Filter window opens.
5. In the Servers list, select the **Broadcast File System** and click **Display Server Sessions**. The Session Data window opens for the Broadcast File System.
6. Select Session ID **00.00.00.00.00.00 199**.
7. Click **Teardown Selected Sessions**. The system tears down and then automatically rebuilds Broadcast File System session (199).

Note: In the DNCS Control window, the bfsServer and osm monitor lights will change to yellow for a few minutes while the system rebuilds the sessions.

8. When the bfsServer and osm monitor lights change from yellow back to green, click **Refresh** in the Session Data window. The newly rebuilt session appears with a green background.

9. Now that you have set up the Home Transport session, verify that your VASP entries are correct. Go to **Verifying Your VASP Configuration**.

Back to top

VASP Entries

Verifying Your VASP Configuration

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP

After you set up the ASI link, verify that your Value Added Service Provider (VASP) entries are correct.

VASP is a generic term for the device that provides a service or functionality to elements on a Digital Broadband Delivery Service (DBDS). A network may include multiple VASP entries, each providing a unique set of services. However, the following VASP entries are required for any DNCS to successfully provide services to subscribers. These entries are created automatically by the system when your DBDS was initially installed:

- Broadcast File System — used by the BFS when starting its sessions
- CFSession UI — used by the user interface (UI) in the session setup request
- GEARServer — used for EAS activity
- HCTM Server — used for DHCT management
- Message Server — used by the system when sending pass-thru messages (this VASP never starts sessions)
- MMM Server — used for EAS activity
- OSM Server — used for DHCT operating system (OS) sessions

Occasionally, one or more of these entries may be missing or not in service. Therefore, it is a good idea to verify your VASP configuration whenever you make changes to your network.

Important: Depending on the services your network offers, there may be more VASP entries listed in the DNCS. However, the seven entries listed above **must** be present **and** in service for the DBDS to function properly.

Back to top

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, contact technical support.

Back to top

Verify Your VASP Configuration

Complete these steps to verify your VASP configuration.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Verify that the following VASP entries appear in the VASP List window and that they show a status of **In Service**.

VASP Entry Name	IP Address	Status
Broadcast File System	10.253.0.1	In Service
CFSession UI	10.253.0.1	In Service
GEARServer	10.253.0.1	In Service
HCTM Server	10.253.0.1	In Service
Message Server	10.253.0.1	In Service
MMM Server	10.253.0.1	In Service
OSM Server	10.253.0.1	In Service

Note: All of the VASP entries in the preceding table connect to the same IP address. These are the system default values. Your IP address entries may be different based on your system configuration. Check your network map to verify the IP addresses for your VASP entries.

5. Do all seven VASP entries appear in the VASP List window as shown in step 4, **and** do they all show a status of **In Service**?
   - If **yes**, go to step 6.
   - If **no**, go to step 7.
6. Do you need to add any VASP entries?
   - If **yes**, go to **Adding a VASP Entry**.

- If **no**, click **File** and select **Close** to close the VASP List window and return to the DNCS Administrative Console. Now that you have set up elements to process system data, set up elements that process content. Go to Adding an MPEG Content Source.

7. Are any of these seven VASP entries missing from the VASP List window?
   - If **yes**, go to **Adding a VASP Entry**.
   - If **no**, go to step 8.

8. Do any of these seven VASP entries have a status other than **In Service**?
   - If **yes**, go to **Activating a VASP Entry**.
   - If **no**, click **File** and select **Close** to close the VASP List window and return to the DNCS Administrative Console. Now that you have set up elements to process system data, set up elements that process content. Go to Adding an MPEG Content Source.

Back to top

Adding a VASP Entry

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > File > New

Complete these steps if you need to add a VASP entry to your system. For more descriptive information about VASP entries, refer to **Verifying Your VASP Configuration** above.

Before you begin, you must have the IP address of the server associated with the VASP entry you are adding (from your system administrator).

1. On the VASP List window, click **File** and select **New**. The Set Up VASP window opens.
2. For **VASP Type**, click to select the type of VASP entry you need to add.
3. Click in the **ID** field and type a unique number that you will use to identify this VASP entry. You can use up to 10 numeric characters.

   Note: We recommend that you establish a numbering scheme that allows you to easily identify the type of service associated with each VASP entry.

   Example: You might give a VASP entry associated with a specific service an ID of 9001. Then, you would assign IDs of 9002, 9003, and so forth to each additional VASP entry you add that is associated with this service.

4. Click in the **Name** field and type the name of this VASP entry. You can use up to 80 alphanumeric characters.

   Note: We recommend that you establish a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds. You could use the last two digits of the IP address for the QAM modulator.

5. Click in the **IP Address** field and type the IP address for the server associated with this VASP entry based on your network map. Be careful to properly place the dots (**.**) between numbers.

6. At the **Status** field, click the **In Service** option.

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

8. Add the new VASP entry information to your network map.

9. Do you need to add another VASP entry?
   - If **yes**, repeat steps 1 through 9.
   - If **no**, click **File** and select **Close** to close the VASP List window and return to the DNCS Administrative Console. Now that you have set up elements to process system data, set up elements that process content. Go to Adding an MPEG Content Source.

Back to top

Activating VASP Entry

Occasionally, a VASP entry is taken out of service, such as during maintenance. Use this procedure to place a VASP entry back into service that had been previously taken out of service.

1. On the VASP List window, click to select the VASP you need to place in service.
2. Click **File** and select **Open**. The Set Up VASP window for that VASP opens.
3. Click the **In Service** option.
4. Click **Save**. The system places the VASP into service. The Set Up VASP window closes and the VASP List window updates to show the changed status for this VASP.
5. Do you need to activate another VASP?
   - If **yes**, repeat steps 1 through 4.
   - If **no**, click **File** and select **Close** to close the VASP List window and return to the DNCS Administrative Console.

6. Now that you have set up elements to process system data, set up elements that process content:
   - If your system uses SimulCrypt technology, go to **Set Up PCG/SCS Pairs**.
   - If your system does not use SimulCrypt technology, go to **Add an MPEG Source**.

Back to top

PCG/SCS Pairs

PowerKEY CAS Gateway Window

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > PCG

The PowerKEY CAS Gateway window provides an at-a-glance status of the PCGs in your system. From this window, you can also modify the PCGs listed here.

What Would You Like to Do?

- Set up PCG/SCS pairs.
- Add a PCG element to the DNCS.
- View the parameters of a specific PCG.
- Modify a PCG provisioning parameters.
- Delete a PCG element from the DNCS.
- Reset a PCG element.
- View a list of existing SCS elements by clicking **SCS Elements**.
- Close the PowerKEY CAS Gateway window by clicking **Exit**.

Back to Top

Setting Up PCG/SCS Pairs Overview

This page provides an overview of the procedures required to set up PowerKEY Conditional Access Gateway/SimulCrypt Synchronizer (PCG/SCS) pairs for the first time. PCG/SCS pairs are required only for systems that use SimulCrypt technology. In these systems, a PCG/SCS pair encrypts content received from a D96xx Re-Multiplexer.

Setting up a PCG/SCS pair on the DNCS requires that you create a PCG element and an SCS element and then configure the connections between the two elements. Once connected and activated, the PCG and SCS work together to encrypt a transport stream. During every crypto period cycle, the PCG receives the request for ECM from the SCS with the Control Word (CW) and the PCG uses the CW to generate the ECM for the session. The PCG then sends the completed ECM to the SCS which encrypts the transport stream with the CW and inserts the ECM in the stream.

Setting up a PCG/SCS pair on the DNCS also requires that you create an MPEG SCS Source element for the D96xx Re-Multiplexer.

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Process Overview

To set up a PCG/SCS pair, you must complete the following steps. For step-by-step instructions for a particular task, click on that task.

1. Add a PCG to the DNCS.

   Note: As part of this procedure, you will configure two interfaces: one that the PCG uses to communicate with the SCS on a private network, and another one to communicate with the DNCS.

2. Add an MPEG SCS Source to the DNCS.

   Note: As part of this procedure, you will configure the port on the D96xx that connects to the SCS.

3. Add an SCS to the DNCS.

   Note: As part of this procedure, you will configure the port on the SCS that connects to D96xx Re-Multiplexer, and you will configure two interfaces: one that the SCS uses to communicate with the PCG on a private network and another one to communicate with the SI-Server. In addition, you will activate the SCS.

Back to top

Add a PCG

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > PCG

For systems using SimulCrypt technology, set up the elements that process content data now that you have set up the elements that process system data (Direct ASI and VASP elements). The first step in setting up elements that process content using SimulCrypt technology is to add a PowerKEY Conditional Access Gateway (PCG) element to the DNCS.

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 another interface to communicate with the DNCS.

Important: You must have a PCG associated with every SCS in your system. A single PCG can be associated with multiple SCS devices.

Back to top

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, contact technical support. You must also have the following information:

- Name used to identify the PCG (The name can be up to 20 alphanumeric characters.)
- NIC-IP address of the interface on the PCG for communicating with the DNCS (from your system administrator)
- MAC address of the interface on the PCG for communicating with the DNCS
- Subnet mask of the interface on the PCG for communicating with the DNCS (from your system administrator)
- Gateway IP address of the interface on the PCG for communicating with the DNCS (from your system administrator)
- IP address of the interface on the PCG for communicating with associated SCSs on a private network (from your system administrator)
- Subnet mask of the interface on the PCG for communicating with associated SCSs on a private network (from your system administrator)
- Gateway IP address the interface on the PCG for communicating with associated SCSs on a private network (from your system administrator)
- The maximum number of sessions the PCG will carry
- A unique number to identify the PCG element
- Number of seconds allowed for communications from the DNCS to the PCG.
- Name of 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
- Number of seconds the PCG waits to receive a control word (CW) before sending an alarm to the DNCS
- Number of seconds each crypto period will last (During a crypto period, the SCS requests an ECM from the PCG.)
- Number of seconds the SCG waits to receive provisioning information from the PCG

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.

Back to top

Adding a PCG

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

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. For 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 in the **Control NIC MAC Address** field and type the MAC address for this NIC on the PCG.

8. Click the **Maximum PCG Session Count** field and type the maximum sessions allowed on the PCG. This is any integer value between 1 and 1000.

9. Click the **Enabled** box to activate the PCG. (When enabled, the pkeManager process communicates with the DNCS.)

10. Leave the **Alarm Threshold %/Security Level** at the default setting. (At this time alarms are not supported.)

11. Click the **DNCS=>PCG Msg Timeout (Seconds)** field and type the number of seconds that the DNCS will wait for any communication with the PCG before timing out. You can enter any whole number between 5 and 60.

12. Click the **PCG=>SCS Msg Timeout (Seconds)** field and type the number of seconds that the PCG will wait for any communication with the SCS before timing out. You can enter any whole number between 5 and 60.

13. Leave the **CW_Provision Msg Repetition Rate (msgs per Crpto-Period)** field at its default value of 1 message per Crypto Period. This setting establishes the rate at which each CW (control word) message is sent from PCG to the Event Information Scheduler (EIS).

14. Click the **ID** field and type any integer value which uniquely identifies this PCG. (This field accepts any positive whole number.)

15. Click the **Config File** field and type the pcg config file name provided as part of the PCG installation (for example, **pcg.cfg**).

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

Note: When power is applied to the PCG for the first time, or when the PCG is rebooted, it uses the pcg.cfg file to determine if the correct version of code has been installed. If the PCG determines that an incorrect version of code has been installed, it requests that the correct code be downloaded.

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

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

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

19. Click in the **SCS Ethernet IP Address** field and type the IP address on this PCG used to communicate with 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.

20. 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.

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

22. Click the **SCS Test Timeout (Seconds)** field and type the number of seconds that the PCG waits to receive confirmation that the SCS channel between the PCG and the SCS interface is functioning as expected. You can use any integer between 5 and 20. This is the number of seconds the PCG waits for communication from the SCS.

23. Click the **CW Provision Message Delay (Seconds)** field and type **10**. This indicates the number of seconds the PCG waits to send an alarm to the DNCS when the PCG does not receive a control word.

24. Click the **Nominal Crypto-Period Duration** field and type the number of seconds the crypto period will last. You can use any integer value between 4 and 10. This is the number of seconds that each crypto period will last.

25. Click the **SCS Provision Timeout (Seconds)** field and type the number of seconds the PCG waits before resending an SCS Provision message when the PCG does not receive a response to the SCS provision message that the PCG sent. You can use any integer value between 5 and 20.

26. Click **Save**. The system saves this information in the DNCS database and closes the New PowerKEY CAS Gateway window. The PowerKEY CAS Gateway window updates to include the new PCG.

27. Add the new PCG to your network map.

28. Do you need to add another PCG?
    - If **yes**, go back to **Adding a PCG**.
    - If **no**, click **Exit** to close the PCG List window and return to the DNCS Administrative Console. Then go to **Add an MPEG SCS Source**.

Back to top

Add an MPEG SCS Source

Add an MPEG SCS Source

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > File > New

After you have added a PCG, next add an MPEG SCS Source. Certain D96xx re-multiplexers are called MPEG SCS sources because they receive program and service data from satellites and convert it into MPEG transport streams that they feed to an SCS for encryption.

Important: You must create an SCS MPEG source for every SCS 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..

Back to top

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, contact technical support. 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, MUX)
- IP 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 logically 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.

Back to top

Process Overview

Be sure to allow yourself adequate time to complete this procedure. To add an MPEG SCS source to the DNCS, you must complete the following tasks. For step-by-step instructions for a particular task, click on that task.

1. Set up the MPEG SCS source basic parameters.
2. Set up the connection from the MPEG SCS source to the SCS.

Note: There must be a one-to-one association between the MPEG Source and the MQAM/SCS.

Back to top

Setting Up the Basic Parameters for an MPEG SCS Source

The first step in adding an MPEG SCS source is to complete these steps to set up the basic parameters.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click **File > New**. The Set Up MPEG Source window opens with the Basic Parameters tab in the forefront.
5. Click the **Headend Name** arrow and select the headend associated with this MPEG source.
6. Click in the **MPEG Source Name** field and type the name of this MPEG source (for example, **HE1_MUX_SCS1**). You can use up to 20 alphanumeric characters.

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

7. 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.

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

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

9. 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 router documentation for instructions on locating the ARP entry table.

10. Click in the **Output Mode** field and select MUX.

Note: If the option MUX is not available, type MUX in the field.

11. Click **Apply**. The system saves the basic parameters for this MPEG SCS source in the DNCS database. The previously disabled Connectivity tab becomes available, and **Save complete** is displayed in the Status area.

12. Your next step is to set up the connection from the MPEG SCS source to the SCS/MQAM. Go to **Setting Up MPEG SCS Source Connections**.

Back to top

Setting Up MPEG SCS Source Connections

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

1. On the Set Up MPEG source window, click the **Connectivity** tab. The Connectivity window opens.

Note: Because no devices are yet 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 **1** to represent the output port on the D96xx Re-Multiplexer that is logically connected to the input port on the SCS.

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 SCS. This number must correspond with the ASI input (usually on your network map) on the associated SCS. Go to **Source and Service Naming Conventions** for the correct TSID naming conventions.

5. Click the **Transport Protocol** arrow and select **ASI** as the type of transport protocol being used to send the data to the SCS.

Note: The Transport Protocol will always be ASI.

6. Click **OK**. The system saves this information in the DNCS database and closes the Port Number Prompt window. The Connectivity tab updates with the information you entered.

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

8. Add the new MPEG SCS source to your network map.

9. Do you need to add another MPEG SCS Source?
   - If **yes**, go back to **Setting Up Basic Parameters for an MPEG SCS Source**.
   - If **no**, click **Cancel** to close the Set Up MPEG Source window, and then click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console. Go to step 10.

10. Your next step is to add the SCS that will be receiving data from this MPEG SCS source. Depending on your configuration, go to **Add an SCS**.

Back to top

Add an SCS

SCS Devices Window

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS

The SCS Devices window provides an at-a-glance status of the SCS elements in your system. From this window, you can also modify the SCS elements listed here.

What Would You Like to Do?

- Add an SCS element to the DNCS.
- View the parameters of an SCS element.
- Modify the modeling parameters of an SCS element.
- Modify the modeling parameters of a SCS ports.
- Delete an SCS element from the DNCS.
- View a list of existing PCG elements by clicking **PCG Elements**.
- Close the SCS Devices window by clicking **Exit**.

Back to Top

Add an SCS

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS

After you add an MPEG SCS Source and if you are using a third-party Event Information Scheduler (EIS) and a third-party SimulCrypt Synchronizer (SCS) for scrambling the stream, you must add this SCS element to the DNCS database.

The SCS and PCG work together to encrypt a transport stream. During every crypto period cycle, the PCG requests the control word (CW) from the SCS and uses the CW to generate the ECM for the session. The PCG then sends the completed ECM to the SCS, which encrypts the transport stream with the CW and inserts the ECM in the stream. All of this occurs during one crypto period cycle.

The SCS uses an interface to communicate with the PCG on a private network, and it uses another interface to communicate with the SI-Server. When you add an SCS element to the

DNCS, these interfaces are configured. Additionally, the connection between the SCS and the MPEG source that you added earlier is configured.

Back to top

Before You Begin

Before you begin, you must have your network map. If you cannot locate your network map, contact technical support. You must also have the following information:

- Name used to identify the SCS (The name can be up to 20 alphanumeric characters.)
- NIC-IP address for the interface on the SCS that will talk to the PCG on a private network (from your system administrator).
- MAC address for the above interface on the SCS (click here for the procedure to locate).
- 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.
- 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 are logically connected to the associated MPEG source.

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.

Back to top

Process Overview

Be sure to allow yourself adequate time to complete this procedure. Adding an SCS element takes approximately 30 minutes. To add an SCS element to the DNCS, you must complete the following tasks. For step-by-step instructions for a particular task, click on that task.

1. Setting Up SCS Modeling Parameters.
2. Setting Up SCS Ports Modeling Parameters.

3. Setting Up SCS Connections.

4. Activating the SCS.

Back to top

Setting Up SCS Modeling Parameters

The first step in adding an SCS is to complete these steps to set up the basic parameters for the modulator.

1. On the DNCS Administrative Console, click the **DNCS** tab, and then click the Network Element Provisioning tab.
2. Click **SCS**. The SCS Device 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. For example, a name of SCS12 could represent a 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 numbers.
6. Click the **MAC Address** field and type the MAC address for this interface on the SCS.
7. Click the **Primary PCG** arrow and select the primary PCG with which this SCS would communicate and get ECMs.
8. Click the **Headend** arrow and select the headend in which the PCG resides.
9. Click the **Max Sessions** field and type the maximum sessions allowed on the SCS device. This is any integer value between 1 and 50.
10. Click **Save**. The system saves this information into the DNCS database and the SCS shows in the SCS Device window. Your next step is to set up the ports on the SCS. Go to Setting Up SCS Ports Modeling Parameters.

Back to top

Setting Up SCS Ports Modeling Parameters

After you set up the SCS modeling parameters, complete these steps to set up the 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 Device window opens.

3. Click the **Select** button next to the SCS you added in Setting Up SCS Modeling Parameters, and then click **Ports for Selected SCS**. The SCS Ports window opens.

4. Click **Add Input Port**. Empty fields appear in the Input area.

5. Click in the **Input Port Number** field, and type **1** (one) to identify the input port.

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

6. Click in the **Input TSID** field, and type the number identifying the transport stream on this SCS input port.

Notes:

- You must specify unique transport stream IDs for both input and output ports.
- The Input Frequency supports any devices that can use Intermediate Frequency (IF). For D96xx devices that receive ASI input, leave this field empty.

7. Click **Save.** The system saves this information into the DNCS database and updates the SCS Ports window to show the information you entered.

8. Click **Add Output Port**. Empty fields appear in the Output area.

9. Is this SCS the Home Transport SCS?
   - If **yes**, click the **Output Home TS** check box to enable this frequency as Home TS, and go to step 10.
   - If **no**, go to step 10.

10. Click in the **Output 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 both input and output ports.

11. Click in the **Output Frequency** field, and type the frequency of the channel (in MHz) you will use to send data from this SCS to the hubs on your system.

Important: We recommend that you enter a value in 8 MHz increments from 108 to 858.

12. Click the **Output 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.

13. Click in the **Output Symbol Rate (Symbols Per Second)** field, and type the symbol rate (s/s).

Important: The recommended PowerKEY DVB System symbol rate is 6,900,000s/s. This symbol rate matches the DHCT Bootloader symbol rate. You can change the symbol rate for all transport streams except the transport stream for the Home D96xx. The symbol rate for the Home D96xx must remain at 6,900,000 s/s.

14. Click **Save**. The system saves this information into the DNCS database and updates the SCS Ports window to show the information you entered.

15. 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

Back to top

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.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Select the source that you created earlier when you added an MPEG source for this SCS, and click **File** and select **Open**. The Set Up MPEG Source window opens for this MPEG SCS source.
5. Click the **Connectivity** tab. The Connectivity window opens.

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

7. Click the **Device Type** arrow and select **SCS** to indicate the type of device being used to receive the data.

Note: When associating an SCS with an MPEG SCS source, the Device Type will always be SCS.

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

9. Click the **Port number** arrow and select the input port number on the SCS device. The first port number on the MPEG should always be 1 (one).

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

11. Click **Save**. Go to **Activating the SCS**.

Back to top

Activating the SCS

After you set up the connections between the SCS and its associated MPEG SCS 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 Device window opens.
3. Click the **Select** box next to the SCS and then click **Open Selected SCS**. The Update SCS Device window opens.
4. Click the **Online** check box to allow the SCS to be modeled in DNCS.
5. Click **Update**. The system saves this information into the DNCS database.
6. Click **Exit** to close the window.
7. Add the new SCS to your network map.
8. Are you setting up your network for the first time?
   - If **yes**, go to **Setting Up DHCTs**
   - If **no**, continue making any other changes that you need to make to your network.

Back to top

DHCTs

Setting Up DHCTs

Now that you have set up all of your other network elements, you are ready to set up your DHCTs in the DNCS.

Before You Begin

Before you begin setting up your DHCTs, you must make sure that you have set up all of your network elements and defined your system as being OpenCable compliant (if applicable).

Back to top

Process Overview

To set up DHCTs in the DNCS, you must complete the following procedures. For step-by-step instructions for a particular procedure, click on that task.

1. Set up new DHCTs.
2. Set up existing DHCTs

Back to top

Setting Up New DHCTs

For instructions on setting up new DHCTs, refer to the appropriate staging guide for each DHCT model. We include the correct staging guide with each shipment of new DHCTs.

Back to top

Setting Up Existing DHCTs

To upgrade the operating system (OS) and Resident Application (ResApp) software on DHCTs that are already deployed, refer to the appropriate upgrade instructions for each DHCT model. If you cannot locate these instructions, contact technical support.

Back to top

Customize DHCT Functionality to Enhance Subscribers' Experience

Special software on each DHCT allows you to customize how a DHCT functions so that you can customize DHCTs to meet the needs of your subscribers.

Back to top

Ways to Customize DHCT Behavior

The following list gives only a few examples of the ways that you can customize a DHCT.

- Allow subscribers to skip unauthorized channels.
- Allow subscribers to select which channel the DHCT tunes to when powered on.
- Allow subscribers to select a preferred audio language for digital services.
- Choose the language that is most common for your area to be used with a DHCT's wireless keyboard.
- Allow subscribers to choose a color scheme for the DHCT user screens, or select a color scheme for subscribers.

Back to top

Ways to Send Customized Behavior to DHCTs

After you have customized how you want the DHCT to function, you can send this configuration to the DHCTs in your system in any of the following ways:

- For all DHCTs in the network (global configuration)
- For a single DHCT (addressable configuration)
- For all DHCTs in a specific hub (hub configuration)
- During the staging process, so that all DHCTs receive this configuration when they are staged (staging defaults)

For assistance performing any of these tasks, refer to the *Enhancing Your Subscriber's Experience: SARA Configurable Options, User's Guide*. To obtain a copy of this publication, see **Printed Resources**.

