ISDS Online Help

Version 2.7.0.0

Contents

Content Element Configuration 59

Broadcast File System (BFS) Host 65

CSM Services 71

SAM Services 81

Other ISDS Features 297

Stopping and Restarting the ISDS 327

Monitoring Your ISDP 339

Maintaining Your ISDP 377

Troubleshooting 531

1

Welcome to the ISDS Help

The ISDS Help provides the help information you need to use the ISDS. The Help contains the following:

- Overview information
- Conceptual information
- Reference information
- Instructions for completing tasks

Online help version 1.3.1.1 (UNIX) is delivered with ISDS version 2.7.

In This Chapter

About This Version of Help

For details about this version of ISDS Online help, see the following topics:

- Help version and copyright information for this help document
- Terms and conditions for use of this version of ISDS Online Help
- Trademarks used in this version of ISDS Online Help

Help Version and Copyright

ISDS Online Help Version 2.7.0.0
June 2010

4038462 Rev A

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

Terms and Conditions

Following are the terms and conditions to which you agree by using the ISDS 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.

Acknowledgments

I understand that the information and materials provided in this ISDS 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 ISDS and for no other purposes.

Disclaimer

Limitation of Liability

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 ISDS only. If you are not an authorized licensee of the Cisco ISDS, 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.

Trademarks

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

- Cisco, Cisco Systems, the Cisco logo, the Cisco Systems logo, AllTouch, Continuum DVP, Explorer, Overlay, PowerKEY, and PowerTV are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.
- CableLabs and DOCSIS are registered trademarks of Cable Television Laboratories, Inc.
- CableCARD, M-Card, OpenCable, OCAP, and tru2way are trademarks of Cable Television Laboratories, Inc.
- HDMI, the HDMI logo, and High-Definition Multimedia Interface are trademarks or registered trademarks of HDMI Licensing LLC.
- Macrovision is a registered trademark of Macrovision Corp.
- MoCA is a trademark of the Multimedia over Coax Alliance.
- *All other trademarks mentioned in this document are the property of their respective owners.*

Publication Disclaimer

ISDS Nomenclature

This document applies to one or more of our network-control platforms. These platforms include, but are not limited to, the Digital Network Control System (DNCS) and the IPTV Service Delivery System (ISDS). Throughout this document, you might see us refer to these platforms as DNCS/ISDS.

This online help system is applicable to the ISDS 2.7 system release.

You might see references to the DNCS in the underlying platform database structure.

We also refer to the 'cable box' as either a DHCT or as a set-top. These terms are interchangeable, and might appear in the same section.

Additional Support and Resources

The following additional resources are also available to help you:

- ***Technical support*** (see "***Contact Us***" on page 7) from our service engineers or customer service representatives
- ***Printed resources*** (on page 8) which can be ordered or viewed from the Internet

Contact Us

If You Have Questions

If you have questions about this product, contact the representative who handles your account for information.

If you have technical questions, telephone your nearest technical support office at one of the following telephone numbers.

The Americas

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 ■ For all products *other than* Digital Broadband Delivery System, call: – Toll-free: 1-800-722-2009 – Local: 678-277-1120 – Fax: 770-236-2306 **Customer Service** ■ Toll-free: 1-800-722-2009 ■ Local: 678-277-1120 ■ Fax: 770-236-5477

The United Kingdom and Europe		
Europe	European Technical Assistance Center (EuTAC), Belgium	**Product Information** ■ Telephone: 32-56-445-444 **Technical Support** ■ Telephone: 32-56-445-197 or 32-56-445-155 ■ Fax: 32-56-445-061

Asia-Pacific		
China	Hong Kong	**Technical Support** Telephone: 011-852-2588-4745 Fax: 011-852-2588-3139

Australia		
Australia	Sydney	**Technical Support** Telephone: 011-61-2-8446-5374 Fax: 011-61-2-8446-8015

Japan		
Japan	Tokyo	**Technical Support** Telephone: 011-81-3-5322-2067 Fax: 011-81-3-5322-1311

Additional Information

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

Printed Resources

You can find related publications at the following web address:

https://www.sciatl.com/subscriberextranet/techpubs
(***https://www.sciatl.com/subscriberextranet/techpubs/news.htm***)

Note: You need your company's user name and password to access this website. If you do not have this information, ***contact the representative who handles your account*** (see "***Contact Us***" on page 7). You also need Adobe Acrobat Reader installed on your system. The website mentioned previously provides a link for downloading the Adobe software.