Back to top

Authorize a DHCT for a Service

Note: Your billing system normally authorizes the DHCTs in your system for all services. Although you can authorize DHCTs for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of DHCTs for services with your billing system vendor.

After a DHCT is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a DHCT must be authorized specifically to receive service packages before it can access services that are contained in those packages.

Before You Begin

Before you can authorize a DHCT for a service, you must have the MAC address, IP address, or serial number of the DHCT.

Time To Complete

Authorizing a DHCT for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the DHCT to receive the new package information.

Performance Impact

Authorizing a DHCT for a service does not impact network performance. You can complete this procedure any time.

Authorizing a DHCT for a Service

Complete these steps to authorize a DHCT for a particular service package.

1. Make sure the test DHCT is connected to a television, as well as to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.
6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT you are testing.

Note: By default, the **Open** and **By MAC Address** options are selected already when you open the DHCT Provisioning window.

7. Click **Continue**. The Set Up DHCT window opens for the test DHCT.

8. Verify that the Admin Status field is set to either In **Service One Way** or **In Service Two Way**.

9. Click the **Secure Services** tab.

10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT to be able to access.

Notes:

-
  - You can select more than one package by holding down the **Ctrl** key as you click on each package.
  - If your system uses a Brick package, the DHCT must be authorized for that package as well. This should have been done when the DHCT was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:
    - **IPPV Enable** - If this DHCT uses IPPV services, enable this option and ensure that the credit limit field is set to a non-zero value.
    - **DMS Enable** - Enable this option. Digital Multicast Service is needed to allow the DHCT to receive secure services.
    - **DIS Enable** - If this DHCT uses VOD services, enable this option, otherwise, leave this option disabled. Digital Interactive Service is needed to support VOD service.
    - **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

    Note: Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to the *Analog Descrambling Support for the Digital Broadband Delivery System Application Guide* for details. To obtain a copy of this publication, see **Printed Resources**.

    - **Fast Refresh Enable** - This option is used to send EMMs to DHCTs during staging. For more information, refer to the *Explorer Digital Home Communications Terminal Staging Guide*. To obtain a copy of this publication, see **Printed Resources**.
    - **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

Back to top

Verify a Successful Service Setup

After you authorize a DHCT for a service, you can try to access the service to verify that you set it up correctly.

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the DHCT time to receive the new service information.

Time To Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the DHCT has had a chance to receive the service information (usually within 15 minutes).

Procedure

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the DHCT is connected to a television and to an RF feed into your network.
2. Make sure the DHCT and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.

   Note: For assistance adding a service to a channel map, see *SI-Server Complete SI Solution User Manual.* To obtain a copy of this document, go to **Printed Resources**.

4. Does the service appear as expected?
   - If **yes**, go to step 5.

- If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact technical support.

5. Is this a PPV service?

4.
   - If **yes**, attempt to purchase an event, then go to step 6.
   - If **no**, you are finished testing the service.

5. Were you able to successfully purchase an event?
   - If **yes**, you are finished testing the service.
   - If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact technical support.

Back to top

Locate MAC Addresses

Locate a DHCT MAC Address

To locate the MAC address of a DHCT, do one of the following:

- Display **Page 1** of the DHCT diagnostic screens.
- Look on the back of the DHCT for a label with the MAC address recorded on it.

Locate the MAC Address of an MQAM Modulator

You can look at the sticker on the side of the MQAM modulator to locate its MAC address. Or, if the modulator is already in operation, complete these steps to use its front panel to locate the MAC address.

1. Go to the front panel of the modulator in question.
2. Press **OPTIONS** repeatedly until you see **MAC Address** appear in the LCD. The number will look something like this: 00:02:DE:81:F5:36.
3. Press **ENTER** to return to the main menu of the LCD window.

Back to top

Locate PCG MAC Addresses

To locate the MAC address of a PCG, look on the back of the PCG for a label with the MAC address recorded on it.

Source and Service Naming Conventions

This page contains the naming conventions for sources and services in the PowerKEY DVB System.

Back to top

TSID Numbering Conventions

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

Back to top

DVB Service ID Numbering Conventions

Sources provisioned in the DNCS should be thought of as being DVB services. DVB services are identified by triple ONID, TSID, and Source (Service) ID. 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.

  The following list illustrates DVB Service ID examples.

  Note: The DVB Service IDs on your system may vary.

  - 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

Back to top

Set Up Services

Overview of Subscriber Services

Important: If you have subscribers with the Explorer Home Entertainment Server, do not use these procedures to set up services. Instead, refer to *Downloading New Client Application Platform Installation Instructions.* To obtain a copy of this document, see **Printed Resources**.

After all of your network elements are installed and you have entered information about each into the DNCS database, you are ready to set up the following types of services for your subscribers. To see instructions for setting up a particular type of service, click on the service type:

- Clear Services — services that are delivered to subscribers unscrambled or unencrypted; for example, programming available through the three major networks (ABC, CBS, and NBC) is usually clear
- Secure Services — services that are encrypted or scrambled so that they are protected from being accessed (stolen) by people who have not paid for the service; usually offered at a price that is in addition to the price for clear services (for example, HBO, ShowTime, and music channels)
- Pay-Per-View (PPV) Services — services that carry PPV events that subscribers can choose to purchase in addition to their normal cable programming; has some of the same characteristics as both clear and secure services

Back to top

Source and Service Naming Conventions

This page contains the naming conventions for sources and services in the PowerKEY DVB System.

Back to top

TSID Numbering Conventions

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

Back to top

DVB Service ID Numbering Conventions

Sources provisioned in the DNCS should be thought of as being DVB services. DVB services are identified by triple ONID, TSID, and Source (Service) ID. 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.

  The following list illustrates DVB Service ID examples.

  Note: The DVB Service IDs on your system may vary.

  - 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

Back to top

Set Up Clear Services

Clear services are delivered to subscribers "in the clear," meaning unscrambled or unencrypted.

Because these services are not encrypted, they are more susceptible to being accessed (stolen) by people who have not paid for the service. Therefore, you may also hear clear services referred to as "non-secure" services.

Back to top

Before You Begin

Before you set up clear services in your network, you must make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to **Setting Up Your Network**.

You may also want to have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Time To Complete

Setting up a clear service takes approximately 45 minutes to an hour to complete.

Back to top

Performance Impact

Setting up a clear service does not impact network performance. You can complete this procedure at any time.

Back to top

Setting Up Clear Services

Complete these procedures to set up a clear service in your network. For step-by-step instructions for a particular procedure, click on that procedure.

1. Make sure you have completed all of the necessary steps specified in **Setting Up Your Network**.
2. Add the service source to the DNCS database.
3. Define parameters for the service source.
4. Do you want to offer the service to only specifically authorized subscribers?
   - If **yes**, go to step 5.
   - If **no**, go to step 6.
5. Add the clear service to a package.
   - If you are adding the clear service to a **new** package, add a service package, and then go to determine and convert the package EID from a hexadecimal to a decimal value. When finished, go to step 6.
   - If you are adding the clear service to an **existing** package, determine and convert the package EID from a hexadecimal to a decimal value. When finished, go to step 6.
6. Do you want to include the service on your EPG?.
   - If **yes**, refer to *Configuring the PowerKEY® DVB System* for instructions. When finished, go to step 7. (To obtain a copy of this user's guide, see **Printed Resources**.
   - If no, go to step 7.
7. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

Back to top

Set Up Secure Services

In contrast to a clear service, a secure service is encrypted or scrambled so that it is protected from being accessed (stolen) by people who have not paid for the service. Encrypted services are considered to be more "secure" from theft than clear services. We use the PowerKEY Conditional Access (CA) system to secure services.

Secure services are usually offered to subscribers at a price that is in addition to the price they pay for clear services. Following are some examples of secure services:

- HBO
- ShowTime
- Music channels

Back to top

Before You Begin

Before you set up secure services in your network, you must make sure all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to **Setting Up Your Network**.

You may also want to have your network map readily available. If you cannot locate your network map, contact technical support.

Important: Before you set up a secure analog service in the DNCS, you must configure your analog system to support DHCTs that descramble analog services. Refer to *Analog Descrambling Support for the Digital Broadband Delivery System Application Guide*. (To obtain a copy of this guide, see **Printed Resources**.)

Back to top

Time To Complete

Setting up a secure service takes approximately 45 minutes to an hour to complete.

Back to top

Performance Impact

Setting up a secure service does not impact network performance. You can complete this procedure at any time.

Back to top

Setting Up Secure Services

Complete these procedures to set up a secure service in your network. For step-by-step instructions for a particular procedure, click on that procedure.

1. Make sure you have completed all of the necessary steps specified in **Setting Up Your Network**.
2. Add the service source to the DNCS database.
3. Define parameters for the service source.
4. Encrypt the content coming from the service source so that it is available only to authorized subscribers.
5. Add an unlimited segment for the service.
6. Add the service segment to a package.
7. Do you want to include the service on your EPG?

- If **yes**, refer to *Configuring the PowerKEY DVB System For System Release i4.3* for instructions. When finished, go to step 8. (To obtain a copy of this guide, see **Printed Resources**.)
- If **no**, go to step 8.

8. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service, and then try to access the service.

Back to top

Add a Service Source

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > File > New

Note: This procedure applies to clear, secure, and PPV services.

The first step in setting up a clear, secure, or PPV service is to add information to the DNCS database about the original content source. After the source has been added to the DNCS, you can use this source to create different services. For example, you can use the signal from Fox Sports World (FOXSW) to create different 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.

Back to top

Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

Back to top

Time To Complete

Adding a content source takes approximately 5 minutes to complete.

Back to top

Performance Impact

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

Back to top

Adding a Content Source

Complete these steps to add a source for a service.

Note: This procedure applies to clear, secure, and PPV services.

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

2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **File > New**. The Set Up Source window opens.
5. 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.

Note: 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.

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

Important: Before make certain that the source ID follows the conventions defined in Source and Service Naming Conventions.

Notes:

1.
   - You must use a number that is greater than 200 for the source ID. Source ID numbers 1 through 200 are reserved for system-built service sources.
   - You can use up to 5 numeric characters.
   - Remember the content source ID. You will need it as you continue to set up the service.

7. Click **Save**. The system saves the source information in the DNCS database and closes the Set Up Source window. The Source List window updates to include the new source.
8. You're ready to define the source that you just added. Go to **Define a Content Source**.

Back to top

Encrypt a Service

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Source > [Source Name] > File > Security Modes > File > New

Note: This procedure applies to secure and PPV services.

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.

Important: When setting up an encrypted session on the PCG, you must also enable scrambling on the MUX using the SI-Server.

Back to top

Time To Complete

Encrypting a service takes approximately 10 minutes to complete.

Back to top

Performance Impact

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

Back to top

Encrypting a Service

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. 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, 2003, as **07042003**. The system inputs the slashes for you and displays 07/04/2003.

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. 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:

12.

- 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.

13. 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.

14. 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.

15. 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.

16. Click **File > Close** to close the Security Mode List window and return to the Source List window.

17. Continue setting up the type of service you would like to provide:
    - 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.

Back to top

Add an Unlimited Segment

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

Important: Follow this procedure to set up secure services only. Do not use this procedure to set up clear or PPV services.

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.

Note: Currently, there are no services that you set up in the DNCS that use limited segments.

Back to top

Time To Complete

Adding an unlimited segment takes approximately 10 minutes to complete.

Back to top

Performance Impact

Adding an unlimited segment does not impact network performance. You can complete this procedure at any time.

Back to top

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 **System 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.

    Note: This feature is not currently supported. Selecting an option other than None has no effect on your system.

11. Verify that **Fingerprint** is set to **None.** If it is not, select **None** to disable this option.

    Note: This feature is not currently supported. Selecting an option other than None has no effect on your system.

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 its duration.

16. Do you need to set up another unlimited segment for this service source?
    - 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:
    - 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.

Back to top

Add a Service Package

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > File > New

Notes:
- This procedure applies to secure and packaged clear services.
- Do not use this procedure for PPV or unpackaged 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.

However, you can package a clear service to make it available only to specifically authorized subscribers. You may want to do this if you have DHCTs that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:
- Unscrambled analog video

- Clear digital video
- Clear digital audio
- Other channel-based services

Back to top

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.
- This version of the DNCS does not support packages within packages.
- This version of the DNCS does not support packages for virtual channels.

Back to top

Time To Complete

Adding a service package takes approximately 10 minutes.

Back to top

Performance Impact

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

Back to top

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. Contact technical support.
  -
  - 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:

- 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.

Back to top

Add a Secure Service to a Package

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Package > [Package Name] > File > Provision

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.

Important: The DNCS does not support packages within packages or packages for virtual channels. This ability will be available in a future release of the DNCS.

Back to top

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 Service Package** before you begin this procedure.

Back to top

Time To Complete

Adding a secure service to a package takes approximately 10 minutes to complete.

Back to top

Performance Impact

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

Back to top

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:
    - 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.

Back to top

Define a Digital Source and Session

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

After you add a service source to the DNCS for a clear, secure, or PPV service, define parameters for that source. Then build a session from the source definition.

Important:

- If you are sending the same source through more than one MQAM modulator, you must define the source for each modulator. For example, if you are sending the same source content through six MQAM modulators, you must define the source six times — once for each modulator.
- When using a D96xx and PCG in place of an MQAM, do not create session definitions for clear channels.
- When using a D96xx re-multiplexer or a PCG, session definitions are required only for encrypted channels.

- When setting up an encrypted session on the PCG, you must also enable scrambling on the MUX using the SI-Server.

Back to top

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 service source
- Number of the channel where the service will be displayed
- Service source ID as you defined it when you added the service source
- 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)

Back to top

Time To Complete

Defining a digital service source and building a session from the source definition takes approximately 20 minutes to complete.

Back to top

Performance Impact

Defining a digital service source and building a session from the source definition does not impact network performance. You can complete this procedure at any time.

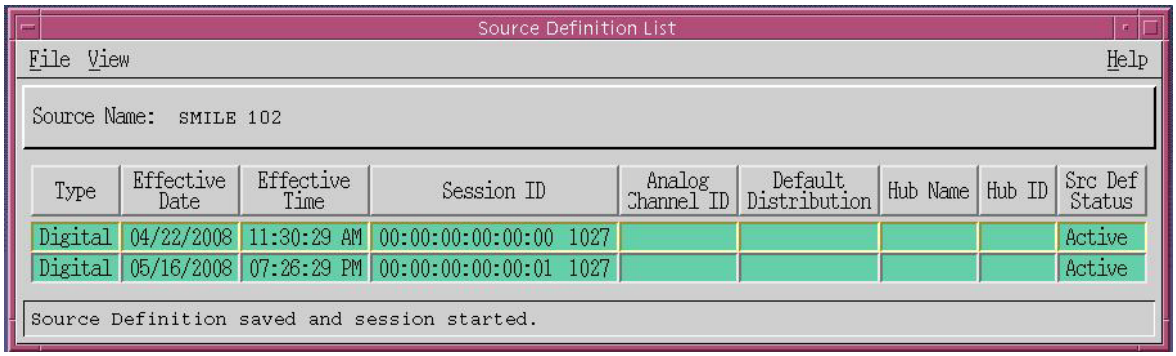
Back to top

Defining a Digital Service Source and Session

Follow this procedure to define a digital source and to then build a session from the source definition.

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 define.
6. Click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
7. Are multiple hubs configured (DNCS/RNCS/DNCS + RNCS)?

Important: 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.

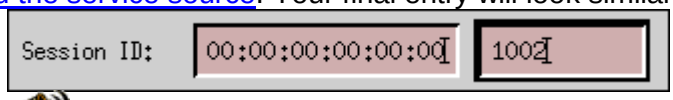


8. Click **File > New Digital**. The Set Up Digital Source Definition window opens.

9. Click in the first **Session ID** field and type the MAC address and ID of the source in the adjacent box.

Note: When entering the MAC address, the system inserts the colons for you.

10. Click in the second **Session ID** field and type the Service Source ID you used when you added the service source. Your final entry will look similar to the following example:



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 0000002969
- If the session ID is 00:00:00:00:00:01 10601, the access criteria in the SI-Server must be 0000012969

11. Digital sources normally become effective as soon as they are saved. Do you want to delay the effective date and time of this digital service source?
    - If **yes**, go to step 12.
    - If **no**, go to step 16.

Note: Subscribers will see a blank channel until either the digital sources are saved or the time that you specify arrives.

12. Click the **Specify effective date and time** option, and then click **Next**. The Set Start Time/Date window opens. Go to step 12.

13. Click in the **Effective Date** field and type the month, day, and year you want subscribers to be able to start viewing content from this source. You must type two digits for the month and day, and four digits for the year. When finished, go to step 13.

> **Example:** You would type July 4, 2003, as **07042003**. The system inputs the slashes for you and displays 07/04/2003.

14. Click in the **Effective Time** field and type the hour, minute, and second you want subscribers to be able to start seeing content from this source. You must type two digits for each value. When finished, go to step 14.

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

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

15. Click **AM/PM** to establish which portion of the day you want subscribers to be able to start viewing content from this source. Go to step 15.

16. Click **Next**. The Define Session window opens.

17. Make the appropriate selection for you system and then click **Next.** The Session Setup window opens.

> **Note:** When an MQAM modulator is used, select **Broadcast programming**. When a D96xx is used, select **SCS-controlled Broadcast**.

18. Click the **Input Device** arrow and select the type of device (the MPEG source) that will be providing the service content (for example, MUX). You would have defined the MPEG content source when you set up your network.

19. Click **Next**. The Select Outputs window opens.

20. Select the modulator that will receive service from this source and click **Next**. The Wrap-Up window opens and displays settings appropriate to the device that you selected.

> **Note:** To select more than one modulator, hold down the **Ctrl** key on your keyboard as you click on each modulator.

21. Enter data in the following fields to set up a session on the ASI ports of an MQAM modulator/SCS:

- In the **MPEG Program Number** field and type the program number being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.

> **Note:** For ease of use, the MPEG Program Number may be the same as the Source ID, but this is not a mandatory requirement.

- In the **Bandwidth** field and type the amount of bandwidth (in Mbps) that the system should allow for this service.

  Note: This value is usually defined by your content service provider. Requirements vary from system to system, but in general, you can use the following guidelines:

  - Standard MPEG video streams use **2** or **3** Mbps.
  - HDTV streams use **13** Mbps.
  - Audio streams use **0.2** Mbps.

22. Click **Next**. The Save Source Definition window opens.

23. Click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

24. Do you need to define another digital source for this service?
    - If **yes**, repeat steps 7 through 22.
    - If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window. Go to step 24.

Note: You would define more than one digital service source if you have more than one MPEG source feeding the same content into different portions of your network.

25. Click **File > Close** to close the Source List window and return to the DNCS Administrative Console.

26. Now that you have defined a session for the source, set up the type of service you would like the session to provide:
    - To set up a clear service, go to step 4 of Set Up Clear Services.
    - To set up a secure (encrypted) service, go to step 4 of Set Up Secure Services
    - To set up a pay-per-view (PPV) service, go to step 4 of Set Up PPV Services.

Back to top

Create a PPV Service

Quick Path:
DNCS Administrative Console > Server Applications tab > PPV Service > File > New

Note: This procedure applies to clear, secure, and PPV services.

After you create a service to provide the PPV event, you must create a PPV service. This PPV service advertises and sells the PPV event. 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.

Back to top

Before You Begin

Before adding a content source to the DNCS, make sure that you have first set up all of your network elements.

Back to top

Time To Complete

Adding a content source takes approximately 5 minutes to complete.

Back to top

Adding a PPV Service

Complete these steps to add a PPV service to advertise events to subscribers.

1. On the DNCS Administrative Console, click the **Server Applications** tab.
2. Click **PPV Service**. The PPV Service List window opens.
3. Click **File > New**. The Set Up PPV Service window opens.
4. On the Set Up PPV Service window, complete all of the following required fields. (Optional fields are labeled.)

- **Service Name** - Enter a unique name for the service. This field is case sensitive.

  Note: Service Names are typically provided by the billing system.

- **Short Description** - Enter a useful descriptive short name, such as RPPV1 or RPPV2 for subscribers to see when they tune to the channel where the PPV service resides. Make a note of the description you have entered. You will need this later when you set up this PPV service in the EPG.
- **Long Description** - Enter a longer description that provides a more complete definition of the service. This is for your benefit only. Subscribers never see the information entered in this field.
- **Logo Index** - Should always be set to "0" (zero).
- **Default Order Telephone Number** - Enter a telephone number that specifies the phone number subscribers should call to order a reservation pay-per-view (RPPV) event advertised by this service.
- **Default Cost (Optional)** - If you desire, enter the default cost for RPPV events. This figure will display if the billing system specifies no cost for the event. (Completing this field is optional.)
- **Default Order Start Interval (Optional)** - Not available at this time.
- **Event Use Service** - Click the arrow and select the service that will be seen on this PPV service channel when the PPV event is purchased. Make a note of the service you select. You will need this later when you set up this PPV service in the EPG.
- **Subscription Service (Optional)** - Not available at this time.
- **Interstitial Service (Optional)** - Not available at this time.

5. Click **Save**. The SARA Server creates a PPV service for the source and automatically does the following:

- Registers this PPV service with the SAM and assigns a URL of ippv to the service.
- Creates an unlimited segment from the service, which you can view in the Segment List.

6. Verify that the service was setup successfully. Go to **Verify a Successful Service Setup**.

Back to top

Set Up PPV Services

A PPV service carries PPV events that subscribers can choose to purchase in addition to their normal cable programming. A PPV service has some of the same characteristics as both a clear and a secure service.

Like a clear service, subscribers can always access a PPV service by tuning to a channel that carries the service. The channel displays a banner that advertises the PPV events that subscribers can purchase through that PPV service.

However, like a secure service, the content for a PPV service is encrypted so that only subscribers who have paid for the content can access the content. In this case, the content is a PPV event.

Back to top

Before You Begin

Before you set up PPV services in your network, you must make sure that all of the network elements responsible for processing the service content are physically installed in your system. The network elements must also have been added to the DNCS database. If necessary, refer to **Setting Up Your Network**.

You may also want to have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Time To Complete

Setting up a PPV service takes approximately 45 minutes to an hour to complete.

Back to top

Performance Impact

Setting up a PPV service does not impact network performance. You can complete this procedure at any time.

Back to top

Setting Up PPV Services

Complete these procedures to set up a PPV service in your network. For step-by-step instructions for a particular procedure, click on that procedure.

1. Make sure you have completed all of the necessary steps specified in **Setting Up Your Network**.

2. Add the service source to the DNCS database.
3. Define parameters for the service source.
4. Encrypt the content coming from the service source so that it is available only to authorized subscribers.
5. Register the service for the PPV event with the SAM.
6. Create a PPV service to advertise PPV events.
7. Add both the PPV service and the Event Use Service to your EPG as defined in *Configuring the PowerKEY® DVB System*. (To obtain a copy of this guide, see **Printed Resources**.)

   Important: If you do not add both services to the EPG, information about the PPV events will be missing from the EPG or from the PPV purchase barker.

8. Verify that the service has been set up successfully by authorizing a test DHCT to receive the service. Then, try to access the service, purchase an event, and view the event.

Back to top

Set Up Credit-Based PPV

In order to satisfy customer requirements to make IPPV possible in a one-way environment and to allow pre-payment of pay-per-view services, a method to pre-position purchase credits is implemented in the DNCS system. This effort is accomplished primarily through the use of a new set of entitlement management messages (EMMs) within the PowerKEY system. A new EMM structure is used to apply and remove credits from clients utilizing the pre-purchased credit mechanism.

Notes:

- The credit-based PPV feature is enabled using the **licenseGen** script.
- The BOSS command **ModifyPpvCredit** can also be used to reset existing credit.

Setting Up the Maximum Credit Available and the Default Expiration Time

Note: The maximum credit per transaction can be limited and the default credit expiration also can be set.

Complete these steps to configure the maximum credit available and the default expiration time.

1. From the DNCS Administrative Console, select the **DNCS** tab and then choose the **System Provisioning** tab.
2. In the System Management area, click **DHCT Mgr**. The DHCT Manager window opens.
3. Click the **PPV Credits** tab.
4. In the Maximum Current Credit field, enter the amount of the maximum credit available.

5. Do you want to enable the credit expiration time?
    - If **yes**, select **Enable Expiration** and then go to step 6
    - If **no**, go to step 8.

6. In the Default Credit Expiration field, enter the default number of days before the credit expires.

7. In the Credit Updation field, enter the credit updating delay (in seconds). This value specifies the delay between one transaction and another.

8. Click **Save**.

Add, Remove, or Reset the Credits for Individual Set-Tops

1. From the DNCS Administrative Console, select the **DNCS** tab and then choose the **Home Element Provisioning** tab. DHCT.
2. Select **DHCT**. The DHCT Provisioning window opens.
3. In the By MAC Address field, enter the **MAC Address** of the set-top.
4. Click **Open**.
5. Click **Continue**.
6. In the Set Up DHCT GUI select the **PPV Credits** tab.
7. Choose one of the following options:
    - To **Add** credits, enter the credits in the **amount** column, click the **Add** check box, and then go to step 8.
    - To **Remove** credits, enter the credits in the a**mount** column, click the **Remove** check box, and then go to step 8.
    - To **Reset** credits, check the **Reset** option and then go step 9.
8. Is the credit expiration enabled?

7.
    - If **yes**, select the **Accept Credit Expiration** check box and enter the number of **Expiration days**. Then go to step 9.
    - If **no**, go to step 9.

8. Click **Send** to initiate the transaction.

Test a Service

Test a Service

Note: Your billing system normally authorizes the DHCTs in your system for all services. Although you can authorize DHCTs for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of DHCTs for services with your billing system vendor.

After you have completed all the steps in setting up a particular type of service, verify that you set up the service successfully by using a test DHCT and a television.

Is the new service packaged?

- If **yes**, first authorize the DHCT to receive the package.
- If **no**, verify a successful service setup by trying to access the service.

Back to top

Authorize a DHCT for a Service

Note: Your billing system normally authorizes the DHCTs in your system for all services. Although you can authorize DHCTs for services directly from the DNCS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of DHCTs for services with your billing system vendor.

After a DHCT is staged and installed into your system, it should receive all of your unpackaged clear services automatically. However, a DHCT must be authorized specifically to receive service packages before it can access services that are contained in those packages.

Before You Begin

Before you can authorize a DHCT for a service, you must have the MAC address, IP address, or serial number of the DHCT.

Time To Complete

Authorizing a DHCT for a service takes approximately 5 minutes to complete. However, it can take up to 15 minutes for the DHCT to receive the new package information.

Performance Impact

Authorizing a DHCT for a service does not impact network performance. You can complete this procedure any time.

Authorizing a DHCT for a Service

Complete these steps to authorize a DHCT for a particular service package.

1. Make sure the test DHCT is connected to a television, as well as to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the DNCS Administrative Console, click the **DNCS** tab.
4. Click the **Home Element Provisioning** tab.
5. Click **DHCT**. The DHCT Provisioning window opens.

6. Click in the **By MAC Address**, **By IP Address**, or **By Serial Number** field and type the appropriate value for the DHCT you are testing.

Note: By default, the **Open** and **By MAC Address** options are selected already when you open the DHCT Provisioning window.

7. Click **Continue**. The Set Up DHCT window opens for the test DHCT.

8. Verify that the Admin Status field is set to either In **Service One Way** or **In Service Two Way**.

9. Click the **Secure Services** tab.

10. Scroll through the **Available** field in the **Packages** area of the window and click to select the package that you want the DHCT to be able to access.

Notes:

-
  - You can select more than one package by holding down the **Ctrl** key as you click on each package.
  - If your system uses a Brick package, the DHCT must be authorized for that package as well. This should have been done when the DHCT was staged.

11. Click **Add**. The package name you selected moves into the **Selected** field.

12. In the Options area, make the following selections as appropriate:
    - **IPPV Enable** - If this DHCT uses IPPV services, enable this option and ensure that the credit limit field is set to a non-zero value.
    - **DMS Enable** - Enable this option. Digital Multicast Service is needed to allow the DHCT to receive secure services.
    - **DIS Enable** - If this DHCT uses VOD services, enable this option, otherwise, leave this option disabled. Digital Interactive Service is needed to support VOD service.
    - **Analog Enable** - If this DHCT needs to display secure analog services, enable this option.

Note: Your system and the DHCT must be designed to display secure analog services for this option to work properly. If necessary, refer to the *Analog Descrambling Support for the Digital Broadband Delivery System Application Guide* for details. To obtain a copy of this publication, see **Printed Resources**.

- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs during staging. For more information, refer to the *Explorer Digital Home Communications Terminal Staging Guide*. To obtain a copy of this publication, see **Printed Resources**.
- **Location** - Leave these fields blank or enter a 0 (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.

13. Click **Save**. The system updates the database with the information you entered for this DHCT.

14. Click **DHCT Instant Hit**. The system displays **Instant Hit succeeded** and sends the necessary EMMs to the DHCT.

15. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

16. Click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console.

17. Your next step is to verify that the service was set up successfully by trying to access the service.

Back to top

Verify a Successful Service Setup

After you authorize a DHCT for a service, you can try to access the service to verify that you set it up correctly.

Before You Begin

Wait at least 15 minutes after setting up a new service to perform this test to allow the DHCT time to receive the new service information.

Time To Complete

Testing a service takes approximately 5 to 10 minutes to complete.

Performance Impact

Testing a service does not impact network performance. You can complete this procedure any time after the DHCT has had a chance to receive the service information (usually within 15 minutes).

Procedure

Complete these steps to verify that you have successfully set up a particular service.

1. Make sure the DHCT is connected to a television and to an RF feed into your network.
2. Make sure the DHCT and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.

   Note: For assistance adding a service to a channel map, see *SI-Server Complete SI Solution User Manual.* To obtain a copy of this document, go to **Printed Resources**.

4. Does the service appear as expected?

- If **yes**, go to step 5.
- If **no**, go back to the appropriate service setup instructions and verify that you completed all the procedures correctly. If you need assistance, contact technical support.

5. Is this a PPV service?

4.
- If **yes**, attempt to purchase an event, then go to step 6.
- If **no**, you are finished testing the service.

5. Were you able to successfully purchase an event?
- If **yes**, you are finished testing the service.
- If **no**, go back to the appropriate service setup instructions and verify that you have completed all procedures correctly. If you need assistance, contact technical support.

Back to top

Locate a DHCT MAC Address

To locate the MAC address of a DHCT, do one of the following:

- Display **Page 1** of the DHCT diagnostic screens.
- Look on the back of the DHCT for a label with the MAC address recorded on it.

Delete a Service

Delete a Service from the SAM

Quick Path:
DNCS Administrative Console > Application Interface Modules tab > SAM Service > [Service Name] > File > Delete

To remove a service from your system, you must delete the service from the SAM.

Before You Begin

Before you remove a service from the SAM, you must first delete the service from the channel map(s) where it appears. Otherwise, all of the DHCTs that tune to that channel may lock up and reboot. For assistance, see *SI-Server Complete SI Solution User Manual.* To obtain a copy of this document, go to **Printed Resources**.

Time To Complete

Deleting a service from the SAM takes approximately 5 minutes to complete.

Back to top

Performance Impact

Deleting a service from the SAM does not impact network performance. You can complete this procedure at any time.

Back to top

Deleting a Service from the SAM

Complete these steps to delete a service from the SAM.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **SAM Service**.
3. In the SAM Service List window, select the service you want to delete.
4. Click **File** and choose **Delete**. A confirmation window opens.
5. Click **Yes** to delete the service from the SAM. The service is removed from the system.
6. Clean up sources, sessions, and segments associated with the deleted SAM service as needed. Any sources, sessions, and segments associated with a deleted SAM service remain active unless you manually delete the source, session, or segment. In addition, any package that contains a segment associated with the deleted SAM service continues to contain that segment unless you manually delete the segment from the package.

Back to top

Configure the EMM Carousel

Overview

The rate at which Refresh EMMs are sent out has been increased. The enhancements included in SR i4.3 allow the DNCS to support up to a maximum of 25 set-tops per second (2 million set-tops a day). A Staging Carousel has also been added. In addition, new variables are available to allow system operators to manage EMM bandwidth dynamically between the following contributing sources.

 **Important:** In order for this feature to function properly, the following environment variables must be added to the /export/home/dncs/.profile file:

export CAM_INSTANT_HIT_MULTIPLE_ENABLE = TRUE
export CAM_INSTANT_HIT_MULTIPLE_NUMBER = # of times the instant hit should be repeated
export CAM_INSTANT_HIT_MULTIPLE_DELAY = delay (in seconds) between the instant hit repeat

Add the Environment Variables to Support EMM Carousel Improvements

For systems upgrading from release 1.4.2 or earlier, 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 entry 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 the 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]

   Notes:

   - Replace the number with the numeric value for how many times the instant hit should be repeated.

   - Replace delay with 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. Go to Configuring the EMM Carousel.

Configuring the EMM Carousel

Quick Path:
DNCS Administrative Console > Network Element Provisioning > QPSK/CMTS/OIT

After the appropriate environment variables have been added and the system is configured properly, allocate the bandwidth for the EMM carousel based on the recommendation as follows.

1. On the DNCS Administrative Console, click **Network Element Provisioning.**
2. Click **QPSK/CMTS/OIT**. The QPSK/CMTS/OIT List window opens.
3. Select an OIT bridge, click **File**, and then select **OIT Bandwidth Config**. The Bandwidth Management for OIT PIDs window opens.

4. Enter the recommended bandwidth configuration for the following and then click **Save**.
    - Adhoc EMM Percentage (25%)
    - Staging EMM Percentage (0%)
    - Renewal EMM Percentage (70%)
    - PPV EMM Percentage (5%)
5. Click **Save**.
6. Close the OIT Bandwidth and OIT Bridge windows.

Configuring the Broadcast File System

Overview of Configuring the Broadcast File System

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 section provides steps for configuring the BFS to support applications on set-tops.

Set Up the BFS In-Band Source

Quick Path:
DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Admin

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

Quick Path:
DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Admin

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 **Source Type**, select **BFS**.
11. For the **Transport Type**, select **ASI Out-ofb-and**.
12. For the **Data Rate**, enter **0.01 Mbps**.
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 14 for each new in-band source you need to set up.

Set Up the BFS Server

Quick Path:
DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Admin

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

Quick Path:
DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Admin

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

Quick Path:
DNCS Administrative Console > DNCS tab > Application Interface Modules tab > BFS Admin

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.

Authorizing Features for Set-Tops

Overview of Authorizing Features for Set-Tops

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 section provides procedures for configuring feature authorization.

Creating Named Entitlements

Quick Path:
DNCS Administrative Console > DNCS tab >System Provisioning tab > Package

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

Quick Path:
DNCS Administrative Console > DNCS tab >System Provisioning tab > Package

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

Quick Path:
DNCS Administrative Console > DNCS tab >System Provisioning tab > Package

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

Quick Path:
DNCS Administrative Console > DNCS tab >System Provisioning tab > Package

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

Quick Path:
DNCS Administrative Console > DNCS tab >System Provisioning tab > Package

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 remove 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.

Configuring Multiple Bootloader Carousels

Overview of Configuring Multiple Bootloader Carousels

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 to design the data rate based on the DHCT type and network bandwidth availability.

Setting Up a New Carousel

Quick Path:
DNCS Administrative Console > Application Interface Modules tab > BFS Admin

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 1 Mbps. If you are setting up multiple carousels, keep the following 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 will 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.

Monitoring the System Remotely

Overview of Monitoring the System Remotely

To get the attention of the system operator quickly whenever any of the DNCS process 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 section provides the information you need for configuring your system so that you can monitor it from a remote machine.

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

Configuring State Administration of Radio, Film, and Television (SARFT)

Overview of Configuring State Administration of Radio, Film, and Television (SARFT)

SR i4.3 supports the Chinese government regulatory authority SARFT (State Administration of Radio, Film, and Television). SARFT has access to all cable companies and runs periodic tests to see if the cable providers are complying with the regulatory requirements. SR i4.3 allows the DNCS to generate the SARFT report for the configured number of days.

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 to 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....

   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 of the report XSDs 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.

Configuring the System for Satellite and Terrestrial Support

Overview of Configuring the System for Satellite and Terrestrial Support

To configure your system for satellite and terrestrial support, you must complete the following tasks:

- Enable Satellite and MMDS Feature.
- Enable Network Binding Feature.
- Configure Satellite Hub
- Stage Satellite Set-Tops
- Configure Satellite OIT Bridge. For more information see Configure Satellite OIT Bridge.
- Provision a Cable SCS and MPEG source for satellite transport
- Provision a Cable SCS and MPEG source for MMDS transport
- Configure the Download Setup for Satellite. For more information see Configure the Multiple Download Setup

Configure the Satellite Hub

Quick Path:
DNCS Administrative Console > DNCS tab >Network Element Provisioning tab > 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.
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 appearing in the screen.
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

Quick Path:
DNCS Administrative Console > DNCS tab >Home Element Provisioning tab > DHCT

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

Quick Path:
DNCS Administrative Console > DNCS tab >Network Element Provisioning tab > SCS

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 in the **Primary PCG** field and enter the headend in the **Headend** field.
11. In the **Max Sessions** field, enter the maximum number of sessions this device is allowed to build.
12. Click **Save**.
13. After saving the SCS device, select the SCS and click **Ports for Selected SCS**.
14. Select a port from the SCS Devices screen and click **Ports for Selected SCS**.
15. Click **Add Input Port** and complete the screen.
16. Click **Add Output Port** and complete the screen.
17. Click **Exit** to return to the Administrative Console.
18. Create an MPEG source for this SCS port. See **Set Up MPEG Sources** for details.
19. Make sure the MPEG source for the SCS appears in the list of sources.
20. From the **Network Element Provisioning** tab, click **Satellite/Terrestrial Transport**. The Satellite Transport Parameters window opens.
21. Click **Add New** to add a row to the screen.
22. 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 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.

23. Click **Save**.

Provision a Cable SCS and MPEG Source for MMDS Transport

Quick Path:
DNCS Administrative Console > DNCS tab >Network Element Provisioning tab > Satellite/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 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**.

Set Up Messaging

Set Up Messaging

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 no 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

 **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.

Create a Message Configuration

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Configuration > New

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.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.

3. Click **Messaging**. The Message List window opens.
4. Select **Configuration** then choose **New**. The Create New Configuration Widow opens with the **Urgency*** selection highlighted.

Note: The Urgency*, Message Time*, and Force Tune* parameters are mandatory settings.

5. Type the configuration name in the Configuration Name field.
6. Select the message priority from the Priority drop-down list.

Note: You can select **Normal**, **Emergency**, or **Alert**.

7. Select how the message can be cleared from the **Cleared By** drop-down list.

Note: You can select **User**, **DHCT**, or **System Only**.

8. Click **Message Time*** and type he following settings into the respective fields:
   - Duration (in seconds): The length of time that the message will appear on the on the TV screen
   - Delay Between Repeats (in seconds): The length of time before the message will reappear on the TV screen
   - Number of Repeats: The number of times the message will repeat prior to the expiration time
   - Expiration Time (in minutes): The length of time that the message will remain in the system
9. Click **Force Tune*** and provide the following information in the respective fields:
   - Force Tune: Enables or disables force tuning. Select **NONE** to disable force tuning. Select **Service Id** to enable force tuning
   - 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
   - Power On: Enables the set-top to power on or to remain powered off (in standby mode) when the message is received
   - Lock Channel: Allows the set-top to tune to the force tuned channel if a Service Id is selected
   - Trigger Key: If enabled, allows users to trigger the force tune by pressing a designated key on the remote control
   - Audio PID: When force tuning is enabled, configure this field to determine which audio format should be available for the user
10. Click **Led Alert** and configure the set-top LED blinking rate (cycles/second, duration (seconds), and period (seconds).
11. Click **Display** and use the options available to configure how the message will display on the TV screen

12. Click **Save** to save the configuration.

Create Message Groups

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Group > New

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 Message Parameters

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Parameters > Parameter List

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_TIME 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

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Message > New

1. From the Message List window, select **Message** and then choose **New**. The Create New Message window opens.

2. In the **Target** section, choose one 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 set-tops 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 configured previously.

Delete a Group

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Group > Group List > Delete

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

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Configuration > Configuration List > Delete

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

Quick Path:
DNCS Administrative Console > DNCS tab > System Provisioning tab > Messaging > Message > Open > Retire

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.

External Download Interface Support

Configure External Download Interface Support

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 followng entry in the /export/home/dncs/.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. Go to Enable the External Download Support Feature.

Enable the External Download Support Feature

Enabling the External Download Support Feature requires a special license. Verify that you have this license and then see ***Configuring the PowerKEY DVB System for System Release i4.3 Instructions*** (part number 4036648) for detailed instructions.

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

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

a. Type **dncsStart** and press **Enter**.

Making Changes to Your Network
Headends

Modifying a Headend

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Headend > [Headend Name] > File > Open

You can modify only the name of a headend. You may want to do this, for example, if the name entered previously does not comply with the naming convention established for other elements in your network.

Back to top

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Modify a Headend

Complete these steps to modify the name of a headend in the DNCS database.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Headend**. The Headend List window opens.
4. Click once on the row containing the headend name you want to modify.
5. Click **File > Open**. The Set Up Headend window opens for the headend you selected.
6. Click in the **Headend 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.

7. Click **Save**. The system saves the new headend name in the DNCS database and closes the Set Up Headend window. The Headend List window updates to include the new headend name. Any devices connected to this headend are updated automatically with the new headend name information.
8. Update the headend name on your network map to reflect this change.
9. Do you need to modify another headend?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **File > Close** to close the Headend List window and return to the DNCS Administrative Console. Go to step 10.
10. Continue making any other changes that you need to make to your network.

Back to top

Deleting a Headend

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Headend > [Headend Name] > File > Delete

In a live system, there is usually no reason to delete a headend. Therefore, this procedure is provided for test situations only.

Before You Begin

Before you can delete a headend, you must delete all of the network elements associated with that headend. In addition, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Delete a Headend

Complete these steps to delete a headend from the DNCS.

1. Are there any hubs associated with this headend?
   - If **yes**, delete those hubs first. Go to **Deleting a Hub**. When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **Headend**. The Headend List window opens.
5. Click once on the row containing the headend you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the headend information from the DNCS database and from the Headend List window.
8. Delete the headend from your network map.
9. Click **File > Close** to close the Headend List window and return to the DNCS Administrative Console.
10. Do you need to delete another headend?
    - If **yes**, repeat steps 1 through 9.

9.

- If **no**, continue making any other changes that you need to make to your network.

Back to top

Hubs

Modifying and Deleting Hubs

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > Hub >

After you add a headend to the DNCS database, you must assign at least one hub to that headend. You can have an unlimited number of hubs per headend. 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 modifying or deleting hubs depends on the following possible system configurations:

- Distributed DNCS disabled and network binding disabled
- Distributed DNCS disabled and network binding enabled
- Distributed DNCS enabled and network binding disabled
- Distributed DNCS enabled and network binding enabled

Choose your system configuration and then follow the procedure for modifying or deleting hubs for that configuration.

Back to top

VASPs

Modifying a VASP Entry

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Open

After a VASP entry has been saved in the DNCS, you can modify only the name of the VASP entry and its status of In Service or Out of Service. To change any other parameters, you must delete the VASP entry, and then re-add it to the DNCS, using the new information.

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Procedure

Complete these steps to modify a VASP entry in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VASP**. The VASP List window opens.
4. Click once on the row containing the VASP entry you want to modify.

5. Click **File** and select **Open**. The Set Up VASP window opens for the VASP entry you selected.

6. To change the name of this VASP entry, click in the **Name** field and change the name as desired. You can use up to 80 alphanumeric characters.

   Note: We recommend that you establish a naming scheme that allows you to easily identify the type of server associated with each VASP entry, the hub where the server resides, and the QAM modulator that the server feeds.

7. To change the status of this VASP entry from **In Service** to **Out of Service**, or vice versa, click the desired option so that is selected (**yellow**).

8. When you finish making changes, click **Save**. The system saves the new VASP information in the DNCS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP information.

9. Update your network map to reflect these changes.

10. Do you need to modify another VASP entry?
    - If **yes**, repeat steps 4 through 9.
    - If **no**, click **File** and select **Close** to close the VASP List window and return to the DNCS Administrative Console. Go to step 11.

11. Continue making any other changes that you need to make to your network.

Back to top

Deleting a VASP Entry

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Delete

Use this procedure to delete a VASP entry from the DNCS.

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Procedure

Complete these steps to delete a VASP entry from the DNCS.

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

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

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

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

5. Click **File** and select **Delete**. A confirmation window opens.

6. Click **Yes**. The confirmation window closes. The system removes the VASP entry from the DNCS database and from the VASP List window.

7. Delete the VASP entry to your network map.

8. Do you need to delete another VASP entry?
   - If **yes**, repeat steps 4 through 7.
   - If **no**, click **File** and select **Close** to close the VASP 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.

Back to top

MPEG Content Sources

Modifying an MPEG Content Source

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > [MPEG Source Name] > File > Open

After an MPEG source has been saved in the DNCS, you can modify any of its parameters, except for the headend associated with it and the device type.

 **Important:** Do not attempt to modify or delete an MPEG Home Transport source without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to an MPEG Home Transport source. For assistance, contact technical support.

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Modify an MPEG Content Source

Complete these steps to modify an MPEG source in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **MPEG Source**. The MPEG Source List window opens.
4. Click once on the row containing the MPEG source you want to modify.
5. Click **File > Open**. The Set Up MPEG Source window for the MPEG source you selected opens.
6. Make the desired changes. If you need help completing any fields, refer to the procedure for **Adding an MPEG Source**.

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

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

8. Update your network map to reflect these changes.

9. Do you need to modify another MPEG source?
   - If **yes**, repeat steps 4 through 8.
   - If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console. Go to step 10.

10. Continue making any other changes that you need to make to your network.

Back to top

Deleting an MPEG Content Source

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > MPEG Source > [MPEG Source Name] > File > Delete

Use this procedure to delete an MPEG content source from the DNCS.

Important: Do not attempt to modify or delete an MPEG Home Transport source without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to an MPEG Home Transport source. For assistance, contact technical support.

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Deleting an MPEG Content Source

Complete these steps to delete an MPEG source from the DNCS.

1. Disconnect any elements associated with this source.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **MPEG Source**. The MPEG Source List window opens.
5. Click once on the row containing the MPEG source you want to delete.
6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the MPEG source information from the DNCS database and from the MPEG Source List window.
8. Delete the MPEG source from your network map.

9. Do you need to delete another MPEG source?
    - If **yes**, repeat steps 4 through 7.
    - If **no**, click **File > Close** to close the MPEG Source List window and return to the DNCS Administrative Console. Go to step 9.
10. Continue making any other changes that you need to make to your network.

Back to top

MQAM Modulators

Modifying a Content MQAM Modulator

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [MQAM Name] > File > Open

After an MQAM modulator is saved in the DNCS database, you can modify any of its parameters except for the headend to which it is assigned.

Important: Do not attempt to modify or delete a Home Transport MQAM modulator without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to the Home Transport MQAM modulator. For assistance, contact technical support.