Help for New Users

These topics can help you find information quickly and learn the basics about the ISDS and how it can help you manage your ISDP.

Navigation Tips

The following tip may help you to navigate more efficiently around the ISDS Help PDF.

Use any of the following methods to find information you need in the ISDS Help:

- Click the topic in the **Bookmarks** list at left.
- Click the **Index** tab at left and click on a keyword.
- Click **Edit > Search**, type in a keyword and press **Enter**.

Using the Search Feature

Follow these steps to use the Search feature.

1. Select **Edit > Find**. The Find field is highlighted.
2. Enter your search term and press **Enter.** The PDF will search and land on the page that contains the first instance of the term you entered.
   - To continue searching for other instances of the term, click the **Find Next** arrow.
   - To search for previous instances of the search term, click the **Find Previous** arrow.

Printing Help Topics

If your system has print capabilities, you can print any Help topic or the complete Help PDF by completing these steps.

1. Click once within the topic to activate that page in the PDF.
2. Select one of the print options in Print Range:
   - All
   - Current view
   - Current page
   - Pages (range)
   - Subset (of the range)

3 When you have selected all your print parameters, print **OK**. The pages you selected print.

Multiple Pages of Information

There may be times when the results of a filter query result in multiple pages of query results. If multiple pages display, you can use the paging controls at the top of the screen to view the pages.

- Use the **Rows per page** control to change the number of query results displayed on each page. Select the number of rows you want to view from the drop-down menu. The screen refreshes to show that number of query results on each page.
- Use the **Next Page** control to view the next page of query results.
- Use the **Previous Page** control to view the previous page of query results.
- Use the **Last Page** control to view the last page of query results.
- Use the **First Page** control to view the first page of query results.
- Use the **Page** control to go directly to a specific page of query query results.

  To use the Page control:

  - Enter the page number in the space provided and click Go to view that page.
- Use the **Search** control to search within the query results.

  To search within the query results:

  - Type the search term and click to view the search results. The system searches the fields within the query results.
  - To clear the search results, clear the search term and click .

2

ISDS Host Configuration

Introduction

When you set up the ISDS host, you establish connections between the ISDS host and other devices that are critical to the system.

This section describes how to set up the ISDS host.

In This Chapter

ISDS Host Settings

Use the following fields when you manage the ISDS host.

Field	Description
Controller Host Name or IP	Name or IP address of the ISDS host. Enter **dncsatm** as the host for the ISDS server.
STUN Server Host Name or IP	Name given to the Simple Traversal of UDP over NATs (STUN) host. A STUN server allows a set-top that resides behind a Network Address Translation (NAT) device to discover its public address. ■ Enter **dncsatm** as the host for the STUN server.
NMS Server Host Name or IP	Name given to the network management system (NMS) host, if an NMS is used. ■ Enter **dncsatm** as the host for the NMS server.
DNS Primary IP Address	The IP address of the primary domain name service (DNS) server. The DNS server translates human-readable computer host names into the IP addresses that networking equipment needs to deliver information
DNS Secondary IP Address	The IP address of the secondary DNS server.
Site Multicast Flow IP Address	The IP address used by the site-wide multicast flow, which is the multicast IP address that all set-tops join when they first boot up. ■ Enter **224.0.23.42** as the IP address of the site-wide multicast flow.
STUN Keepalive	Specify the frequency that keepalive messages are sent to the STUN server. **Example:** If the default value of 20 is entered in this field, the STUN server sends a keepalive message to the ISDS server once every 20 seconds during periods of inactivity between the two servers. ■ You can enter a value of 20 to 3000 in this field. ■ The default value for this field is 20 seconds. A keep alive message maintains the integrity of the connection between the STUN server and the ISDS server during prolonged periods of inactivity in communication between the two.