Before You Begin

Before you begin, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Modify a Content MQAM Modulator

Complete these steps to modify a QAM, MQAM, GQAM, or GoQAM modulator in the DNCS.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **QAM**. The QAM List window opens.
4. Click once on the row containing the MQAM modulator you want to modify.
5. Click **File** and select **Open**. The Set Up MQAM window opens, as appropriate.
6. Make the desired changes. If you need help completing any fields, refer to Adding a Content MQAM Modulator.

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

7. When you finish making changes, click **Save**. The system saves the new MQAM modulator information in the DNCS database and closes the Set Up MQAM window. The QAM List window updates to include the new modulator information.

8. Update to your network map to reflect these changes.

9. Do you need to modify another MQAM modulator?
   - If **yes**, repeat steps 4 through 8.
   - If **no**, click **File** and select **Close** to close the QAM List window and return to the DNCS Administrative Console. Go to step 10.

10. Continue making any other changes that you need to make to your network.

Back to top

Deleting a an MQAM Modulator

Quick Path: DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [MQAM] > File > Delete

You can use this procedure to delete any MQAM modulator that carries content.

Important: Do not attempt to modify or delete a Home Transport MQAM modulator without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to the Home Transport MQAM modulator. For assistance, contact technical support.

Before You Begin

Before you delete an MQAM modulator, first tear down all of the sessions associated with the modulator. If you delete a modulator without first tearing down its related sessions, system performance may be degraded. Performance degrades because the DNCS uses its resources attempting to associate sessions with a modulator that no longer exists. Click here to learn how to tear down sessions.

In addition, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Procedure

Complete these steps to delete an MQAM modulator from the DNCS.

1. First tear down all sessions that are running on the modulator you want to delete.
2. On the DNCS Administrative Console, click the **DNCS** tab.
3. Click the **Network Element Provisioning** tab.
4. Click **QAM**. The QAM List window opens.
5. Click once on the row containing the MQAM modulator that you want to delete.

   Note: Even though an MQAM modulator takes up four rows on the QAM List, you need to select only one of the rows to delete it.

6. Click **File > Delete**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes. The system removes the selected modulator information from the DNCS database and from the QAM List window.

8. Delete the selected modulator from your network map.

9. Do you need to delete another QAM modulator?
   - If **yes**, repeat steps 5 through 8.
   - If **no**, click **File > Close** to close the QAM List window and return to the DNCS Administrative Console. Go to step 10.

10. Continue making any other changes that you need to make to your network.

Back to top

Reset an MQAM Modulator

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > QAM > [Select an MQAM modulator] > File > Reset

Important: Do not attempt to modify or delete a Home Transport MQAM modulator without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to the Home Transport MQAM modulator. For assistance, contact technical support.

Resetting an MQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

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

2. When the QAM List window opens, click to select the MQAM modulator that you want to reboot.

   Notes:
   - Each MQAM modulator is listed two times (once for each of the modulator's two RF output channels), but select only the first occurrence.

3. Click **File** and then select **Reset.** The Question window appears with the question, **Are you sure you want to reset QAM modulator 'name of modulator'?**

4. Click **Yes**. The QAM List window displays the following message: **The reset request has been received by QAM modulator 'name of modulator.'**

Back to top

Tear Down Sessions

Quick Path for All Active Sessions for All Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > [Select Session] > Teardown Selected Session

Quick Path for All Active Sessions for Selected Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select QAM Devices] > Display [x] Sessions > [Select Session] > Teardown Selected Session

Important: Before deleting a content modulator MQAM or PCG from the DNCS, first tear down sessions associated with the device. Deleting a MQAM modulator or PCG without first tearing down its related sessions can degrade system performance. Performance can degrade because the DNCS uses its resources to attempt to associate sessions with a modulator that no longer exists. These sessions are called orphaned sessions.

Complete these steps to tear down sessions on an MQAM content modulator or PCG:

1. If you have not already done so, display the appropriate sessions. For assistance, refer to display active sessions.

2. When the list of sessions displays, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete. Or, if you want to tear down all sessions, click **Select All Displayed Sessions**.

   Note: If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.

3. Click **Teardown Selected Sessions**. The system tears down the sessions you selected and updates the status of all sessions.

4. Click **Exit all Session screens** to close the Session Data window.

5. You can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind.

Back to top

PCGs

Modify PCG Provisioning Parameters

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > PCG > [Select a PCG] > Open Selected PCG

After you have created and saved a PCG element, you can modify any of its parameters, except for the following parameters:

- Control NIC MAC Address where the PCG resides
- Maximum PCG Session Count
- ID
- Max streams

Back to top

Modifying PCG Provisioning Parameters

Complete these steps to modify PCG parameters:

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 **Select** button next to the PCG you want to modify.
4. Click **Open Selected PCG**. The Update PowerKEY CAS Gateway window opens.
5. Make the desired changes. If you need help completing any fields, go to Add a PCG Element.
6. When you finish making changes, click **Update**. The system saves the new PCG information in the DNCS database and closes the Update PowerKEY CAS Gateway window. The PowerKEY CAS Gateway window updates to include the new PCG information.
7. Update your network map to reflect these changes.
8. Do you need to modify another PCG element?
   - If **yes**, repeat steps 3 through 7.
   - If **no**, click **Exit** to close the PowerKEY CAS Gateway window and return to the DNCS Administrative Console. Then go to step 9.
9. Continue making any other changes that you need to make to your network.

Back to top

Delete a PCG Element

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > PCG > [Select a PCG] > Delete Selected PCG

This topic describes how to remove a PCG element from the DNCS.

Before You Begin

Before you delete a PCG element, first tear down all of the sessions associated with the PCG. If you delete a PCG without first tearing down its related sessions, system performance may be degraded. Performance degrades because the DNCS uses its resources attempting to associate sessions with a PCG that no longer exists. Click here to learn how to tear down all sessions.

In addition, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Procedure

Complete these steps to delete a PCG from the DNCS.

1. First tear down all sessions that are running on the PCG you want to delete.
2. On the DNCS Administrative Console, click the **DNCS** tab, and then click the **Network Element Provisioning** tab.

3. Click **PCG**. The PowerKEY CAS window opens.
4. Click the **Select** button next to the PCG element you want to delete.
5. Click **Delete Selected PCG**. A confirmation window opens and asks "Are you sure you want to delete the selected PCG?".
6. Click **OK**. The confirmation window closes and the system removes the PCG information from the DNCS database and from the PowerKEY CAS Gateway window.
7. Delete the selected PCG element from your network map.
8. Do you need to delete another PCG element?
   - If **yes**, repeat steps 3 through 7.
   - If **no**, click **Exit** to close the PowerKEY CAS Gateway window and return to the DNCS Administrative Console. Then to step 9.
9. Continue making any other changes that you need to make to your network.

Back to top

Reset a PCG

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > PCG > [Select a PCG] > Reset Selected PCG

Resetting an MQAM modulator from the DNCS reboots the modulator. Follow these steps to reboot a modulator from the DNCS.

1. From the DNCS Administrative Console, click the **DNCS** tab, the **Network Element Provisioning** tab, and then click **PCG**. The PowerKEY CAS Gateway window opens.
2. Click to select the PCG that you want to reset.

3. Click **Reset Selected PCG.** The PowerKEY CAS Gateway window refreshes to indicate that a reset request was sent to the PCG.

Tear Down Sessions on PCGs

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select PCGs in a List] > Display [x] Sessions > [Select Session] > Teardown Selected Session

Important: Before deleting a PCG from the DNCS, first tear down sessions associated with the PCG. Deleting a PCG without first tearing down its related sessions can degrade system performance. Performance can degrade because the DNCS uses its resources to attempt to associate sessions with a PCG that no longer exists. These sessions are called orphaned sessions.

Complete these steps to tear down sessions on PCG:

1. If you have not already done so, display the appropriate sessions. For assistance, refer to display active sessions.

2. When the list of sessions displays, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete. Or, if you want to tear down all sessions, click **Select All Displayed Sessions**.

Notes:

- Do not select PCGs from multiple lists. You can only view sessions for one type of PCG at a time.
- To select a group of PCGs, hold down the **Shift** key while selecting the first and last PCG in the group.
- To select more than one PCG, hold down the **Ctrl** key while selecting each PCG.
- If you make a mistake and select a session that is carried by another PCG, click the **Select** box again to clear your selection.

3. Click **Teardown Selected Sessions**. The system tears down the sessions you selected and updates the status of all sessions.

4. Click **Exit all Session screens** to close the Session Data window.

5. You can now safely delete the PCG that carried these sessions without leaving orphaned sessions behind.

Back to top

SCSs

Update SCS Device Window

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS > [Select an SCS] > Open Selected SCS

The Update SCS Device window provides an at-a-glance status of the parameters for a specific SCS element. From this window, you can modify a the parameters of specific SCS element.

What Would You Like to Do?

- Modify the modeling parameters of an SCS element.
- Modify the modeling parameters of a SCS ports.
- Close the SCS Devices window by clicking **Exit**.

Back to Top

View SCS Parameters

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS > [Select SCS] > Open Selected SCS

You may want to view the parameters of a specific SCS so that you can quickly view or make changes to the parameters. Follow these steps to view the parameters of a specific SCS.

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 the **Select** button for the SCS whose parameters you want to view.
4. Click **Open Selected SCS**. The Update SCS Device window opens for the SCS you selected. From this window, you can complete any of the following tasks:
    - Modify the modeling parameters of an SCS element.
    - Modify the modeling parameters of a SCS ports.
    - Close the SCS Devices window by clicking **Exit**.

Back to Top

Modify SCS Ports

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS > [Select an SCS]

Important: Do not attempt to modify or delete the Home Transport SCS without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to the Home Transport SCS. For assistance, contact technical support.

After you have created and saved SCS ports for an SCS element, you can modify any of the port parameters, except for the input port number. 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 Devices window opens.
3. Click the **Select** button next to the SCS element whose ports you want to modify and select one of the following options:
    - Click **Ports for Selected SCS**. The SCS Ports window opens.
    - Click **Open Selected SCS** and then click **Maintain Ports**. The SCS Ports window opens.
4. Make the desired changes. Make the desired changes to any of the parameters except the Input Port Number. If you need help completing any fields, go to Setting Up SCS Ports Modeling Parameters.

5. When you finish making changes, click **Save**. The system saves this information into the DNCS database and updates the window with the information you entered.

6. Update your network map to reflect these changes.

7. Do you need to modify the ports of another SCS element?
   - If **yes**, **SCS Devices** in the DNCS/SCS Devices/SCS Ports path at the top of the window to display the SCS Devices window. Then repeat steps 3 to 6.
   - If **no**, click **Exit** to close the SCS Devices window and return to the DNCS Administrative Console. Then go to step 8.

8. Continue making any other changes that you need to make to your network.

Back to top

Modify SCS Modeling Parameters

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS > [Select an SCS]

Important: Do not attempt to modify the Home Transport SCS without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our engineers before making changes to the Home Transport SCS. For assistance, contact technical support.

After you have created and saved an SCS element, you can modify any of its modeling parameters, except for the port number and the output TSID. Complete these steps to modify any SCS parameter except for the ID:

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 the **Select** box next to the SCS element you want to modify and click **Open Selected SCS**. The Update SCS Device window opens.

4. Make the desired changes to any of the parameters except the ID parameter. If you need help completing any fields, go to Add an SCS.

5. When you finish making changes, click **Update**. The system saves this information to the DNCS database and closes the Update SCS Device window. The SCS Devices window updates to include this information.

6. Update your network map to reflect these changes.

7. Do you need to modify another SCS element?
   - If yes, repeat steps 3 to 6.
   - If no, click **Exit** to close the SCS Devices window and return to the DNCS Administrative Console. Then go to step 8.

8. Continue making any other changes that you need to make to your network.

Back to top

Delete an SCS Element

Quick Path:
DNCS Administrative Console > DNCS tab > Network Element Provisioning tab > SCS > [Select an SCS]

Important: Do not attempt to delete the Home Transport SCS without our assistance. Certain Home Transport modifications may degrade system performance. For this reason, always consult our support engineers before making changes to the Home Transport SCS. For assistance, contact technical support.

Before you can delete an SCS element, you must first delete any ports and any sessions that have been configured for the SCS element. After the ports have been deleted, you can then delete the SCS element.

Deleting an SCS Element

The following procedure describes how to verify that SCS ports have been deleted from an SCS element and how to then delete the SCS element. Complete these steps to delete an SCS element:

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 the **Select** button next to the SCS element you want to delete, and then click **Ports for Selected SCS**. The SCS Ports window opens.
4. Are any ports present?
   - If **yes**, click the **Select** buttons for all existing ports, and then select **Delete Selected Ports**. The system removes the SCS port information from the DNCS database.
   - If **no**, click **SCS Devices** in the DNCS/SCS Devices/SCS Ports path at the top of the window. The SCS Devices window opens.

   Important: Make certain that all ports are deleted from the SCS element before attempting to delete the SCS element.

5. From the SCS Devices window, click the **Select** button next to the SCS element whose ports you just verified in step 4 , and then select **Delete Selected SCS**. A window opens and prompts you to verify that you want to delete the selected SCS.
6. Click **OK**. The message window closes and the system removes the SCS from the SCS Devices window. This information is saved in the DNCS database.
7. Update your network map to reflect these changes.

8. Do you need to delete another SCS element?
   - If **yes**, repeat steps 3 to 7.
   - If **no**, click **Exit** to close the SCS Devices window and return to the DNCS Administrative Console. Then go to step 9.

9. Continue making any other changes that you need to make to your network.

Back to top

DHCTs

Modifying a DHCT

Quick Path:
DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Open

Use this procedure to modify the settings for an individual DHCT in your network.

Before You Begin

Before you begin, you must have either the MAC address or the serial number of the DHCT you want to modify. In addition, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Back to top

Procedure

Complete these steps to modify the settings for an individual DHCT.

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. In the **Select Option** area, click the **Open** option, if it is not already selected.
5. Do you know the MAC address for the DHCT you want to modify?
   - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the DHCT you want to modify. Go to step 6.
   - If **no**, click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the DHCT you want to modify. Go to step 6.
6. Click **Continue**. The Set Up DHCT window opens for the DHCT you selected.
7. Make the desired changes. If you need help completing any fields, refer to the appropriate staging or upgrade guide for this DHCT model. If you cannot locate these guides, contact technical support.
8. When you finish making changes, click **Save**. The system saves the new DHCT information in the DNCS database.

9. Click **Close** to close the Set Up DHCT window and return to the DHCT Provisioning window.

10. Update your network map to reflect these changes.

11. Do you need to modify another DHCT?
    - If **yes**, repeat steps 4 through 10.
    - If **no**, click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console. Go to step 12.

12. Continue making any other changes that you need to make to your network.

Back to top

Deleting a DHCT

Quick Path:
DNCS Administrative Console > DNCS tab > Home Element Provisioning tab > DHCT > Delete

Use this procedure to delete an individual DHCT from the DNCS.

Before You Begin

Before you begin, you must have either the MAC address or the serial number of the DHCT you want to delete. In addition, you must have your network map readily available. If you cannot locate your network map, contact technical support.

Procedure

Complete these steps to delete an individual DHCT from the DNCS.

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. In the **Select Option** area, click the **Delete** option.
5. Do you know the MAC address for the DHCT you want to delete?
    - If **yes**, click the **By MAC Address** option, then click in the corresponding field, and type the MAC address for the DHCT you want to delete. Go to step 6.
    - If **no**, click the **By Serial Number** option, then click in the corresponding field, and type the serial number for the DHCT you want to delete. Go to step 6.
6. Click **Continue**. A confirmation window opens.
7. Click **Yes**. The confirmation window closes and returns you to the DHCT Provisioning window. The system removes the DHCT information from the DNCS database. If the DHCT is powered on and connected to a television, it will now display encrypted video.
8. Delete the DHCT from your network map.
9. Do you need to delete another DHCT?
    - If **yes**, repeat steps 4 through 8.

- If **no**, click **Cancel** to close the DHCT Provisioning window and return to the DNCS Administrative Console. Go to step 10.

10. Continue making any other changes that you need to make to your network.

Back to top

Monitoring Your Network
DBDS Monitoring Overview

The following topics can help you use tools on the digital network control system (DNCS) to monitor your digital broadband delivery system (DBDS):

DNCS Administrative Console Status window - The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server. In addition, if your DBDS uses Spectrum Network Management System (NMS), you can monitor most of the devices in your network.

Monitoring DNCS Processes - The DNCS Control window provides a list of all the major processes on the DNCS workstation along with the working state of each, giving you an at-a-glance status of the DNCS.

Monitoring SARA Server Processes - The AppServer Control window provides a list of all the major processes on the SARA Server workstation along with the working state of each, giving you an at-a-glance status of the SARA Server.

DHCT Performance - You can monitor DHCT performance by turning on the performance monitoring function. The DHCT performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of DHCTs.

UI Servers - You can obtain an at-a-glance status of DNCS User Interface (UI)I Servers or configure a UI Server.

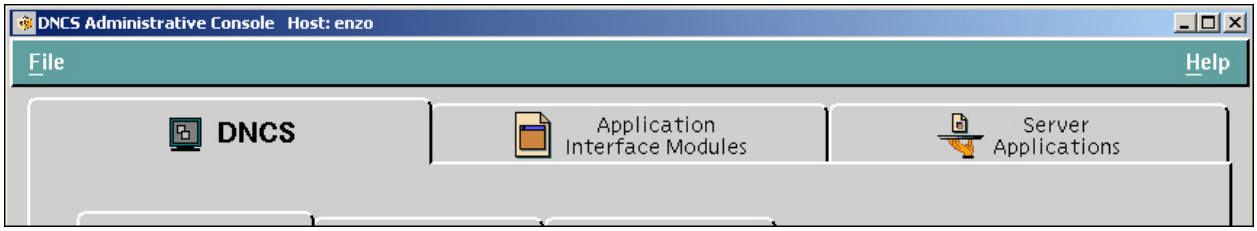
Back to Top

Status at a Glance

DNCS Administrative Console Window

The DNCS Administrative (Admin) Console window is the primary window you use to work with the DNCS. The Admin Console is divided into tabs that allow you to perform activities related to various aspects of the DBDS.

For more information, click on a specific tab in the following illustration.



Back to top

DNCS Administrative Console Status Window

The DNCS Administrative Console Status window helps you determine the status of the DNCS and of the SARA Server.

For more information, click on either the **DNCS** or **AppServer** section in the following illustration.

Back to top

DNCS Status

The **DNCS** section of the Administrative Console Status window indicates whether or not the DNCS software is in operation based on the following conditions:

- *Running* — the DNCS software package is present and in operation
- *Inactive* — the DNCS software package is present, but not in operation

In addition, if you click the **Control** button in the DNCS section, the DNCS Control (or Monitor) window opens, which allows you to monitor all of the major DNCS processes.

Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

Back to top

SARA Server Status

The **AppServer** section of the Administrative Console Status window indicates whether or not the SARA Server is in operation based on the following conditions:

- *Running* — the SARA Server software package is present and in operation
- *Inactive* — the SARA Server software package is present, but not in operation
- *Not Responding* — the SARA Server does not respond when the DNCS tries to communicate with it
- *Not Installed* — a SARA Server host is defined in the host table, but the SARA Server software package is not present; usually indicates that you are not using the SARA Server, but the application server of another vendor
- *Blank* — no SARA Server host is defined in the host table, and the SARA Server software package is not present; usually indicates that you are not using the SARA Server, but the application server of another vendor

When you click the **Control** (or **Monitor**, depending on how the SARA Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major SARA Server processes.

CAUTION: Do not attempt to start or stop an AppServer process manually unless our technical representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers. Contact technical support.

The SARA Server executes applications, such as those in the following list, that are necessary for providing digital services to subscribers.

- **DHCT config server** (DHCT Configuration Server) - Sends the SetPIN transactions to the DHCT.
- **ppvfileserver** (Pay-per-view File Server) - Generates PPV files for SARA and places those files on the Broadcast File Server.
- **ppvServer** (Pay-per-view Server) - Receives PPV event definitions from the billing system and the PPV UI and stores them in the database. The ppvServer also notifies the ppvfileserver process when it is time for the ppvfileserver to generate updated files.

Note: Other processes that show in the AppServer Control window are not used in the international system.

For more information on the SARA Server, refer to *Configuring the PowerKEY DVB System for System Release i4.3.* To obtain this guide, refer to **Printed Resources**.

Back to top

DNCS Processes

Monitoring DNCS Processes

You can monitor all of the major DNCS processes by clicking the **Control** button in the DNCS area of the DNCS Administrative Console Status window to open the DNCS Control window. The DNCS Control window provides a list of all the major processes on the DNCS workstation, along with the working state of each.

Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

We recommend that you leave the DNCS Control window open and visible at all times to help you monitor your system. For more information on monitoring DNCS processes, click here.

Working States of DNCS Processes

A colored circle in the **State** column indicates the working state of a particular process as described in the following list:

- **Green** — The process as a whole is running, although a subprocess may be paused.
- **Yellow** — The process has not finished starting up or shutting down, or is waiting on a subprocess to finish starting up or shutting down.
- **Red** — The process has stopped or did not start.

After the DNCS is up and running, all of these processes should have a **green** working state. 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.

However, if a process remains in a red or yellow working state, this indicates that the process is not functioning properly. Click here for instructions on the corrective action to take.

CAUTION: Do not attempt to start or stop a DNCS process manually unless our technical representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers. Contact technical support.

Back to top

Descriptions of DNCS Processes

The following table describes each of the processes listed on the DNCS Control window.

Process	Description
bfsRemote	**Broadcast File System (BFS) Remote** — Manages the processes (dataPump processes) that continuously transmit BFS data **Note:** The BFS facilitates delivery of information to DHCTs.
bfsServer	**BFS Server** — Manages the addition and deletion of files from the BFS
bigManager	**Broadband Integrated Gateway (BIG) Manager** — Monitors and manages the operation of BIGs, including establishing sessions and allocating MPEG program-specific information (PSI) **Note:** The international system does not use BIGs.
bossDiagnosticsServer	**Business Operations Support System (BOSS) Diagnostics Server** — Acts as an SNMP proxy agent between the billing system and DHCTs by going through the DNCS to retrieve information from DHCTs for the billing system
bossServer	**BOSS Server** — Communicates with the billing system, the DHCT Manager, and the DNCS Administrative Console
bsm	**Broadcast Segment Manager** — Receives notification from the SI Manager when broadcast sources start, and then forwards the notifications to the Conditional Access (CA) system
caaServer	**CA Authority (CAA) Server** — Creates and sends the CAA and entitlement authorization (EA) entitlement management messages (EMMs) required for staging DHCTs

camAm	**CA Manager (CAM) Authorization Manager** — Creates EMMs for security elements to authorize DHCTs to receive secure events
camAuditor	**CAM Auditor** — Refreshes or creates EMMs on DHCTs, which allow the subscriber to view secure events
camEx	**CAM Exclusive Sessions** — Provides conditional access for VOD sessions; generates interactive session keys (ISKs) for each session and ISK EMMs for delivery to the QAM modulators and DHCTs; generates entitlement control messages (ECMs) for the QAM modulators so they can encrypt these sessions
camFastRefresh	**CAM Fast Refresh** — Queries the database for EMMs, puts the EMMs in files, and puts the files on the BFS (files are refreshed periodically when EMMs are changed in the system); sends staging EMMs over inband BFS to DHCTs that are candidates for the Fast Refresh List
camPsm	**CAM Program Segment Manager (PSM)** — Sends PPV and CA Time-of-Day global broadcast authenticated messages (GBAMs); inserts CA information, including ECMs into the program segment at the QAM modulator level
camTEDChecker	**CAM Transaction Encryption Device (TED) Checker** — indicates whether or not the TED is running as follows: **Green** — the TED is in service and the keys have been initialized **Yellow** — the TED software is running, but the keys have not been initialized **Red** — the TED software is not running For more information about the TED, refer to *Transaction Encryption Device FX Server Installation and Operation Guide*. To obtain a copy of this guide, see **Printed Resources**.
CCardServer	**CableCARD Server** — Creates and maintains the PowerKEY CableCARD Module BFS file of CableCARD Module/host pair authorizations; also provides global configuration information to the CableCARD Module population
dncsSnmpAgent	**DNCS Simple Network Management Protocol (SNMP) Agent -** Retrieves alarms from all network elements, and then sends the alarms to our DBDS Alarm Management System (NMS) or to a third-party NMS. **Note:** For more information about the DBDS Alarm Management System, contact the representative who handles your account.

dncs-snmpd-big dncs-snmpd-qam dncs-snmpd-qpsk	**DNCS SNMP** — Ensures that network elements that are not SNMP-compliant (BIGs and QAM modulators, MQAM modulators and QPSK modulators) can communicate with the network management system through SNMP protocol. In other words, the dncs-snmp acts as a proxy agent for each of these elements. **Note:** SR i4.3 does not use BIGs or QPSK modulators.
drm	**Digital Resource Manager** — Manages the allocation of DBDS resources for setting up sessions
dsm	**Digital Session Manager** — Manages digital video sessions (broadcast and exclusive) on the DNCS
EARS	**Emergency Alert Receiver Server** — SR i4.3 does not use this process.
emmDistributor	**EMM Distributor** — Distributes EMMs to DHCTs over the out-of-band path
eventManager	**Event Manager** — Ensures that events critical to RCS processes are routed to the appropriate processes. For example, when an RNCS/LIONN receives an Emergency Alert Message (EAM), Event Manager is notified of the EAM and passes an “EAM event” on to the MMMserver process on the DNCS. By notifying Event Manager, all appropriate DHCTs—those deployed in the central site as well as those deployed in remote sites-—receive the EAM.
hctmConfig	**Home Communications Terminal (HCTM) Configuration** — Exchanges and periodically transmits user-to-network configuration (UNconfig) information to DHCTs **Note:** UNconfig information is configuration information that is exchanged between the DHCT as the user (U) and the network (N). This information tells DHCTs where to find system information, program information, and so on.
hctmInd	**HCTM Indications** — Handles the periodic UNConfigIndications that were previously part of the hctmConfig process
hctmMac	**HCTM Media Access Control (MAC)** — Verifies connections and disconnections of DHCTs and modulators; associates an Internet protocol (IP) address with each DHCT
hctmProvision	**HCTM Provisioning** — Ensures that setup information is in the database and available for DHCTs
idm	**Inventory and Directory Manager** — Provides a repository for public key certificates for DHCTs and service providers

ippvManager	**Impulse-Pay-Per-View (IPPV) Manager** — Polls DHCTs for PPV information for those orders made using the remote control for the television
ippvReceiver	**IPPV Receiver** — Receives purchased event information from the DHCT, then forwards or returns this information to the billing system upon request
logManager	**Logging Manager** — Enables the configuration of logging levels on a DNCS and RNCS/LIONN through the Logging Summary window on the DNCS
MMMServer	**Multi-Media Message Server** — Used for sending multimedia messages to DHCT(s).
oitRemote	**Out of Band/In Band Translator Remote** — Manages Out of Band/In Band Translator (OIT) data transmission threads for each host computer. oitRemote communicates with the oitServer process to obtain configuration information, such as PIDs and data rates.
oitServer	**Out of Band/In Band Translator Server** — Manages OIT database tables, which store configuration information such as PIDs and data rates. oitServer also communicates with the oitRemote process to handle distribution of the OIT transmission functions.
osm	**Operating System (OS) Manager** — Allows you to load image files into the BFS that can then be distributed to DHCTs (for example, OS images, resident application images, and other application images)
PassThru	**PassThru** — Sends pass-thru Digital Storage Media Command and Control (DSM-CC) messages to DHCTs
pkeManager	**PowerKEY Element Manager** — facilitates the management of PowerKEY Control Gateways and Netcrypt Bulk Encryptors
qamManager	**Quadrature Amplitude Modulation (QAM) Manager** — Delivers setup information to QAM, MQAM, and GQAM modulators
qpskManager	**Quaternary Phase-Shift Keyed (QPSK) Manager** — SR i4.3 does not use this process.
ResAppServer	**Resident Application Server** — Provides miscellaneous services for the SARA Server, including access to data in the DNCS database
saManager	**Service Application Manager** (more commonly referred to as *SAM*) — Defines a service, which is the combination of an

	application (WatchTV, music, PPV, and so forth) and the application parameters (source number, URL, and so forth)
sgManager	**Service Group Manager** — Provides information about service groups to VOD servers and DHCTs as follows: • Places data onto a BFS carousel that a DHCT can access to automatically determine to which service group the DHCT belongs • Provides data to servers through either SNMP or a flat file; in either case, a server can use the data to determine which modulator the server should use to send data to a specific service group
siManager	**System Information (SI) Manager** — Facilitates the distribution of SI tuning table information to MQAM modulators.
sseManager	SR i4.3 does not use this process.

Back to top

Stopping DNCS Processes

Complete these steps to stop all of the processes on the DNCS.

CAUTION: When DNCS processes are stopped, two-way communication also stops in the DBDS. You will not be able to offer any PPV services during this time. In addition, you will be able to offer only limited EPG functionality, and you will not be able to stage DHCTs.

Important: If you are restarting the DNCS, complete this procedure only after you stop the network management system and the SARA Server processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click the **Control** button in the DNCS area.

   Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

   The DNCS Control (or Monitor) window opens with a list of all the DNCS processes and their working states. A *green* working state indicates that a process is running.

2. Use the mouse to place the cursor on any open area on the DNCS desktop, but not on the DNCS Administrative Console, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **DNCS Stop**. The DNCS begins shutting down all of its processes. This process can take from 5 minutes to an hour to complete depending on the size of your system, how many sessions are active, and so forth. When finished, all of the processes listed on the DNCS Control window should have a *red* working state, which indicates

that they are not running. In addition, the DNCS area of the DNCS Administrative Console Status window will change to "Inactive."

4. Open an xterm window on the DNCS.

5. At the prompt, type **dncsControl** and press **Enter**. The Dncs Control main menu opens in another xterm window.

6. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all DNCS processes, along with their current working states ("running" or "stopped").

7. Press **Enter** to update the working states of the DNCS processes. Continue to press **Enter** every few seconds until all processes show **Curr Stt: stopped(1)**.

Important: Do not go to the next step until all processes are stopped.

8. Type **x** and press **Enter** to return to the Dncs Control main menu.

9. Type **x** and press **Enter** again to close both the Dncs Control main menu and the second xterm window.

10. Are you in the process of restarting the DNCS?
    - If **yes**, your next step is to restart all DNCS processes.
    - If **no**, you are finished with this procedure.

Back to top

Restarting DNCS Processes

After you stop all of the processes on the DNCS, complete these steps to restart them.

Important: You must restart the DNCS and its processes in the correct order. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click the **Control** button in the DNCS area. The DNCS Control window opens with a list of all the DNCS processes and their working states. A *red* state indicates that a process is not running.

   Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

2. Use the mouse to place the cursor on any open area on the DNCS desktop, but not on the DNCS Administrative Console, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **DNCS Start**. On the DNCS Control window, all of the processes change to a *green* state, which indicates that they are running.

   Note: It may take several minutes before all processes show a green state. Do not go to the next step until all of the processes are in a green state.

4. Your next step is to restart all of the processes on the SARA Server.

Back to top

SARA Application Server Processes

Monitoring SARA Server Processes

You can monitor all of the major SARA Server processes by clicking the **Control** button in the AppServer area of the DNCS Administrative Console Status window to open the AppServer Control window.

The AppServer Control window provides a list of all the major processes on the SARA 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 your system.

Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

For assistance on monitoring SARA Application Server processes, refer to *Configuring the PowerKEY DVB System.* To obtain this guide, see **Printed Resources**.

Back to Top

Stopping SARA Server Processes

Complete these steps to stop all of the processes on the SARA Server. If you are using an application server from another vendor, stop your application server according to the vendor's instructions.

1. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.
2. Click the left mouse button and select **xterm**. An xterm window opens.
3. At the prompt, type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
4. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all SARA Server processes, along with their current working states ("running" or "stopped").
5. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.
6. Click the left mouse button and select **App Serv Stop**. The SARA Server begins shutting down all of its processes. This takes approximately 2 minutes to complete.
7. Press **Enter** to update the working states of the SARA Server processes. Continue to press **Enter** every few seconds until all processes show **Curr Stt: stopped(1)**.

Important: Do not go to the next step until all processes are stopped.

8. Are you restarting the DNCS?
   - If **yes**, your next step is to stop all of the processes on the DNCS.
   - If **no**, you are finished with this procedure.

Back to top

Restarting SARA Server Processes

Complete these steps to restart all of the processes on the SARA Server. If you are using an application server from another vendor, restart your application server according to the vendor's instructions.

Important: If you are in the process of restarting the DNCS, complete this procedure only after you restart all the DNCS processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. Is the xterm window open on the SARA Server that shows the working states of all SARA Server processes?
   - If **yes**, go to step 6.
   - If **no**, go to step 2.

2. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **xterm**. An xterm window opens.

4. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.

5. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. A list appears of all the SARA Server processes and shows their current working states.

6. Do all processes show **Curr Stt: running(2)**?
   - If **yes**, go to step 12.
   - If **no**, go to step 7.

7. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.

8. Click the left mouse button and select **App Serv Start**. The SARA Server begins to restart all of its processes. This takes approximately 2 minutes to complete.

9. Press **Enter** every few seconds to update the working states until all processes show **Curr Stt: running(2)**.

10. Type **x** and press **Enter** to return to the Applications Control main menu.

11. Type **x** and press **Enter** again to close both the Applications Control main menu and the second xterm window.

12. In the first xterm window, type **exit** and press **Enter** to close the first xterm window.

Back to top

Session List

Session List

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List

The Session Filter window displays lists of QAM modulators, PCGs, and servers organized by type. These organized lists make it easier for you to find specific devices for session monitoring.

After you display the sessions you are interested in, you can perform a variety of tasks, such as viewing details for a specific session or tearing down sessions.

What Would You Like to Do?

From the Session Filter window, you can perform any of the following tasks for the devices in your system that carry sessions:

- Display active sessions by type.
- Display active and completed session by type.
- Display unlisted active sessions.
- Close the Session Filter window by clicking **Exit**.

Back to Top

Display Active Sessions

Quick Path for All Active Sessions for All Modulators/PCGs in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions

Quick Path for All Active Sessions for Selected Modulators/PCGs in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select QAM Modulators/PCGs/Servers in a List] > Display [x] Sessions

The Session List displays all QAM modulators, PCGs, and servers in your system that are currently carrying at least one session. To make it easy to find sessions on a specific device, devices are organized into separate lists by type.

You can display active sessions for a specific device or group of devices within the same list. You can also display active sessions for all devices in a list.

Follow these steps to display active sessions in your system.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.

3. Click **Session List**. The Session Filter window opens and lists all of the QAM modulators, PCGs, and servers in your system that are currently carrying at least one session.

4. Complete *one* of the following steps.
    - To view active sessions for a few specific devices select the devices from the appropriate list.

      Notes:

        - Do not select devices from multiple lists. You can only view sessions for one type of device at a time.
        - To select a group of devices hold down the **Shift** key while selecting the first and last device in the group.
        - To select more than one device, hold down the **Ctrl** key while selecting each device.
    - To view active sessions for *all* devices in a list, do not make any selections.
    -

5. From the left navigation pane, click the appropriate menu option for the sessions you want to view. For example, if you are interested in sessions on PCGs, click **Display PCG Sessions**. The Session Filter window closes, and the Session Data window opens and lists the *active* sessions for the appropriate PCGs. From this window, you can perform any of the following tasks:
    - Learn about the data shown in the Session Data window.
    - Display details about a selected session.
    - Display elements of a selected session, such as the devices that process the session.
    - Display active and completed sessions.
    - Display information about session resources.
    - Tear down selected sessions.
    - Filter the sessions to display only sessions of a particular type and status.
    - Close the Session Data window by clicking **Exit**.

Back to Top

Display Active and Completed Sessions

Quick Path for Active and Completed Sessions for All Modulators in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > Display All [x] Sessions

Quick Path for Active and Completed Sessions for Selected Modulators in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select QAM Modulators/PCGs/Servers in a List] > Display [x] Sessions > Display All [x] Sessions

The Session List window displays all QAM modulators, PCGs, and servers in your system that are currently carrying at least one session. To make it easier to find sessions on specific devices, devices are organized into separate lists by type. For example, regular QAM modulators are listed separately from table-based QAM modulators.

When you click an option, such as Display QAM Sessions, from the Session List window, only active sessions are listed at first. If you want to view both active and completed sessions, you can easily add completed sessions to the list.

Follow these steps to display active and completed sessions in your system.

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Session List**. The Session Filter window opens and lists all of the QAM modulators and servers in your system that are currently carrying at least one session.
4. Complete *one* of the following steps.
   - To view active sessions for a few specific QAMs, PCGs, or servers, select the devices from the appropriate list.

     Notes:

     - Do not select devices from multiple lists. You can only view sessions for one type of device at a time.
     - To select a group of devices, hold down the **Shift** key while selecting the first and last device in the group.
     - To select more than one device, hold down the **Ctrl** key while selecting each device.
   - To view active sessions for *all* devices in a list, do not make any selections.
5. From the left navigation pane, click the appropriate menu option for the sessions you want to view. For example, if you are interested in PCGs, click **Display PCG Sessions**. The Session Filter window closes, and the Session Data window opens and lists the *active* sessions for the appropriate devices.
6. From the left navigation pane, click the appropriate menu option for the sessions you want to view. For example, if you want to add completed sessions to the list of active sessions for PCGs, click **Display All PCG Sessions**.

Back to Top

Display Unlisted Active Sessions

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display Unlisted Active Sessions

The menu option **Display Unlisted Active Sessions** is helpful with troubleshooting. Selecting this option displays sessions that are listed as "active" and may be functioning, but are not correctly configured. For example, any sessions with an invalid VASP association would display when this option is selected.

To display unlisted active sessions, complete these steps:

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **Utilities** tab.
3. Click **Session List**. The Session Filter window opens and lists all of the devices in your system that are currently carrying at least one session.
4. Click **Display Unlisted Active Sessions**. The Active Sessions Missing VASP Data window opens.
5. To correct these sessions, make note of the following data.
    - Session ID (To find this identifier, locate the Session ID column on the Session List.)
    - MPEG program number (To find this number, select the session and click Display Details of Selected Session.)
6. Then tear down the session and restart it.
7. To close this window, click **Exit**.

Back to top

View Session Data

Session Data Overview

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select Device]

After you display the sessions you are interested in, you can perform a variety of tasks, such as viewing details for a specific session or tearing down sessions.

What Would You Like to Do?

From the Session Data window, you can perform any of the following tasks for the devices in your system that carry sessions:

- Learn about the session data that is displayed.
- Display details about a session.
- Display information about elements or devices that process the session.

- Display all sessions carried on these devices by clicking **Display All <Device Name> Sessions**.
- Select all sessions currently displayed by clicking **Select All Displayed Sessions**.
- Update session data by clicking **Refresh**.
- Tear down selected sessions.
- Filter the sessions to display only sessions of a particular type and status.
- Close the Session Data window by clicking **Exit all Session screens**.

Back to Top

Session Data

When you display information about sessions carried on QAM modulators/PCGs, the DNCS displays the following information about the sessions:

- **Session ID** - Lists the session ID that was assigned by the system administrator when the session was set up. The following colors in the Session ID field indicate the state of the session:
  - **Green** indicates that the session is active.
  - **Blue** indicates that the session has successfully completed.
  - **Red** indicates that the session has failed.
- **Type** - Lists the following types of sessions:
  - **Continuous feed sessions** are used for broadcast or pay-per-view services
  - **Exclusive sessions** are used for video-on-demand (VOD) services
- **State** - Lists the current state of the session. The DNCS lists the following states
  - **Active** sessions are those that are currently running.
  - **Completed** sessions are those that have successfully completed, or have been torn down by the user.
  - **Failed** sessions are those that have stopped running.
- **VASP Name** - Lists the Value Added Service Provider (VASP) that provides a service or functionality to elements of the session.
- **QAM Name, Port, Frequency** - Lists the name of the QAM modulator/PCG-SCS that carries the session, as well as the frequency of the channel being used to send data from the QAM modulator/PCG to the hubs on your system.
- **Start Time** - Lists the time that the session began.
- **Teardown Reason** - Lists the reason that the session has been torn down, for example, "user initiated."

Back to Top

Display Details About a Session

Quick Path for All Active Sessions for All Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > [Select Session] > Display Details of Selected Session

Quick Path for All Active Sessions for Selected Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select Devices] > Display [x] Sessions > Display Details of Selected Session

Follow these instructions to display information about a specific session.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to one of the following procedures:
   - Display active sessions
   - Display active and completed sessions

2. When the list of sessions displays, click the **Select** box next to the session that you want to examine in more detail.

3. Click **Display Details of Selected Session**. A window opens and displays details about the resources associated with the selected session.
   - **MPEG Program number of the session** - The MPEG program number given to this session when it was built.
   - **PMT PID** - The packet identifier (PID) that carries the program map table (PMT) for this program. The PMT gives details about a program and the elementary streams that comprise it.
   - **PCR PID** - The PID that carries the program clock reference (PCR) for this program so the DHCT can synchronize video and audio elementary streams.
   - **ECM PID** - The PID that carries the entitlement control message (ECM) for the program. ECMs enable an event to be encrypted for transmission to a DHCT and allow the event to be decrypted by the DHCT if the DHCT is properly provisioned. ECMs are generated by the DBDS whenever a package starts and its segments are active.

   Note: A PID distinguishes transport packets containing the data of one elementary stream from those carrying the data of other elementary streams.

4. When you have finished examining the details, you can perform either of the following tasks:
   - To close the Session Details window, click **Exit all Session screens**.
   - To view details about a resource, go to Display Details About a Resource.

Back to Top

Display Session Elements

Quick Path for All Active Sessions for All Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > [Select Session] > Display Elements of Selected Session

Quick Path for All Active Sessions for Selected Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select Devices] > Display [x] Sessions > Display Elements of Selected Session

Follow these instructions to display information about the elements that carry a session.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to one of the following procedures:
   - Display active sessions
   - Display active and completed sessions

2. When the list of sessions displays, click the **Select** box next to the session that you want to examine in more detail.

3. Click **Display Elements of Selected Session**. A window opens and displays details about the elements that process the session.

   - **Device Name** - the name of the element that carries the session
   - **Input Port** - the number of the port that receives the session
   - **Input TSID** - the identifier of the transport stream as it enters the device that carries this session
   - **Input MPEG Program Number** - the number of the MPEG program as it enters the device
   - **Output Port** - the number of the port where the session exits the device
   - **Output TSID** - the identifier of the transport stream as it exits the device that carries this session
   - **Output MPEG Program Number** - the number of the MPEG program as it exits the device

4. To close the Session Details window, click **Exit all Session Screens.**

Back to Top

Display Details About a Resource

Quick Path for All Active Sessions for All Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > [Select Session] > Display Details of Selected Session > [Select Resource] > Display Selected Resource Details

Quick Path for All Active Sessions for Selected Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select QAM Devices] > Display [x] Sessions > Display Details of Selected Session > [Select Resource] > Display Selected Resource Details

Follow these instructions to display details about the resources for a specific session.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to one of the following procedures:

- Display active sessions
- Display active and completed sessions

2. When the list of sessions displays, click the **Select** box next to the session that you want to examine in more detail.

3. Click **Display Details of Selected Session**. A window opens and displays details about the session.

4. Click the **Select** box next to the resource that you want to examine.

5. In the Resources area, click the **Select** box next to any of the following resources that you want to examine:

- MPEG program resources of the server and client
- Downstream transport stream resources of the server and client
- Headend resources

6. Click **Display Selected Resource Details**. A window opens and displays details about the resource.

Note: The details that display vary according to the resource you select. The following lists all possible details in alphabetical order for easy reference.

- **Allocation Time** - A time stamp indicating when the session-setup request is sent to the DNCS.
- **Bandwidth** - The amount of bandwidth used by the selected transport stream ID (TSID).
- **Headend Flag** - The headend that transmits the session to the access network. A value of 1 indicates the headend named by the headend ID.
- **Headend NSAP** - The network service access point address of the headend transmitting the session.
- **PCR PID** - The PID that carries the program clock reference (PCR) for this program so the DHCT can synchronize video and audio elementary streams.
- **PMT PID** - The packet identifier (PID) that carries the program map table (PMT) for this program. The PMT gives details about a program and the elementary streams that comprise it.
- **Program Number** - The number of the MPEG program that the session carries
- **Rel Time** - A time stamp indicating when session resources are released by the DNCS
- **Resource Number** - The number assigned to the resource you selected.
- **Resource State** - The current state of the resource you selected. The following lists possible values.

- Active = sessions that are currently running.
- Completed = sessions that have successfully completed, or have been torn down by the user
- Failed = sessions that have stopped running

- **Session ID** - The session identifier for the selected resource.
- **TSID** - The number identifying the transport stream that carries the session.

7. Do you want to view details of another resource?
   - If **yes**, click **Session Resources** from the navigation path at the top of the window. Then repeat steps 4 and 5 to display the details of another resource.
   - If **no**, click **Exit all Session screens** to close the Resource Details window.

Back to Top

Tear Down Sessions

Quick Path for All Active Sessions for All Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > [Select Session] > Teardown Selected Session

Quick Path for All Active Sessions for Selected Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select QAM Devices] > Display [x] Sessions > [Select Session] > Teardown Selected Session

Important: Before deleting a content modulator MQAM or PCG from the DNCS, first tear down sessions associated with the device. Deleting a MQAM modulator or PCG without first tearing down its related sessions can degrade system performance. Performance can degrade because the DNCS uses its resources to attempt to associate sessions with a modulator that no longer exists. These sessions are called orphaned sessions.

Complete these steps to tear down sessions on an MQAM content modulator or PCG:

1. If you have not already done so, display the appropriate sessions. For assistance, refer to display active sessions.

2. When the list of sessions displays, click in the **Select** box to the left of one or more sessions to select all of the sessions that you want to delete. Or, if you want to tear down all sessions, click **Select All Displayed Sessions**.

   Note: If you make a mistake and select a session that is carried by another modulator, click the **Select** box again to clear your selection.

3. Click **Teardown Selected Sessions**. The system tears down the sessions you selected and updates the status of all sessions.

4. Click **Exit all Session screens** to close the Session Data window.

5. You can now safely delete the modulator that carried these sessions without leaving orphaned sessions behind.

Back to top

Filter Sessions

Quick Path for All Active Sessions for All Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > Display [x] Sessions > Define Session Filter

Quick Path for All Active Sessions for Selected Devices in a List:
DNCS Administrative Console > DNCS tab > Utilities tab > Session List > [Select QAM Devices] > Display [x] Sessions > Define Session Filter

Follow these instructions to display sessions according to their type and status.

1. If you have not already done so, display the appropriate sessions. For assistance, refer to one of the following procedures:
   - Display active sessions
   - Display active and completed sessions

2. When the list of sessions opens, click **Define Session Filter**. The Filter displays at the top of the window.

3. Click the **Session Type** arrow and select the type of sessions that you want to view. Choose from the following options:
   - **All** displays all types of sessions.
   - **Continuous Feed** displays uninterrupted content sessions used for broadcast or pay-per-view services, and uninterrupted BFS sessions
   - **Exclusive** displays sessions used by interactive services, such as VOD.
   - **Partially Encrypted** displays sessions that are partially encrypted.