CVT Interval	Determines how often the Code Version Table (CVT) is sent in the site-wide IP multicast flow. **Example:** If the default value of 10 is entered in this field, the CVT table will be sent in the site-wide IP multicast flow once every 10 seconds. ■ You can enter a value of 1 to 20 in this field. ■ The default value for this field is 10 seconds. The CVT contains information about download channels and code versions for set-tops grouped by manufacturer, hardware version, and so on. Once the set-top has left the site-wide multicast and has joined the cluster-specific multicast, the set-top listens for status messages that are sent periodically. The status messages contain the latest version of the CVT. If the version of the CVT has changed, then the set-top can re-join the site-wide multicast to get the latest, up-to-date CVT. Bootloader software, which runs in the set-top, determines if an update of the operating system is needed by periodically checking the CVT.
UN Passthru Interval	Defines how often (in seconds) the ISDS transmits UNPassThru messages. ■ The default setting is 10.

Setting Up the ISDS Server

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > Syst Config > ISDS tab

1. From the ISDS Administrative Console, click the **System Provisioning** tab.
2. Click the **Sys Config** tab. The ISDS System Configuration window opens.
3. Click the **ISDS** tab.
4. Enter information as described in ISDS Server Settings.
5. Click **Save**. The system saves the information and the status bar at the bottom of the window shows "Save complete."
6. Click **Close** to close the ISDS System Configuration window.

3

User Accounts

Introduction

The User Access List window allows you to add user accounts to the ISDS.

A dncs user account is established for you when your ISDS is installed. Because this account provides access to the applications required to manage and maintain the ISDS, we strongly recommend that you do not change the default settings for this account.

This section describes the procedures and security information required to manage user accounts.

In This Chapter

Creating a User Account

Follow these steps to create a user account.

1. In an ISDS xterm window where you are logged in as root, type **/dvs/dncs/etc/create_users** and press **Enter**.
2. Select the appropriate user type. For more information, see Types of Users.
3. Type the **name of the new user** and press **Enter**.

   Notes:

   - The user name must be between 6 and 8 characters.
   - The user name can contain alphanumeric characters.
   - The user name cannot contain special characters.

   Result: A Do you wish to continue adding this user (Y/N)? prompt displays.
4. Press **y** for yes and press **Enter**.
5. When prompted, type the **password** for the user and press **Enter**.
6. Re-enter the **password** for the user and press **Enter**.
7. Do you want to force the user to change passwords upon their first successful login?
   - If **yes**, type **passwd -r files -f [user name]** and press **Enter**.
   - If **no**, you are finished with this procedure.

4

Network Element Configuration

Introduction

The next step in setting up your network elements in the ISDS is to set up all of the logical network elements.

In This Chapter

Guidelines for Setting Up Network Elements

Remember the following guidelines as you set up logical network elements in your network:

- If you are setting up elements in an RCS, each site must have at least one headend.
- Each headend must have at least one hub.
- Each hub must have at least one cluster.
- Each cluster must have at least one localization code.

Headends

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Headend

The first logical element you must set up in your network is a headend. A headend is a logical element that represents a group of Digital Content Managers (DCMs).

You must add at least one headend per site. You can add an unlimited number of headends to the ISDS.

Add a Headend

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

Important: This procedure can be used for all systems except an RCS. If you use an RCS, follow the procedure in ***Add a Headend to an RCS Site*** (on page 255) to add headends to an RCS site. A different method is required because RCS headends must be associated with a particular site.

Complete these steps to add a headend to your network.

1. On the ISDS Administrative Console, click the **ISDS** 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 ISDS 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 this procedure from step 4.
   - If **no**, click **File > Close** to close the Headend List window and return to the ISDS Administrative Console. Go to ***Adding a Hub*** (see "***Add a Hub***" on page 22).

Modify a Headend

Quick Path: ISDS Administrative Console > ISDS 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.

Important: This procedure can be used for all systems except an RCS. A different method is required because RCS headends must be associated with a particular site.

1. On the ISDS Administrative Console, click the **ISDS** 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 ISDS 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. Change the headend name on your network map.
9. Do you need to modify another headend?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the Headend List window and return to the ISDS Administrative Console.

Delete a Headend

Important: This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to delete headends from an RCS site. A different method is required because these headends must be associated with a particular site.

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

1. Are there any hubs associated with this headend?
   - If **yes**, delete those hubs first. Go to ***Delete a Hub*** (on page 24). When finished, return to this procedure.
   - If **no**, go to step 2.
2. On the ISDS Administrative Console, click the **ISDS** 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 ISDS 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 ISDS Administrative Console.