4. Click the **Session Status** arrow and select the status that you want to view. Choose from the following options:
   - **All** displays sessions regardless of their status.
   - **Active** displays only sessions that are running.
   - **Failed** displays only sessions that have stopped running.

5. Click **Filter**. The Session Data window opens and displays sessions according to the parameters you selected in steps 3 and 4.

6. What do you want to do next?
   - To display sessions according to another type and status, click **Define Session Filter** and repeat steps 3 and 4.
   - To close the Session Data window, click **Close**.

Back to Top

Restart a Session

Quick Path:
DNCS Administrative Console > System Provisioning tab > Source > [Select Source for Session] > File > Source Definition > [Select Source Definition] > Start Session > [Follow Set Up Digital Source Definition Window Prompts]

After you tear down a session, follow this procedure to restart it from the Set Up Digital Source Definition window. Tearing down and restarting a session is helpful in correcting unlisted, active sessions.

Note: Restarting a session from the Set Up Digital Source Definition window automatically opens the Define Session window with predefined values for most settings based on the data you used to set up the session. This method allows you to easily identify and change any incorrect information as you use the Define Session window to restart the session with correct parameters.

1. On the DNCS Administrative Console, click the **System Provisioning** tab.
2. Click **Source**. The Source List window opens.
3. Select the source for the session, click **File** and choose **Source Definition**. The Source Definition List opens for the source you selected.

   Note: You can find the source for a session by looking through the Source ID column to find the ID that corresponds to the session ID.

4. Select the source definition with the status of Tear Down and click **File** and choose **Open**. The Set Up Digital Source Definition window opens for the source definition you selected.
5. Click **Start Session**. The Define Session window opens.
6. If necessary, select the correct source type, and then click **Next**. The Session Setup window opens.
7. If necessary, select the correct input device, and then click **Next**. The Select Outputs window opens.
8. Select the modulator or PCG that will receive content from this source and click **Next**. The Wrap-Up window opens and displays settings and values for the device.

   Note: To select more than one modulator or PCG, hold down the **Ctrl** key on your keyboard as you click on each modulator or PCG.

9. Verify that the values shown are correct and click **Next**. The Save Source Definition window opens.

   Note: If any values are incorrect, change them.

10. Click **Save**. The system saves the source definition in the DNCS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

Back to top

DHCT Performance

Monitoring DHCT Performance

You can monitor the DHCT performance by turning on the performance monitoring function. Monitoring this performance can help you in troubleshooting your system should the need arise. The DHCT performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of DHCTs. When you activate the DHCT performance monitoring feature, the system records information in the following files:

- hctmcfgperfmon.csv
- hctmmacperfmon.csv
- hctmprovperfmon.csv

After performance monitoring is activated, the system checks these files every reporting cycle to see if any data information has changed. If so, the system updates the information.

Important: Before you can activate DHCT performance monitoring for the first time, you must create the **hctmpm.time** file in the / dvs/dncs/ tmp/PerformanceMonitoring directory.

What Would You Like to Do?

- Create the hctmpm.time file.
- Activate DHCT performance monitoring or modify the reporting interval.
- De-activate DHCT performance monitoring.
- Read DHCT performance report files.

Back to top

Monitoring DHCT Performance

You can monitor the DHCT performance by turning on the performance monitoring function. Monitoring this performance can help you in troubleshooting your system should the need arise. The DHCT performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of DHCTs. When you activate the DHCT performance monitoring feature, the system records information in the following files:

- hctmcfgperfmon.csv
- hctmmacperfmon.csv
- hctmprovperfmon.csv

After performance monitoring is activated, the system checks these files every reporting cycle to see if any data information has changed. If so, the system updates the information.

Important: Before you can activate DHCT performance monitoring for the first time, you must create the **hctmpm.time** file in the / dvs/dncs/ tmp/PerformanceMonitoring directory.

What Would You Like to Do?

- Create the hctmpm.time file.
- Activate DHCT performance monitoring or modify the reporting interval.
- De-activate DHCT performance monitoring.
- Read DHCT performance report files.

Back to top

Creating the hctmpm.time File

Before you can activate DHCT performance monitoring for the first time, you must create the **hctmpm.time** file in the /dvs/dncs/tmp/PerformanceMonitoring directory.

Caution: Do not delete this file after you create it. Doing so could make future monitoring efforts difficult.

Complete these steps to create the hctmpm.time file.

Note: UNIX commands are case-sensitive.

1. Open an xterm window.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **print "0" > hctmpm.time** and press **Enter**. A prompt appears.

The zero ("0") in the previous command indicates the number of seconds between reporting intervals. Any value that is 10 or less indicates that DHCT performance monitoring is turned off. Every three minutes (180 seconds), the DNCS checks to see if DHCT performance monitoring is turned on.

Back to top

Activating or Modifying DHCT Performance Monitoring

After you create the hctmpm.time file, you can complete these steps to activate DHCT performance monitoring. You can also use these steps to modify the reporting intervals.

Note: UNIX commands are case-sensitive.

1. Open an xterm window.
2. Type **cd / dvs/dncs/ tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **vi hctmpm.time** and press **Enter**. The system opens the hctmpm.time file.
4. Replace the value in the top line with any number greater than 10 based on how many seconds you want the system to check for DHCT data transactions. For example, if you want the system to perform this check every 5 minutes, you would type **300**.

Note: Any value of 10 or less de-activates DHCT performance monitoring.

5. Type **:wq** and press **Enter**. The system saves your change and closes the hctmpm.time file. A prompt appears.

6. Type **exit** and press **Enter**. The xterm window closes.

Back to top

De-Activating DHCT Performance Monitoring

Complete these steps to de-activate DHCT performance monitoring.

Note: UNIX commands are case-sensitive.

1. Open an xterm window.
2. Type **cd / dvs/dncs/ tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Type **vi hctmpm.time** and press **Enter**. The system opens the hctmpm.time file.
4. Replace the value in the top line with any number that equals 10 or less.

5. Type **:wq** and press **Enter**. The system saves your change and closes the hctmpm.time file. A prompt appears.

6. Type **exit** and press **Enter**. The xterm window closes.

Back to top

Reading DHCT Performance Report Files

When you turn on the DHCT performance monitoring feature, the system records the number of certain types of data transactions in the following files:

- hctmcfgperfmon.csv
- hctmmacperfmon.csv
- hctmprovperfmon.csv

The fields in these files are separated by commas, hence the " csv" (comma-separated-values) designation. Separating the fields by commas allows you to view this information in Microsoft Excel, if you wish.

Each line in these files begins with a date/time stamp, which indicates when the information was gathered. The first line is a header that describes the content of the columns in the lines that appear below the header.

For example, the hctmcfgperfmon.csv file shows reported information in the following format:

04-30-2003 13:28:01,number of UN config receive requests,number of UN config request confirms,number of config input queue full detected
04-30-2003 13:28:31,33,0,0

The first line of the preceding example shows that DHCT performance monitoring was activated on 4-30-2003 at 13:28:01. The data being reported includes the following:

- Number of UN config receive requests
- Number of UN config request confirms
- Number of config input queue full detected

The second line shows that 30 seconds later, at 13:28:31, there were 33 UN config receive requests, zero UN config request confirms, and the config input queue was never detected as full during this reporting interval. While this data alone may not be a clear indication of trouble, data gathered and compared over time may help to assist in troubleshooting.

Back to top

Monitored DHCT Data Transactions

The DHCT performance monitoring feature reports on the following data transactions for the hctmConfig, hctmMac, and hctmProvision processes.

Process	Monitored Transactions
hctmConfig	• Number of " UNConfig receive" requests • Number of " UNConfig request" confirms • Number of times the config input queue was detected as full
hctmMac	• Number of DAVIC connections made • Number of DAVIC connections lost • Number of "verify request" received • Number of "verify response sent" • Number of "verify response sent" errors • Number of "verify request received sent to provisioning" • Number of times hctmMac input queue was detected as full
hctmProvision	• Number of "verify request received by provisioning" • Number of "verify response sent" • Number of "verify response sent" errors

This information is reported in the hctmcfgperfmon.csv, hctmmacperfmon.csv, and hctmprovperfmon.csv files, respectively.

Back to top

Reset the PIN on a DHCT

Quick Path:
DNCS Administrative Console > Server Applications tab >DHCT Config

Complete the following procedure 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.

Note: Make sure that the variable PKDVB_APPSERV_NOT_PRESENT is set to 1 (one) in the /export/home/dncs/.profile file.

1. Is your system configured with the Application Server?
    - If **yes**, go to step 2.
    - If **no**, go to step 7.
2. On the DNCS Administrative Console, select 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.
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.

GUI Servers

UI Server Manager

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers

The UI Server Managers window provides an at-a-glance status of the Managers that monitor UI Servers. UI Server Managers monitor groups of UI Servers. If a UI Server stops

unexpectedly, its Manager automatically restarts the UI Server. From this window, you can also modify the Managers listed in it so that you can more easily manage the UI Servers of your system.

Note: UI servers provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console.

Back to Top

What Would You Like to Do?

- Check the status of applications (UI Servers) belonging to a UI Server Manager.
- Add a new Server Manager.
- Modify a Server Manager.
- Delete a Server Manager.
- Update the data about your UI Server Managers by clicking **Re-read configuration file**.

Back to Top

Check the Status of Managers

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers

Follow these steps to view the status of UI Servers belonging to a particular Manager:

1. From the DNCS Administrative Console, click the DNCS tab if it is not already in the forefront.
2. Click the **Utilities** tab.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. The **Manager status** column on the far right provides an at-a-glance status of each Manager. The following lists each possible status for a Manager:
   - **Green** along with the message "**active**" indicates that the Manager process is running. The time indicates the time that Manager started. The number of requests indicates the number of service requests the Manager has processed since it was started.
   - **Red** along with the message "**inactive**" indicates that the Manager process is not running.
   - **Red** and the message "**unknown**" indicate that the status of the Manager process is unknown.
5. To close the Select Server Manager window, click **Close page**.

Back to Top

Add a UI Server Manager

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > Add new Server Manager

From the primary UI management window, you can add a UI Server Manager. Follow these instructions to add a UI Servers Manager.

Note: This action is not normally performed on a production system.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. Click **Add new Server Manager**. The Add Manager Server table appears.
5. Click in the **Server Manager name** field and enter a name for the Manager.
6. Click in the **Manager Host Name** field and enter the name of the host where this Manager resides.
7. Click in the **Manager port** field and type the port number on the DNCS that the Manager will monitor.
8. Click **Add new data**. The Add Manager Server table closes and the new Manager appears in the list.
9. To close the Select Server Manager window, click **Close page**.

Back to Top

Modify a UI Servers Manager

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers

From the primary UI management window, you can modify the parameters listed for a UI Server Manager. Follow these instructions to modify a UI Servers Manager.

Note: This action is not normally performed on a production system.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.

3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. Click in any of the following fields and make your changes.
   - Server Manager Name
   - Manager Host Name
   - Manager port

5. Click **Save Server Manager data**. A confirmation message appears and asks you if you want the system to remember the data you entered for this manager.

6. Click the answer that fits your needs. The message closes, and the system saves your changes.

7. To close the Select Server Manager window, click **Close page**.

Back to Top

Delete a UI Servers Manager

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > Delete selected Server Manager

From the primary UI management window, you can also delete a UI Server Manager. Follow these steps to delete a UI Servers Manager

Note: This action is not normally performed on a production system.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.

2. Click the **Utilities** tab. The Utilities tab moves to the forefront.

3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. Click the **Please select a server manager** button next to the Manager you want to delete.

5. Click **Delete selected Server Manager**. A confirmation message appears and asks you if you want the system to remember the data you entered for this manager.

6. Click the answer that fits your needs. The message closes and another message alerts you that the deletion was successful.

7. Click **OK**. The message closes and the Select Manager Server window opens again.

8. To close this window, click **Close page**.

Back to Top

Manage UI Servers

UI Servers Belonging to a Manager

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > Select Server Manager

From this window, you can obtain an at-a-glance status of each application (UI Server) in your system. UI servers provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console. Modifying some of the settings for a UI server allows system administrators to customize the behavior of a server and better manage your system. This window also allows you to add new UI servers and to modify, delete, or restart existing UI servers.

Back to Top

What Would You Like to Do?

From this window, you can perform any of the following tasks:

- View the status of applications (UI servers) that belong to a Manager.
- Add a new application.
- Modify a new application.
- Delete an application.
- Stop a UI Server.
- Start a UI Server.
- Update data about the UI servers currently shown by clicking **Re-read configuration file**.

Back to Top

Check Status of Applications

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > Select Server Manager

Follow these steps to view the status of UI servers belonging to a particular manager:

Note: Applications (UI servers) provide a link from the DNCS servers and database to the Web servers that provide the actual content for the Web-based windows on the DNCS Administrative Console.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.

3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. In the far left column of this page, click the **Please select a server manager** button next to the Manager whose applications (UI Servers) you want to examine.

5. Click **Select Server Manager**. The Configure UI Servers window opens and lists the applications (UI Servers) belonging to the Manager you selected.

6. To determine the status of each application (UI server), find the **Status** column on the far right and use it to view the status of each application (UI server). The following list describes each possible status for an application (UI server):

- **Green** along with the message "**active**" indicates that the Manager process is running. The time indicates the time that server started up. The number of requests indicates the number of service requests the server has processed since it was started.
- **Red** along with the message "**inactive**" indicates that the Manager process is not running.
- **Red** and the message "**unknown**" indicate that the status of the Manager process is unknown.

7. To close this window, click **Close configuration page**.

Back to Top

Add a New Application

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > Select Server Manager > Add new application

Follow these steps to add a new application (UI server) to a Manager.

Note: This action is not normally performed on a production system.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. In the far left column, click the **Please select a server manager** button next to the Manager to which you want to add an application (UI Server).

5. Click **Select Server Manager**. The Configure UI Servers window opens and lists the applications (UI Servers) belonging to the Manager you selected.

6. Click **Add new application**. The Configure UI Servers table opens.

7. Click in the **Web service name** field and enter a name for the application that provides content for this application (UI Server).

8. Click in the **Host name** field and enter a name for the application (UI Server).

9. Click in the **Host port** field and enter the number of the port that the application (UI Server) monitors.

10. Click **Add new data**. The Configure UI Servers table closes and the new application (UI server) appears in the list.

11. To close this window, click **Close configuration page**.

Back to Top

Modify a New Application

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > Select Server Manager > [Enter Changes] > Save Server Manager Data

Follow these instructions to modify an application (or UI Server).

Note: This action is not normally performed on a production system.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.
4. In the far left column, click the **Please select a server manager** button next to the Manager whose applications (UI servers) you want to modify.
5. Click **Select Server Manager**. The Configure UI Servers window opens and lists the applications (UI Servers) belonging to the Manager you selected.
6. Click in any of the following fields and make your changes.
    - Web service name
    - Host name
    - Host port
7. Click **Save application data**. A confirmation message appears and asks you if you want the system to remember the data you entered for this manager.
8. Click the answer that fits your needs. The message closes, and the system saves your changes.
9. To close this window, click **Close configuration page**

Back to Top

Delete an Application

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > Select Server Manager > [Select Application] > Delete Selected Application

Follow these steps to delete an application (or UI Server) from a Manager.

Note: This action is not normally performed on a production system.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. In the far left column, click the **Please select a server manager** button next to the Manager whose application (UI Server) you want to delete.

5. Click **Select Server Manager**. The UI Servers window appears and lists the applications (UI Servers) belonging to the Manager you selected.

6. Click the **Select** button next to the application (UI Server) you want to delete.

7. Click **Delete selected application**. The application (UI Server) is removed from the list.

8. To close this window, click **Close configuration page.**

Back to Top

Stop a UI Server

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > [Select UI Server] > Stop selected UI Server

Sometimes you may need to stop and restart a UI server. For example, if the database is brought down and restarted, you will need to stop and restart the database UI server. Follow these steps to stop a UI Server.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. In the far left column, click the **Please select a server manager** button next to the Manager whose UI Server you want to stop.

5. Click **Select Server Manager**. The UI Servers window appears and lists the UI servers belonging to the Manager you selected.

6. Click the **Select** button next to the UI Server you want to stop.

7. Click **Stop selected UI Server**. The UI Server stops.

8. You can now start the UI Server you have stopped, or close this page by clicking **Close configuration page**.

Back to Top

Start a UI Server

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > GUI Servers > [Select Manager] > [Select UI Server] > Start selected UI Server

Sometimes you may need to stop and restart a UI server. For example, if the database is brought down and restarted, you will need to stop and restart the database UI server. After you have stopped a UI server, follow these steps to restart a UI Server.

1. From the DNCS Administrative Console, click the **DNCS** tab. The DNCS tab moves to the forefront.
2. Click the **Utilities** tab. The Utilities tab moves to the forefront.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

4. In the far left column, click the **Please select a server manager** button next to the Manager whose UI Server you want to start.

5. Click **Select Server Manager**. The UI Servers window appears and lists the UI Servers belonging to the Manager you selected.

6. Click the **Select** button next to the UI Server you want to start.

7. Click **Start selected UI Server**. The UI Server starts.

8. To close this page, click **Close configuration page**.

Back to Top

Maintaining Your Network
Maintenance Schedule

If you have ever owned a car, you know that there are certain tasks you must perform to keep a car performing at its best. The same is true for your DBDS. To provide continuous, quality service to your subscribers, you must keep your system in top condition by performing certain tasks on a regular basis. You must perform some tasks twice a day, while others must be performed only once a month or even less often. Click on the following links as appropriate to see when you should perform certain tasks.

Note: Some of these maintenance tasks require you to pre-configure your system to collect certain data. This requirement is noted with each applicable task. Also, the information presented here is not exhaustive. For a more complete description of maintenance tasks, refer to the *Maintenance Recommendations for the DBDS System Guide*. To obtain a copy of this guide, see **Printed Resources**. If you have questions about any of these tasks, contact technical support.

In addition, regularly check that the EAS is functioning properly. Refer to FCC guidelines or, if applicable, guidelines set by your local municipality to determine how often you should check the EAS functionality.

Important: We recommend that you run the Doctor Report every morning and every evening. However, you should always run the Doctor Report anytime you suspect or experience problems. For further information about the Doctor Report, refer to the *DBDS Utilities Installation Instructions and User Guide.* To obtain a copy of this guide, see **Printed Resources**.

Back to top

Maintenance: Twice a Day

Monitor the items in the following table twice a day. This table contains columns with the following information for each item:

- **Objective** — what you want to see to verify normal operation
- **Doctor** — whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the **Notes** column for additional information. For example, another logging capability may need to be turned on for the Doctor Report to show the item being monitored.
- **Notes** — additional information you may need when you monitor a particular item

Back to top

Item	Objective	Doctor	Notes
DNCS Processes	All running	Yes	saManager does not usually run on systems with Pioneer Application Servers.
Application Server Processes	All running	Yes	Does not apply to systems with Pioneer Application Servers.
System Time Messages (STMs)	Delivered within the last 12 seconds	Yes	Need to enable siManager logging Can also verify with a DHCT. The DHCT time comes from the STMs. Reboot a DHCT. If you see the correct time on its display, then STMs are being delivered.
PPV Files	Updated within the last 60 minutes	Yes	Does not apply to systems with Pioneer Application Servers.
Entitlement Unit Table (EUT)	Updated within the last 60 minutes	Yes	If the information in the EUT is wrong, subscribers may not be able to tune to channels they are authorized to receive.
GBAMs	TOD and purchase GBAMs delivered within the last 60 seconds	Yes	Need to enable camPsm logging
BFS Status	• All carousels up • Sessions active • One process per carousel • BFSDir updated within the last 60 minutes	Yes	Make sure the out-of-band data rate is under the maximum.

Alarms	No alarms present	No	
ECM Delivery Errors	No errors present	No	Need to enable camPsm logging
QAM RPC Errors	No errors present	Yes	Need to enable qamManager logging
1 Minute BIG Ping	• Average round-trip less than 10 microseconds • 0% packet loss	No	
1 Minute SARA Server Ping from DNCS	• Average round-trip less than 10 microseconds • 0% packet loss	No	Does not apply to systems that do not have a SARA Server
1 Minute DNCS Ping from SARA Server	• Average round-trip less than 10 microseconds • 0% packet loss	No	Does not apply to SARA Server
1 Minute DHCT Ping	• Average round-trip less than 10 microseconds • 0% packet loss	No	
1 Minute QAM Ping	• Average round-trip less than 10 microseconds • 0% packet loss	No	
PPV Events	Can purchase, view, and cancel events	No	
Boot DHCT	Enter advanced services within 2 minutes	No	

Back to top

Maintenance: Once a Day

Monitor the items in the following table once a day. This table contains columns with the following information for each item:

- **Objective** — what you want to see to verify normal operation
- **Doctor** — whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the **Notes** column for additional

information. For example, another logging capability may need to be turned on for the Doctor Report to show the item being monitored.

- **Notes** — additional information you may need when you monitor a particular item

Back to top

Item	Objective	Doctor	Notes
DNCS Corefiles	No core files	Yes	Capture all corefiles and deliver to SciCare Services, especially if they occur near the time of another problem.
SARA Server Corefiles	No core files	Yes	Capture all corefiles and deliver to SciCare Services.
DNCS Disk Utilization	Each volume using less than 80%	Yes	
SARA Server Utilization	Each volume using less than 80%	Yes	
DNCS Swap Space	More than 200 megabytes	Yes	
SARA Server Swap Space	More than 200 megabytes	Yes	
DHCT Software Associations	Make sure each DHCT type is set to either CVT or OSM, not both	No	Doctor reports the OSM associations. You can use the Image List GUI to view CVT associations.
Time Sync	• DNCS synchronized with an external source • SARA Server synchronized with the DNCS	Yes	You could also synchronize the SARA Server with an external source, and then synchronize the DNCS with the SARA Server.
EPG	Seven days' worth of grid information available, along with long descriptions	Yes*	Doctor Report shows EPG file sizes only. An operator must manually check the EPG information through a DHCT.
Clear Services	All services okay	No	
Subscription Services	All services okay	No	

Purchase Report	Information collected okay	No	
Database Backup	Backup performed successfully	No	Use dncsDbBackup tape. **Note:** For details, see *Backing Up and Restoring the Database Technical Bulletin*, P/N 740236.
ICMP Redirects	Low number of redirects	No	• Can be done at various points in the network. • Requires a sniffer or diagnostics on the switches or routers. • Ping can help if you use the **-v** option with the **ping** command.
Subnet Routes	All routes configured properly	No	
QAM Resets	No resets	No	You can obtain this information from bootpd log.
QPSK Resets	No resets	No	You can obtain this information bootpd log.
DHCT Resets	Monitor number	No	• Need to enable cmd2000 or hctmMac tracing. • Run signonCount for DHCT activity - this does not directly give reboots, but it allows you to see the consequences of any that have occurred.
Authorization Delays	Acceptable	No	Need CFET tools.
Queue Depths	Acceptable	No	Need CFET tools.
Number of PPV Events	Appropriate Number	Yes*	Doctor Report shows the number, but the operator must determine if the number is appropriate for the system.
DNCS Load Average	Less than 2.0 per CPU (compare to previous day's check)	Yes*	• Doctor Report shows the previous day's average. • Can also run the Top utility to gather this information.

Database Report — Poll Non-Responders	Monitor percentage	Yes*	Doctor Report shows the database numbers.