10 Do you need to delete another headend?

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

Hubs

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

A hub is a logical element identified by a multicast IP address which set-tops join to acquire system information (SI). In the network topology, a hub belongs to a headend. A cluster belongs to a hub.

After you add a headend to the ISDS database, you must assign at least one hub to that headend. You can have an unlimited number of hubs per headend.

Hub Settings

Use the following fields when you manage hubs in the ISDS.

Field	Description
Headend Name	The headend associated with this hub.
Hub Name	The name you will use to identify this hub. You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.
Hub ID	The number you will use to identify this hub. Be sure to use an ID number that is consistent with the numbering scheme used on your network map. **Example:** You might type **11** as a numerical representation for Headend 1, Hub 1. **Important:** You will not be able to modify this field later.
Multicast Flow IP Address	The unique multicast IP address associated with the flow through this hub.
Source IP	The IP address of the ISDS (dncsatm) that controls this hub.
Timezone	The time zone where this hub is located.
DST Zone ID	The DST Zone ID for this hub. For more information, see: ■ ***DST Settings*** (on page 240) ■ ***View a DST Rule*** (on page 242)

Add a Hub

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Hub > Add Hub

Important: This procedure can be used for all systems except an RCS. If you are using an RCS, follow a different method to add hubs to an RCS headend. A different method is required because RCS hubs must be associated with a particular site. See ***Add a Hub to an RCS Site*** (on page 256) for more information.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Hub**. The Hub Summary window opens.
4. Click **Add Hub**. The Set Up Hub window opens.
5. Complete the fields on the screen as described in Hub Settings.
6. Click **Save**. A confirmation message opens.
7. Click **OK**. The system saves the hub information in the ISDS database and the Hub Summary window updates 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 this procedure from step 4.
   - If **no**, click **Exit** to close the Hub Summary window.
10. Go to ***Clusters*** (on page 26).

Modify a Hub

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

Important: This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to modify hubs in an RCS headend. A different method is required because these hubs must be associated with a particular site.

After a hub has been saved in the ISDS, you can modify only the following parameters for that hub:

- Hub name
- Timezone information
- DST Zone ID information

To change any other parameters, you must delete the hub, and re-add it to the ISDS, using the new information.

1. On the ISDS Administrative Console, click the **ISDS** 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 > Open**. The Set Up Hub window opens.

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 To change the time zone information for this hub, click the **Timezone** arrow and select the time zone where this hub is located.

8 To change the daylight saving time setting for this hub, click the **DST Zone ID** arrow and select the DST Zone ID for the hub. (For more information on DST Zone ID, see the **DST Zone ID** field in Daylight Saving Time Rules Settings. For more information on DST rules, see Configure Daylight Saving Time Rules Window.)

9 When you finish making changes, click **Save**. A confirmation message opens.

10 Click **OK**. The Set Up Hub window updates to include the new hub information. Set-tops receive updates within 10 minutes to an hour, depending on the size of your system. Rebooting a set-top causes it to apply updates immediately.

11 Update your network map to reflect these changes.

12 Do you need to modify another hub?

   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the Hub List window.

Delete a Hub

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

Important: This procedure can be used for all systems except an RCS. If you use an RCS, follow a different method to delete hubs from an RCS headend. A different method is required because these hubs must be associated with a particular site.

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.

You Need to Know

Before You Begin

Follow these instructions to delete a Hub from the ISDS.

1 Are there any clusters associated with this hub?

   - If **yes**, delete those clusters first. Go to ***Delete a Cluster*** (on page 27). When finished, return to this procedure.
   - If **no**, go to step 2.

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

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

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

5 Click once on the hub you want to delete.

6 Click **File > Delete**. A confirmation message opens.

7 Click **OK**. The message closes. The system removes the hub information from the ISDS 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 this procedure.
- If **no**, click **File > Close** to close the Hub Summary window.

Clusters

A cluster is a logical element that represents a collection of set-tops.

The cluster to which a set-top is assigned determines the channel map and system information (SI) that the set-top receives. Each cluster corresponds to a single multicast carousel that carries all of the cluster-specific data for that cluster.

Cluster Settings

Use the following fields when you manage clusters in the ISDS.