Back to top

Maintenance: Once a Week

Monitor the items in the following table once a week. This table contains columns with the following information for each item:

- **Objective** — what you want to see to verify normal operation
- **Doctor** — whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the **Notes** column for additional information. For example, another logging capability may need to be turned on for the Doctor Report to show the item being monitored.
- **Notes** — additional information you may need when you monitor a particular item

Back to top

Item	Objective	Doctor	Notes
DNCS Load Average	Less than 2.0 per CPU (compare to previous week's check)	Yes*	• Doctor Report shows the previous day's average. • Can also run the Top utility to gather this information.
SNMP Poll — Poll Non-Responders	Monitor percentage	Yes*	Doctor Report shows the database numbers.
Dataspace	Less than 75 percent used	Yes	Use Informix utilities and the Doctor Report.
Tempspace	Less than 75 percent used	Yes	• Warning = 75% to 84% used • Error = 85% or greater used • These values will vary depending on how much memory you have allocated for Tempspace.
Database Table Extents	Less than 10 extents per table	Yes	Defrag database by using dncsDbData

			(dbexport/dbimport) to move excess extents to disk.
Number of DHCTs	Monitor for growth	Yes	
Number of Source Definitions	Monitor for growth	Yes	
Number of QAM Modulators	Monitor for growth	Yes	
Number of QPSK Modulators and Demodulators	Monitor for growth	Yes	
BFS Carousel Rates	• Less than 300 kilobits per second out-of-band • Less than 11 Megabits per second (Mbps) for System Release (SR) 1.2.x or earlier • Less than 27 Mbps for SR 1.4 or later	Yes	
Number of DHCT Types	• As few as possible • No "0 DHCT" types	Yes	
SI_INSERT_RATE	Above calculated value	Yes	
DCM Verification	Verify that all DCMs are set up properly	No	

Back to top

Maintenance: Every Two Weeks

Perform the maintenance tasks in the following table every two weeks. This table contains columns with the following information for each task:

- **Objective** — what you want to accomplish by performing the task
- **Notes** — additional information you may need to perform the task

Back to top

Item	Objective	Notes
Run the EMM Deleter	Delete all unneeded staging EMMs	You determine which EMMs to delete based on the age of the EMMs.

Back to top

Maintenance: Every Month, Every Three Months, or After Every System Upgrade

Create a complete image of your system once a month, once every three months, or after every system upgrade.

Back to top

Maintenance: After Every EMM CD Installation

After every EMM CD installation, run the Doctor Report to determine how many DHCT types are installed in your system. You should have as few DHCT types as possible and absolutely no "0 DHCT" types.

Back to top

Maintenance: After Every Session Change and Every Source Definition Change

After every session change and after every source definition change, run the Doctor Report to check the value of SI_INSERT_RATE. This value should be above the calculated value.

Back to top

Maintenance: Spring and Fall Time Changes

After every Spring and Fall time change, run the Doctor Report to make sure that all hubs and DHCTs have the correct settings.

Back to top

Maintenance Schedule

If you have ever owned a car, you know that there are certain tasks you must perform to keep a car performing at its best. The same is true for your DBDS. To provide continuous, quality service to your subscribers, you must keep your system in top condition by performing certain tasks on a regular basis. You must perform some tasks twice a day, while others must be performed only once a month or even less often. Click on the following links as appropriate to see when you should perform certain tasks.

Note: Some of these maintenance tasks require you to pre-configure your system to collect certain data. This requirement is noted with each applicable task. Also, the information presented here is not exhaustive. For a more complete description of maintenance tasks, refer to the *Maintenance Recommendations for the DBDS System Guide*. To obtain a copy of this

guide, see **Printed Resources**. If you have questions about any of these tasks, contact technical support.

In addition, regularly check that the EAS is functioning properly. Refer to FCC guidelines or, if applicable, guidelines set by your local municipality to determine how often you should check the EAS functionality.

Important: We recommend that you run the Doctor Report every morning and every evening. However, you should always run the Doctor Report anytime you suspect or experience problems. For further information about the Doctor Report, refer to the *DBDS Utilities Installation Instructions and User Guide.* To obtain a copy of this guide, see **Printed Resources**.

Back to top

Maintenance: Twice a Day

Monitor the items in the following table twice a day. This table contains columns with the following information for each item:

- **Objective** — what you want to see to verify normal operation
- **Doctor** — whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the **Notes** column for additional information. For example, another logging capability may need to be turned on for the Doctor Report to show the item being monitored.
- **Notes** — additional information you may need when you monitor a particular item

Back to top

Item	Objective	Doctor	Notes

DNCS Processes	All running	Yes	saManager does not usually run on systems with Pioneer Application Servers.
Application Server Processes	All running	Yes	Does not apply to systems with Pioneer Application Servers.
System Time Messages (STMs)	Delivered within the last 12 seconds	Yes	Need to enable siManager logging Can also verify with a DHCT. The DHCT time comes from the STMs. Reboot a DHCT. If you see the correct time on its display, then STMs are being delivered.
PPV Files	Updated within the last 60 minutes	Yes	Does not apply to systems with Pioneer Application Servers.
Entitlement Unit Table (EUT)	Updated within the last 60 minutes	Yes	If the information in the EUT is wrong, subscribers may not be able to tune to channels they are authorized to receive.
GBAMs	TOD and purchase GBAMs delivered within the last 60 seconds	Yes	Need to enable camPsm logging
BFS Status	• All carousels up • Sessions active • One process per carousel • BFSDir updated within the last 60 minutes	Yes	Make sure the out-of-band data rate is under the maximum.
Alarms	No alarms present	No	
ECM Delivery Errors	No errors present	No	Need to enable camPsm logging
QAM RPC Errors	No errors present	Yes	Need to enable qamManager logging
1 Minute BIG Ping	• Average round-trip less than 10 microseconds • 0% packet loss	No	

1 Minute SARA Server Ping from DNCS	• Average round-trip less than 10 microseconds • 0% packet loss	No	Does not apply to systems that do not have a SARA Server
1 Minute DNCS Ping from SARA Server	• Average round-trip less than 10 microseconds • 0% packet loss	No	Does not apply to SARA Server
1 Minute DHCT Ping	• Average round-trip less than 10 microseconds • 0% packet loss	No	
1 Minute QAM Ping	• Average round-trip less than 10 microseconds • 0% packet loss	No	
PPV Events	Can purchase, view, and cancel events	No	
Boot DHCT	Enter advanced services within 2 minutes	No	

Back to top

Maintenance: Once a Day

Monitor the items in the following table once a day. This table contains columns with the following information for each item:

- **Objective** — what you want to see to verify normal operation
- **Doctor** — whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the **Notes** column for additional information. For example, another logging capability may need to be turned on for the Doctor Report to show the item being monitored.
- **Notes** — additional information you may need when you monitor a particular item

Back to top

Item	Objective	Doctor	Notes
DNCS Corefiles	No core files	Yes	Capture all corefiles and deliver to SciCare Services, especially if they occur near the time of another problem.

SARA Server Corefiles	No core files	Yes	Capture all corefiles and deliver to SciCare Services.
DNCS Disk Utilization	Each volume using less than 80%	Yes	
SARA Server Utilization	Each volume using less than 80%	Yes	
DNCS Swap Space	More than 200 megabytes	Yes	
SARA Server Swap Space	More than 200 megabytes	Yes	
DHCT Software Associations	Make sure each DHCT type is set to either CVT or OSM, not both	No	Doctor reports the OSM associations. You can use the Image List GUI to view CVT associations.
Time Sync	• DNCS synchronized with an external source • SARA Server synchronized with the DNCS	Yes	You could also synchronize the SARA Server with an external source, and then synchronize the DNCS with the SARA Server.
EPG	Seven days' worth of grid information available, along with long descriptions	Yes*	Doctor Report shows EPG file sizes only. An operator must manually check the EPG information through a DHCT.
Clear Services	All services okay	No	
Subscription Services	All services okay	No	
Purchase Report	Information collected okay	No	
Database Backup	Backup performed successfully	No	Use dncsDbBackup tape. **Note:** For details, see *Backing Up and Restoring the Database Technical Bulletin*, P/N 740236.
ICMP Redirects	Low number of redirects	No	• Can be done at various points in the network. • Requires a sniffer or diagnostics on the switches

			or routers. • Ping can help if you use the **-v** option with the **ping** command.
Subnet Routes	All routes configured properly	No	
QAM Resets	No resets	No	You can obtain this information from bootpd log.
QPSK Resets	No resets	No	You can obtain this information bootpd log.
DHCT Resets	Monitor number	No	• Need to enable cmd2000 or hctmMac tracing. • Run signonCount for DHCT activity - this does not directly give reboots, but it allows you to see the consequences of any that have occurred.
Authorization Delays	Acceptable	No	Need CFET tools.
Queue Depths	Acceptable	No	Need CFET tools.
Number of PPV Events	Appropriate Number	Yes*	Doctor Report shows the number, but the operator must determine if the number is appropriate for the system.
DNCS Load Average	Less than 2.0 per CPU (compare to previous day's check)	Yes*	• Doctor Report shows the previous day's average. • Can also run the Top utility to gather this information.
Database Report — Poll Non-Responders	Monitor percentage	Yes*	Doctor Report shows the database numbers.

Back to top

Maintenance: Once a Week

Monitor the items in the following table once a week. This table contains columns with the following information for each item:

- **Objective** — what you want to see to verify normal operation

- **Doctor** — whether or not you can run the Doctor Report to monitor the item. An asterisk (*) in this column indicates that you need to refer to the **Notes** column for additional information. For example, another logging capability may need to be turned on for the Doctor Report to show the item being monitored.
- **Notes** — additional information you may need when you monitor a particular item

Back to top

Item	Objective	Doctor	Notes
DNCS Load Average	Less than 2.0 per CPU (compare to previous week's check)	Yes*	• Doctor Report shows the previous day's average. • Can also run the Top utility to gather this information.
SNMP Poll — Poll Non-Responders	Monitor percentage	Yes*	Doctor Report shows the database numbers.
Dataspace	Less than 75 percent used	Yes	Use Informix utilities and the Doctor Report.
Tempspace	Less than 75 percent used	Yes	• Warning = 75% to 84% used • Error = 85% or greater used • These values will vary depending on how much memory you have allocated for Tempspace.
Database Table Extents	Less than 10 extents per table	Yes	Defrag database by using dncsDbData (dbexport/dbimport) to move excess extents to disk.
Number of DHCTs	Monitor for growth	Yes	
Number of Source Definitions	Monitor for growth	Yes	
Number of QAM Modulators	Monitor for growth	Yes	
Number of QPSK Modulators and	Monitor for growth	Yes	

Demodulators			
BFS Carousel Rates	• Less than 300 kilobits per second out-of-band • Less than 11 Megabits per second (Mbps) for System Release (SR) 1.2.x or earlier • Less than 27 Mbps for SR 1.4 or later	Yes	
Number of DHCT Types	• As few as possible • No "0 DHCT" types	Yes	
SI_INSERT_RATE	Above calculated value	Yes	
DCM Verification	Verify that all DCMs are set up properly	No	

Back to top

Maintenance: Every Two Weeks

Perform the maintenance tasks in the following table every two weeks. This table contains columns with the following information for each task:

- **Objective** — what you want to accomplish by performing the task
- **Notes** — additional information you may need to perform the task

Back to top

Item	Objective	Notes
Run the EMM Deleter	Delete all unneeded staging EMMs	You determine which EMMs to delete based on the age of the EMMs.

Back to top

Maintenance: Every Month, Every Three Months, or After Every System Upgrade

Create a complete image of your system once a month, once every three months, or after every system upgrade.

Back to top

Maintenance: After Every EMM CD Installation

After every EMM CD installation, run the Doctor Report to determine how many DHCT types are installed in your system. You should have as few DHCT types as possible and absolutely no "0 DHCT" types.

Back to top

Maintenance: After Every Session Change and Every Source Definition Change

After every session change and after every source definition change, run the Doctor Report to check the value of SI_INSERT_RATE. This value should be above the calculated value.

Back to top

Maintenance: Spring and Fall Time Changes

After every Spring and Fall time change, run the Doctor Report to make sure that all hubs and DHCTs have the correct settings.

Back to top

Scheduling Service Updates

Quick Path:
DNCS Administrative Console > Application Interface Modules tab > SAM Config

In addition to various other functions, the SAM also communicates service operation attributes to the DHCTs in the network on a regular basis. The frequency of this communication is determined by the SAM Update Timer. The default is 1200 seconds (20 minutes).

You can adjust how many seconds the DNCS waits after you make changes to the SAM or to a channel map before the DNCS generates new SAM files to be broadcast to DHCTs. Adjusting this schedule is useful in various situations.

For example, if you perform frequent single service channel updates, then a short timer (60 seconds) is useful. On the other hand, if you are making many updates that take a long time to enter, a longer timer (5 minutes) is useful.

Before You Begin

Before you change the SAM Update Timer setting, consult with your system administrator. Also, keep in mind that the delay time between updates should be at least 30 seconds to allow the system enough time to fully process each update.

Back to the top

Time To Complete

Changing the SAM Update Timer setting takes approximately 10 minutes to complete.

Back to the top

Performance Impact

Changing the SAM Update Timer setting does not impact network performance. You can complete this procedure at any time.

Back to the top

Procedure

Complete these steps to schedule the service updates through the SAM Update Timer setting.

1. On the DNCS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Config**. The SAM Configuration window opens.
3. Click in the **Update Timer** field and enter how many seconds the DNCS should wait after you make changes to the SAM before generating new SAM files to broadcast to the DHCTs in your network. This value should be at least **30** seconds.
4. Click in the **Schedule Timer** field and enter a value that is at least two times the Update Timer value. The Schedule Timer is a fail-safe mechanism to ensure DHCTs get updated on a regular basis. The Schedule Timer checks the SAM database to see if there have been any changes since the last update. If so, the system generates new SAM files and broadcasts them.
5. Click **Save**. The system saves these settings in the DNCS database and reconfigures the SAM to send broadcast service updates accordingly.
6. Click **Done** to close the SAM Configuration window and return to the DNCS Administrative Console.

Back to top

Troubleshooting Your Network
Troubleshoot a DBDS

Important: We recommend that you run the Doctor Report every morning and every evening. However, you should always run the Doctor Report anytime you suspect or experience problems. For further information about the Doctor Report, refer to *DBDS Utilities Installation Instructions and User Guide*. To obtain a copy of this publication, see **Printed Resources**.

Click on the symptom that best describes the trouble you are having.

- DNCS process is not running.
- Programs are experiencing interference (for example snow or static.)

Back to top

DNCS Process Not Running

After the DNCS is up and running, all of the DNCS processes should have a green working state on the DNCS Control window. However, if a process remains in a **red** or **yellow** working state, this indicates that the process is not functioning properly. If this occurs, perform the following corrective steps.

Important: If you are unsure of how to perform any of these steps, contact technical support.

1. Save the log files in the **/dvs/dncs/tmp** directory. The log files associated with the process have the format of <process name>.xxx, where xxx is a three-digit number.
2. Save the dncsLog files in the **/var/log** directory. The log files have the format dncsLog.x, where x is a single-digit number.
3. Save any corefiles in the **/dvs/dncs/tmp/corefiles/<processName>** directory. Corefiles will have the format core.xxxxx, where xxxxx is a five-digit number.
4. Is the current working state of the process in question **red** or **yellow**?
    - If it is **red**, go to step 5.
    - If it is **yellow**, stop here and contact technical support.
6. Try to restart the process as follows:
    - In the DNCS Control window, click once on the process name.
    - Click **Process > Start Process**.
7. Did the process change to a **green** working state?
    - If **yes**, the process is now running. No further action is necessary.
    - If **no**, contact technical support.

Program Interference

If DHCTs are experiencing program interference (for example, snow or static), try changing the appropriate QAM frequencies by 250 kHz from their current settings.

Back to top

Online Help Graphics Do Not Print

If you try to print a Help page and the graphics do not print, you probably did not wait long enough for the page to load completely before printing. Reload the Help page and make sure all of the graphics have loaded before attempting to print the page.

Logging

Logging Utility

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Logging

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.*].

Back to Top

What Would You Like to Do?

- Learn about logging levels.
- Adjust the logging level of a process.
- Adjust the logging level of libraries.

Back to Top

Logging Levels

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Logging

By selecting a level of logging for a specific site, you can control the type of information that the DNCS will record about processes running at a site. The default level is the Error level, but you can choose any of the following levels of logging for any process shown as well for any of its libraries.

- **Emergency** - At this level, the DNCS records issues that require immediate attention and may result in a major malfunction of DNCS applications.
- **Alert** - At this level, the DNCS records information about problems with the operating system, such as the system is out of memory or a disk partition is full.
- **Critical** - At this level, the DNCS records information about DNCS problems, such as a process core or a database failure.
- **Error Conditions (the default logging level)** - At this level, the DNCS records operational problems, such as hardware is offline or a code error.
- **Warning** - At this level, the DNCS records information about potential problems that operators should know about.
- **Notice** - At this level, the DNCS records information about normal, but significant events.
- **Information** - At this level, the DNCS records informational messages.
- **Debug** - At this level, the DNCS records information that may help in debugging a problem.

Back to Top

Adjust the Logging Level of a Process

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select Levels] > Save

Follow these 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 **Logging Levels** box 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.*].

Back to Top

Adjust the Logging Level of Libraries

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Logging > [Select Process] > Display Libraries

Follow these 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 **Select** 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 **Logging Levels** box 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.*]**.

Back to Top

Tracing

Tracing Overview

Quick Path:
DNCS Administrative Console > DNCS tab > Utilities tab > Tracing

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.

What Would You Like To Do?

Enable Tracing on the DNCS.

Learn About Tracing on the Application Server.

Enable Tracing on the Application Server.

Disable Tracing on the Application Server.

View the Log Files on the Application Server.

Enabling 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.

About Tracing on the Application Server

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. SciCare 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.

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.

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 Enable Tracing on the Application Server 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

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.

Viewing the Log Files on the Application Server

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 mqam.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.

Restarting the DNCS
Restarting the DNCS

We recommend that you restart the DNCS every two weeks as a normal maintenance process to free up system memory, swap space, and so forth. There may also be other situations, such as for troubleshooting, in which you may want to restart the DNCS. For more information on maintaining your DBDS, refer to the

Important: You must restart the DNCS in the proper order. Otherwise, some processes may not function properly.

Note: If you are upgrading the DNCS, do not use these procedures to restart the DNCS after the upgrade. Instead, use the procedures provided in the upgrade installation instructions that came with the upgrade software.

Before You Begin
You must have the **dncs** user password to complete some of the tasks necessary to restart the DNCS. If you do not know the password, contact your system administrator.

Time to Complete
Restarting the DNCS properly can take from 10 minutes to several hours, depending on the size of your system, how many sessions are active, and so forth.

Performance Impact
Performing some of the tasks necessary to restart the DNCS can affect service to your subscribers. To minimize this impact, we strongly recommend that you restart the DNCS during a maintenance window.

Process Overview
Properly restarting the DNCS involves completing the following tasks in order:

1. Stop all SARA Server processes.
2. Stop all DNCS processes.
3. Restart all DNCS processes.
4. Restart all SARA Server processes.

Back to top

Stop Critical Processes

Stopping SARA Server Processes
Complete these steps to stop all of the processes on the SARA Server. If you are using an application server from another vendor, stop your application server according to the vendor's instructions.

1. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.
2. Click the left mouse button and select **xterm**. An xterm window opens.
3. At the prompt, type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
4. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all SARA Server processes, along with their current working states ("running" or "stopped").
5. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.
6. Click the left mouse button and select **App Serv Stop**. The SARA Server begins shutting down all of its processes. This takes approximately 2 minutes to complete.
7. Press **Enter** to update the working states of the SARA Server processes. Continue to press **Enter** every few seconds until all processes show **Curr Stt: stopped(1)**.

   Important: Do not go to the next step until all processes are stopped.

8. Are you restarting the DNCS?
   - If **yes**, your next step is to stop all of the processes on the DNCS.
   - If **no**, you are finished with this procedure.

Back to top

Stopping DNCS Processes

Complete these steps to stop all of the processes on the DNCS.

CAUTION: When DNCS processes are stopped, two-way communication also stops in the DBDS. You will not be able to offer any PPV services during this time. In addition, you will be able to offer only limited EPG functionality, and you will not be able to stage DHCTs.

Important: If you are restarting the DNCS, complete this procedure only after you stop the network management system and the SARA Server processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click the **Control** button in the DNCS area.

   Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

   The DNCS Control (or Monitor) window opens with a list of all the DNCS processes and their working states. A *green* working state indicates that a process is running.

2. Use the mouse to place the cursor on any open area on the DNCS desktop, but not on the DNCS Administrative Console, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **DNCS Stop**. The DNCS begins shutting down all of its processes. This process can take from 5 minutes to an hour to complete depending on the size of your system, how many sessions are active, and so forth. When finished, all of the processes listed on the DNCS Control window should have a *red* working state, which indicates that they are not running. In addition, the DNCS area of the DNCS Administrative Console Status window will change to "Inactive."

4. Open an xterm window on the DNCS.

5. At the prompt, type **dncsControl** and press **Enter**. The Dncs Control main menu opens in another xterm window.

6. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all DNCS processes, along with their current working states ("running" or "stopped").

7. Press **Enter** to update the working states of the DNCS processes. Continue to press **Enter** every few seconds until all processes show **Curr Stt: stopped(1)**.

Important: Do not go to the next step until all processes are stopped.

8. Type **x** and press **Enter** to return to the Dncs Control main menu.

9. Type **x** and press **Enter** again to close both the Dncs Control main menu and the second xterm window.

10. Are you in the process of restarting the DNCS?
    - If **yes**, your next step is to restart all DNCS processes.
    - If **no**, you are finished with this procedure.

Back to top

Restart Critical Processes

Restarting DNCS Processes

After you stop all of the processes on the DNCS, complete these steps to restart them.

Important: You must restart the DNCS and its processes in the correct order. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. On the DNCS Administrative Console Status window, click the **Control** button in the DNCS area. The DNCS Control window opens with a list of all the DNCS processes and their working states. A *red* state indicates that a process is not running.

Note: Depending on the system release you have, this may be a **Monitor** button, instead of a Control button.

2. Use the mouse to place the cursor on any open area on the DNCS desktop, but not on the DNCS Administrative Console, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **DNCS Start**. On the DNCS Control window, all of the processes change to a *green* state, which indicates that they are running.

Note: It may take several minutes before all processes show a green state. Do not go to the next step until all of the processes are in a green state.

4. Your next step is to restart all of the processes on the SARA Server.

Back to top

Restarting SARA Server Processes

Complete these steps to restart all of the processes on the SARA Server. If you are using an application server from another vendor, restart your application server according to the vendor's instructions.

Important: If you are in the process of restarting the DNCS, complete this procedure only after you restart all the DNCS processes. Restarting the DNCS in the incorrect order could cause some processes to function incorrectly.

1. Is the xterm window open on the SARA Server that shows the working states of all SARA Server processes?
   - If **yes**, go to step 6.
   - If **no**, go to step 2.

2. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.

3. Click the left mouse button and select **xterm**. An xterm window opens.

4. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.

5. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. A list appears of all the SARA Server processes and shows their current working states.

6. Do all processes show **Curr Stt: running(2)**?
   - If **yes**, go to step 12.
   - If **no**, go to step 7.

7. Use the mouse to place the cursor on any open area on the SARA Server desktop, and then click the middle mouse button. A list of options appears.

8. Click the left mouse button and select **App Serv Start**. The SARA Server begins to restart all of its processes. This takes approximately 2 minutes to complete.

9. Press **Enter** every few seconds to update the working states until all processes show **Curr Stt: running(2)**.

10. Type **x** and press **Enter** to return to the Applications Control main menu.

11. Type **x** and press **Enter** again to close both the Applications Control main menu and the second xterm window.

12. In the first xterm window, type **exit** and press **Enter** to close the first xterm window.

Back to top

Glossary

A

Access Network: An HFC network in a DBDS consisting of two elements: (1) fiber optic transmission systems that extend from a hub to the HFC nodes, and (2) a coaxial bus network extending from the HFC nodes to the DHCTs at the end of the Access Network. The HFC network sends analog signals. QAM modulators allow digital signals to be carried on this analog medium.

AM Fiber: Amplitude Modulation fiber; a medium most often used by digital delivery systems to transport audio, video, and data from the headend to the hub. AM fiber has a maximum range of approximately 100 kilometers (62 miles).

App Server: See Application Server.

Application Server: Frequently referred to as the App 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: Virtual Channel Server (VCS), Interactive Program Guide (IPG), DHCT Configuration, Pay-Per-View (PPV) Event and Service setup, and Emergency Alert System (EAS) messaging. The Application Server uses multi-mode fiber to transfer data through the ATM switch to the DNCS or router. Data is sent in ATM cells over permanent virtual circuits (PVCs).

ASI: Asynchronous Serial Interface; allows the intermittent transfer of data one bit at a time rather than in a steady stream.

B

BFS: Broadcast File System (also known as the DNCS carousel); the primary means of communication between Application Servers and DHCTs; supports the data carousel and helps to establish the server-client relationship between the DNCS and the DHCTs. The BFS software can reside on the DNCS or on another host machine. The BFS uses data carousels to send the files to a DHCT that tell the DHCT how to run a specific application properly. For example,

the BFS provides a DHCT with information the DHCT needs to process a typical broadcast.

BFS Data: Consists of files, such as PPV information, operating system/resident application images, and application data files that must be sent from the DNCS to the DHCTs on a system.

Bootp: Bootstrap protocol; process by which a network element (for example, a QAM modulator determines the IP address of its Ethernet interface.

Broadcast File System: See BFS.

C

CA: See Conditional Access.

CableLabs: The more commonly used name for Cable Television Laboratories, Inc., publisher of the OCI-N Cable Network Interface Specification. Founded in 1988, CableLabs is a research and development consortium of cable television system operators representing North America and South America. CableLabs plans and funds research and development projects that will help cable companies take advantage of future opportunities and meet future challenges in the cable television industry. In addition, CableLabs acts as a clearinghouse to provide information on current and prospective technological developments that are of interest to the cable industry.

Carousel: A logical element that carries information from a BFS server to DHCTs that request the information. The carousel makes the information available to all DHCTs in the system. However, only those DHCTs specifically authorized and looking for the information will receive it. Carousels are sometimes referred to as sources or data pumps.

CCI Bits: Copy Control Information bits; used to define which content should be secured over the back-channel interface between the CableCARD module and the host device.

CF Session: See Continuous Feed Session.

CGMS/A: Copy Generation Management System/Analog (CGMS/A) protects analog outputs from being recorded to devices such as

DVD recorders and digital VCRs. A DHCT may also receive CGMS/A in analog content, as embedded XDS data. A DHCT has the capability to output CGMS/A information on the composite and component analog outputs. The CGMS/A data is copied from the source content to the appropriate VBI line. When analog content is encoded and recorded, the CGMS/A settings are stored in a secure manner along with the content and restored on playback.

Clear Service: A service that is delivered to subscribers unscrambled or unencrypted; for example, programming available through the three major networks (ABC, CBS, and NBC) is usually clear. See also Non-Encrypted Service.

Conditional Access: The system, software, and components necessary to provide or deny subscribers selective access to specific services. See also PowerKEY Conditional Access System.

Continuous Feed Session: A logical element that defines and allocates resources that the network uses to deliver a particular service to subscribers. When you add (build) a CF session, you establish the source that is sending the service, such as an IRT, and the QAM or MQAM modulator that is used to transport the service onto the network. It may help to think of a CF session as a pipeline through the DBDS that is designated to deliver a service.

Copy Control Information: See CCI Bits.

Copy-Protected Content: Video and/or audio content that is coded to prevent it from being copied by recording devices, such as digital video recorders or personal computers.

D

Data Pump: See Carousel.

DAVIC: Digital Audio/Video Council; an international group of approximately 250 companies developing an "end-to-end" standard for interactive digital media, including interfaces and requirements for applications, systems, and networks. The group includes members of the original MPEG Joint Technical Committee (JTC).

DBDS: Digital Broadband Delivery System; network of hardware and software that works in conjunction with a traditional analog cable

system to deliver MPEG-2 encoded video, audio, analog services, and digital data to subscribers through their DHCTs. Although analog and digital systems use separate signal processing and separate monitoring and control equipment, they share the HFC network for delivering signals to DHCTs. The same 6 MHz bandwidth slot that is required for a single analog channel allows 8 or more digital programs to be broadcast when using a DBDS. A DBDS also offers a real-time reverse path from the DHCT to the DNCS, allowing subscribers to initiate actions directly over the cable network and use interactive services. The end result is that cable operators can greatly increase the number of services that they can offer to subscribers.

DCM: The major purposes of the Digital Content Manager (DCM) are re-multiplexing and grooming of content. The DCM supports extensive transport stream and program analysis to allow the operator to easily configure the program streams as well as troubleshoot any content transport problem. The device performs program-level bit rate measurements on both incoming and outgoing streams. The DCM is controlled using a simple and intuitive browser-accessible graphical user interface (GUI).

DFAST: Dynamic Feedback Arrangement Scrambling Technique (DFAST) a content-protection method that prevents devices from trying to obtain information (snooping) on the CableCARD/Host interface (PCMCIA bus). DFAST re-encrypts content by re-scrambling the bits of a program for hand-off to a Host device, such as a TV. The Host device decrypts the protected digital content for subscriber viewing.

DHCP: Dynamic Host Configuration Protocol; TCP/IP protocol that manages a pool of IP addresses.

DHCT: Digital Home Communications Terminal; a 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. DHCTs also modulate digital data over the HFC network to send data,

such as event purchases, to QPSK demodulators. The type of data carried on each data channel is as follows: (1) from the data FAT channel, the DHCT receives application files, modulation mode data,and satellite and transponder data; (2) from the FDC, the DHCT receives system messages, as well as tuning and management data; (3) 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.

DHEI: DigiCable Headend Expansion Interface; a proprietary interface cable that goes from an IRT to a QAM or MQAM modulator.

DigiCable Headend Expansion Interface: See DHEI.

Digital Audio/Video Council: See DAVIC.

Digital Broadband Delivery System: See DBDS.

Digital Content Manager: See DCM.

Digital Home Communications Terminal: See DHCT.

Digital Network Control System: See DNCS.

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 Scientific-Atlanta's Explorer® DHCTs with broadcast services that are displayed on subscribers' televisions throughout a cable network. The DNCS works with the ATM switch and 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.

DS-1: Digital Signal Level 1; represents a transmission rate of 1.54 Mbps; usually carries 24 voice circuits or other data services.

DS-3: Digital Signal Level 3; represents a transmission rate of 45 Mbps; equivalent to approximately 28 DS-1 circuits; one of the standard network transmission types that the BIG uses.

DTCP: Digital Transmission Content Protection (DTCP) protects content output on the 1394 port. Unless content is marked "Copy Freely," the stream is encrypted on this port.

DVB: A standard developed by the Digital Video Broadcasting (DVB) Group, a European organization that has authored many specifications for satellite and cable broadcasting of digital signals. Part of the DVB work has been focused specifically on conditional access.

DVI: Digital Visual Interface (DVI) is a secure connection between a television and an external DHCT that uses encryption to prevent privacy.

Dynamic Host Configuration Protocol: See DHCP.

E

EID: Entitlement Identifier; when you add a service package to your system, the DNCS automatically assigns an EID to that package. DHCTs use this information to determine whether or not they are authorized to receive a particular service or application.

Element: Term used to refer to DBDS devices, groups of devices, and software components that must be provisioned from the DNCS. See also Logical Element and Physical Element.

Emergency Alert System: EAS; the FCC established the EAS in 1994 as a tool for the President of the United States and others to warn the public about various emergency weather conditions and civil disturbances. In the interest of public safety, the FCC requires cable systems to receive these emergency alert messages (EAMs and distribute them to the public. In addition, the FCC requires cable operators to conduct weekly and monthly tests of the EAS. For more information, refer to the "Digital EAS Configuration and Troubleshooting Guide For Use With SR 2.1 and Later."

EMM: Entitlement Management Message; contains information for a specific DHCT that enables that DHCT to access secure services. For example, EMMs enable DHCTs to decrypt premium broadcasts that have been encrypted to keep subscribers who have not purchased the broadcasts from using them. In other words, EMMs are the key by which an authorized DHCT can access secure services. A DHCT must receive a minimum of 33 EMMs to display secure services. However, the number of EMMs that a DHCT contains depends on the number of services authorized for that

DHCT. Scientific-Atlanta ships a CD-ROM containing specific EMMs for each group of DHCTs that Scientific-Atlanta ships to you. It is critical that you make sure the DHCT shipping record matches the CD packing slip before you stage a group of DHCTs. If you try to stage DHCTs using the wrong EMMs, the DHCTs will not operate properly. EMMs should be installed on the DNCS immediately, even if you plan to stage the DHCTs later. See also TED.

Encrypted Service: A service that is encrypted, or scrambled, so that it is protected from being accessed (stolen) by people who have not paid for the service. Because encrypted services are considered to be "secure" from theft, you may also hear them referred to as secure services. You can use Scientific-Atlanta's PowerKEY Conditional Access system to encrypt non-interactive services. Encrypted services are usually offered to subscribers at a price that is in addition to the price they pay for non-encrypted services. Some examples of encrypted non-interactive services include HBO, ShowTime, and PPV. See also Non-A service that is encrypted, or scrambled, so that it is protected from being accessed (stolen) by people who have not paid for the service. Because encrypted services are considered to be "secure" from theft, you may also hear them referred to as secure services. You can use Scientific-Atlanta's PowerKEY Conditional Access system to encrypt non-interactive services. Encrypted services are usually offered to subscribers at a price that is in addition to the price they pay for non-encrypted services. Some examples of encrypted non-interactive services include HBO, ShowTime, and PPV. See also Non-Encrypted Service.

Entitlement Identifier: See EID.

Entitlement Management Message: See EMM.

Entitlement Unit Table: See EUT.

EUT: Entitlement Unit Table; lists all packages with their associated sources. DHCTs use this table as a reference when tuning to channels. If subscribers try to tune to a channel that is not in their authorized package, they will see a message informing them that they are not authorized for that channel.

F

FCC: Federal Communications Commission; federal organization set up by the Communications Act of 1934; has authority to regulate all interstate (but not intrastate) communications originating in the United States (radio, television, wire, satellite, and cable).

FDC: Forward Data Channel; carries digital data (tuning, management, Internet, and at least two days of IPG data) in ATM cells, at a rate of at least 1.54 Mbps, on RFsignals from the ATM switch to a router, which then forwards the data to the correct network; sometimes referred to as the out-of-band data channel. DHCTs are always tuned to one of these channels.

FEC: Forward Error Correction; system of data transmission in which redundant bits generated at the transmitter are used by the receiver to detect, locate, and correct transmission errors before delivering the data to the local data communications link; avoids requiring the transmitter to resend information.

Federal Communications Commission: See FCC.

File Transfer Protocol: See FTP.

FTP: File Transfer Protocol; allows users to transfer text and binary files to and from a personal computer, list directories on the foreign host, delete and rename files on the foreign host, and perform wildcard transfers between hosts.

G

GBAM: Global Broadcast Authenticated Message; mechanism that allows IPPV purchases to be secured. Two minutes before the Buy window opens, the DNCS broadcasts GBAMs to DHCTs until the Buy window closes. If the subscriber attempts to purchase an event during this time period or if the subscriber has purchased the event in advance, the DHCT searches for the GBAM associated with the event. If it finds the GBAM and if the subscriber has enough credits, the DHCT can purchase the event. Note that although an event may be ordered in advance, its purchase can be secured only during the time that GBAMs are sent, which is during the Buy window and two minutes before.

Global Broadcast Authenticated Message: See GBAM.

GQAM: Gigabit Quadrature Amplitude Modulation Modulator. A QAM modulator that provides up to sixteen 6 MHz outputs while occupying only one unit of rack space.

H

HDCP: High-bandwidth Digital Content Protection (HDCP) protects content on the DVI/HDMI port.

Headend: A logical element that represents a group of IRTs, QAM modulators, BIGs, and other network devices that provide services to a particular group of DHCTs.

HFC: Hybrid Fiber-Coaxial Network; a network that uses a combination of fiber optics and coaxial cable to transport signals from one place to another.

Hub: A logical element that represents the point at which out-of-band (QPSK-modulated) frequencies are combined with inband (QAM-modulated) frequencies for transmission to subscribers through the RF network. Each headend must have at least one hub.

Hybrid Fiber-Coaxial Network: See HFC Network.

I

Interactive Client: Part of an application that instructs a DHCT on how to download, install, and run that application. Depending on the application, there may be more than one interactive client file. The interactive client files are installed when the vendor installs (or helps you install) the application itself, and reside on the same server.

Internet Protocol: Standard that was originally developed by the United States Department of Defense to support the interworking of dissimilar computers across a network. IP is perhaps the most important of the protocols on which the Internet is based. It is the standard that describes software that keeps track of the internetwork addresses for different nodes, routes, and outgoing/incoming messages on a network. Some examples of IP applications include email, chat, and Web browsers.

IP: See Internet Protocol.

IP Address: A 32-bit sequence of numbers used for routing IP data. Each IP address identifies a specific component on a specific network. The address contains a network address identifier and a host identifier.

L

LCD: See Liquid Crystal Display.

Liquid Crystal Display: An alphanumeric display using liquid crystal sealed between two pieces of glass. The display is divided into hundreds or thousands of dots, which form characters, letters, and numbers.

Logical Element: Represents a group of elements; does not represent a specific device. For example, headends and node sets are logical elements.

M

MAC Address: Media Access Control Address; a unique 48-bit number that identifies the input/output card of a particular device. The MAC address is programmed into the card by the manufacturer.

Macrovision: A method of content protection that modifies the NTSC signal at analog composite outputs (but not analog component Y-Pr-Pb outputs). This capability enables cable system providers to inhibit subscribers from copying digital content through the analog outputs (RF, S-Video, or composite) of the DHCT.

Mbps: A unit of measure representing one million bits (megabits) per second.

Media Access Control Address: See MAC Address.

MHz: A unit of measure representing one million hertz (megahertz) or one million cycles per second; measures bandwidth.

Motion Picture Experts Group: See MPEG.

MPEG: Motion Picture Experts Group; a joint committee of the International Standards Organization (ISO) and the International Electrotechnical Commission (EG). This committee develops and

maintains the MPEG specification for a series of hardware and software standards designed to reduce the storage requirements of digital video and audio. The common goal of MPEG compression is to convert the equivalent of about 7.7 MB down to under 150 K, which represents a compression ratio of approximately 52 to 1.

MPEG Source: Equipment that takes incoming data, converts it into MPEG data, then sends it to a specific QAM or MQAM modulator for delivery to DHCTs over the forward inband data path.

MQAM Modulator: Multiple Quadrature Amplitude Modulation Modulator; device with two input ports that allow it to receive MPEG transport streams simultaneously from two different sources. The MQAM modulator separates the content in these transport streams, encrypts it, modulates it, and then sends it to DHCTs on the cable network. The four, independent radio frequency (RF) outputs on the back panel of an MQAM modulator allow the cable operator to use only one unit of rack space for the hardware and one unit of rack space for ventilation, while providing the same number of RF output channels as four QAM modulators. For more information about MQAM modulators, refer to the Model D9477-1 and Model D9477-2 MQAM Installation and Operation Guide.

Multiple Quadrature Amplitude Modulation Modulator: See MQAM Modulator.

Multiplex: Process of combining all audio, video, still picture, and other data streams into one encoded master file.

Mux: Abbreviation for multiplex.

N

Naming Service Process: Provides a means for different servers and processes to communicate with each other in the DBDS. Each time you restart the DNCS or the orbixd process, Orbix creates a naming service process. If there is more than one naming service process in the system, the EAS will not function properly.

Nesting: The practice of placing service packages within other service packages.

Network Management System: See NMS.

NMS: Network Management System; a software system designed specifically to monitor a network and to facilitate troubleshooting.

Non-Encrypted Service: A service sometimes referred to as a clear service because it is delivered to subscribers "in the clear," meaning unscrambled or unencrypted. For example, programming available through the three major networks (ABC, CBS, and NBC) is usually non-encrypted. Because these services are not encrypted, they are more susceptible to being accessed (stolen) by people who have not paid for the service. Therefore, you may also hear non-encrypted services referred to as non-secure services. See also Encrypted Service.

Non-Interactive Service: A service that consumers most likely think of when they use their televisions to watch programs or listen to music. Non-interactive services can be secured (encrypted) so that they can be offered only to authorized subscribers. They can also be made available for a short duration of time rather than being provided continually. However, non-interactive services do not require a subscriber’s interaction once they begin. For subscribers, their experience is basically the same as it has been since television first became popular: they passively watch or listen to the content that is broadcast into their homes. You can set up two basic types of non-interactive services: non-encrypted and encrypted.

Non-Secure Service: See Non-Encrypted Service.

O

Organizational Unit Identifier: The first six numbers from the MAC address for a particular type of DHCT. For example, if the MAC address for a specific DHCT is 00:02:DE:11:22:33, the OUI for that type of DHCT is 00:02:DE. You can see the OUI for each DHCT type in the DNCS database by going to the DNCS DHCT Type List (DNCS Administrative Console > DNCS tab > Element Provisioning tab > Type).

Orphaned Session: A session without an associated QAM or MQAM modulator.

OS: Operating system.

OUI: See Organizational Unit Identifier.

P

PAT: A Program Allocation Table identifies all the programs in a transport stream and associates each program number with packet identifiers (PIDs) that carry information about the programs in the stream. When the DHCT tunes to a channel, it extracts the PAT and other information and uses this data to display the application for the subscriber.

Physical Element: A hardware device. For example, DHCTs and QAM modulators are physical elements within the DBDS.

PowerKEY Conditional Access System: Contained within the TED; the PowerKEY Conditional Access System provides security for the DBDS by using the following keys: Secret key; Public key; Private key. The Conditional Access software allows you to secure services so that only subscribers who are authorized can use those services. You could compare Conditional Access to the password protection feature on a PC. Scientific-Atlanta's PowerKEY Conditional Access Module is a point-of-deployment (POD) module that enables cable operators to fulfill the industry commitment to OpenCable. See also OpenCable.

PowerTV Operating System: DHCT application environment that allows application programs (for example, WatchTV) to operate. You can compare the PowerTV OS to the Windows, UNIX, or Mac OS, which must be loaded onto a PC for the PC to be able to run application programs such as word processing programs, Internet browsers, or spreadsheet programs.

PPV: Pay-Per-View.

Provisioning: The process of preparing a device or service so that the DNCS recognizes it and so that it operates properly.

PVR: Personal video recorder; see DVR.

Q

QAM Modulator: Quadrature Amplitude Modulation Modulator; a device that receives MPEG packets and modulates them onto a radio frequency (RF) carrier over the hybrid fiber-coaxial (HFC) network. The type of data that a QAM modulator receives is dependent upon what equipment is connected to it in the DBDS, as indicated in the following examples: (1) when it is connected to an IRT or to a Grooming BIG, the QAM modulator receives programming data; (2) when it is connected to a BFS BIG, the QAM modulator receives system and service data. QAM modulation converts a 6-MHz channel slot into a 27- or 36-Mbps data channel that allows eight or more digital programs to be broadcast. Because the QAM modulator always performs the same function — receiving MPEG packets and modulating them onto an RF carrier — the procedure for setting up a QAM modulator is the same, regardless of the type of data the QAM modulator processes. See also Program QAM Modulator and BFS QAM Modulator.

Quadrature Amplitude Modulation Modulator: See QAM modulator.

R

Real-Time Encoder: See RTE.

Res App Software: See SARA.

Router: A device that directs data to different networks as follows: (1) one network involves devices that receive sources into the headend (for example, IRTs and MDRs); (2) another network involves program and service devices (for example, Grooming BIGs and program QAM modulators); (3) another network handles data management devices that are in the local hub (for example, QPSK modulators); and (4) another network handles data devices in the headend (for example, BFS BIGs and BFS QAM modulators)

S

SAM: Service Application Manager; a process that associates a specific service with an application that defines the medium to be used for that service, such as the Music or Watch TV applications. For example, the SAM associates the Watch TV application with a service called The Golf Channel.

SARA: Scientific-Atlanta Resident Application; software that allows a DHCT to run different applications to provide various services for the subscriber. For example, SARA runs the PPV application. You could compare SARA to a word processing program, an Internet browser, or a spreadsheet program. SARA is sometimes referred to as the DHCT software or the Res App software.

Scientific-Atlanta Resident Application: See SARA.

Secure Service: A service that is encrypted or scrambled so that it is protected from being accessed (stolen) by people who have not paid for the service; usually offered at a price that is in addition to the price for clear services (for example, HBO, ShowTime, music channels, and PPV). See also Encrypted Service.

Service Application Manager: See SAM.

Service Authorization: A process of authorizing a DHCT to receive specific services.

Sessions: Define and allocate the resources that the network uses to deliver source content. When you build a session, you establish the equipment where the source content originates, such as an IRT, and the specific distribution equipment that places the source content on the HFC network, such as a QAM modulator. It may help to think of a session as a pipeline through the DBDS that is allocated to deliver content from a particular source.

SI Data: System Information Data; tuning information sent from the DNCS to DHCTs; provides the information that DHCTs need to be able to tune to a particular service.

SI Source: System Information Source; tells DHCTs on your system where they can locate SI data.

Simple Network Management Protocol: See SNMP.

SNMP: Simple Network Management Protocol; protocol that governs network management and the monitoring of network devices and their functions.

STM: System Time Message; contains the current system time; delivered to DHCTs approximately every 12 seconds and appears on their displays.

System Information Data: See SI Data.

System Information Source: See SI Source.

System Time Message: See STM.

T

TED: Transaction Encryption Device; a computer that is connected directly to the DNCS workstation with a short Ethernet connection. The PowerKEY Conditional Access system uses either the TED server or the TED FX server. Both servers ensure that secure applications remain secure as they are transported through the DBDS. However, the TED FX server provides a faster transaction encryption rate and is able to encrypt more EMMs per second than the TED Server. When the DNCS receives a request to authorize a service to a specific DHCT, the DNCS generates EMMs. The DNCS then sends these EMMs to the TED/TED FX server to be encrypted. After the TED/TED FX server encrypts the EMMs, it sends the encrypted EMMs to the DNCS. The DNCS then sends the encrypted EMMs through the DBDS to the DHCT. See also EMM.

Transaction Encryption Device: See TED.

Transport Network: A network of transmission equipment that carries programming (audio, video, and data) in an MPEG format over QAM-modulated signals from the headend to the hub, passing the programs to the Access Network. Currently, most digital delivery systems use AM fiber to do this. However, more and more systems are beginning to use SONET.

U

Uniform Resource Locator: A standardized way of representing different documents, media, and network services on the World Wide Web. The URL is most commonly referred to as the Web address for a particular item. For example, the URL, or Web address, for Scientific Atlanta is http://www.scientificatlanta.com.

URL: See Uniform Resource Locator.

V

Value Added Service Provider: See VASP.

VASP: Value Added Service Provider; generic term for a server that is a part of the DBDS with data files that contain system information and configuration information. VASP data does not directly involve audio and video program services. Setting up a VASP enables the DNCS to recognize the server and establishes a path for them to communicate with each other.

VCS: Virtual Channel Service.

Video-on-Demand: See VOD.

VOD: Video-on-Demand; services that allow a subscriber to use the remote control to select, purchase, and view a movie; once purchased, the viewer can then forward, reverse, pause, and play the movie just as he or she would with a VCR.

X

xOD: Anything-on-Demand; a service that provides subscribers with unlimited, on-demand access to virtually any digital content; includes VOD and SVOD.

Index