Field	Description
Name	The name you will use to identify this cluster.
ID	The Cluster ID fills in automatically, you do not enter it.
Source IP	The IP address of the ISDS (dncsatm) associated with this source.
SRM Host Name	The name of the Session Resource Manager. **Example:** Enter the IP address of the Business Management System (BMS).
Group Destination Address	The IP address associated with the cluster. **Example:** You might type **232.30.30.3** to indicate that this cluster is associated with the 30303 zip code.
Hub Association	The hub associated with the cluster.
Staging Bridge	Indicates whether or not the hub is used to stage set-tops.
EAS Service ID	Not available at this time.

Add a Cluster

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Cluster > New

After you add a hub to the ISDS database, you must assign at least one cluster to that hub.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Cluster**. The ISDS Cluster Parameters window opens.
4. Click **New**. A row of empty fields appears for the new cluster.

   Note: The ID field defines the identification number for a cluster and cannot be specified. This value is assigned by the ISDS and is automatically added to the cluster when it is saved to the system.
5. Enter information as described in Cluster Settings.

6 Click **Save**. The system saves the cluster information in the ISDS database and the ISDS Cluster Parameters window updates to include the new cluster and also assigns an ID to the cluster.
7 Add the new cluster to your network map.
8 Do you need to add another cluster?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to close the ISDS Cluster Parameters window.

Modify a Cluster

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Cluster

After a cluster has been saved in the ISDS, you can modify all parameters except the Cluster ID for that cluster.

To change the Cluster ID, you must delete the cluster, and re-add it to the ISDS, using the new information.

Follow these instructions to modify a cluster.

1 On the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **Cluster**. The ISDS Cluster Parameters window opens.
4 Select the cluster that you want to modify. A check mark appears in the Select box and the row is highlighted.

   Note: You can also click in the exact field you wish to modify. The row for that cluster becomes highlighted and a check mark appears in the Select box for that cluster.
5 Modify the parameters as required based on the definitions in Cluster Settings.
6 Do you need to modify another cluster?
   - If **yes**, repeats steps this procedure from step 4.
   - If **no**, go to step 7.
7 Click **Save**. The ISDS Cluster Parameters window updates to include the new information for the cluster. set-tops receive updates within a few minutes to an hour, depending on the size of your system. Rebooting a set-top causes it to apply updates immediately.
8 Update your network map to reflect these changes.
   - Click **Cancel** to exit the ISDS Cluster Parameters window.

Delete a Cluster

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Cluster > [Cluster name] > Delete

You may need to delete a cluster because you are no longer using it or because you need to redefine the headend or ID. Complete the following steps to delete a cluster from the ISDS.

Important: Deleting a cluster automatically deletes any localization codes assigned to the cluster.

Follow these instructions to delete a cluster.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Cluster**. The ISDS Cluster Parameters window opens.
4. Select the cluster that you want to delete. A check mark appears in the Select box and the row is highlighted.
5. Click **Delete**. A confirmation message opens.
6. Click **OK**. The message closes. The system removes the cluster information and any associated localization codes from the ISDS database and from the ISDS Cluster Parameters window.
7. Remove the cluster from your network map.
8. Do you need to delete another cluster?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to close the ISDS Cluster Parameters window.

Localization Codes

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Localization

A localization code provides for a subgrouping of set-tops and allows the set-tops to transmit UNConfig data. Creating a group of set-tops smaller than a cluster allows you to categorize set-tops for the purposes of customization and personalization of data and data delivery.

For example, you might assign a group of set-tops to the same Localization Code so that these set-tops receive the same billing information or advertisements.

In the US, the localization code ID is the ZIP+4 code for the service address. For international installations, alternate localization IDs will need to be established according to local designations.

Localization Code Settings

Use the following fields when you manage localization codes in the ISDS.

Field	Description
ID	A unique numerical identifier you will use to identify this localization code. ■ If you are in the US, enter the ZIP+4 code for the service address for this cluster. ■ If you are not in the US, you will need to establish an alternate localization ID process according to local designations.
Name	The name you will use to identify this localization code. You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming scheme used on your network map.
Cluster Association	The cluster associated with this localization code.

Add a Localization Code

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Localization > New

After you add a cluster to the ISDS database, assign at least one localization code to the cluster. One cluster can have more than one localization code assigned to it.

Follow these instructions to add a localization code.

1 From the ISDS Administrative Console, click the **ISDS** tab.

2 Click the **Network Element Provisioning** tab.
3 Click **Localization**. The ISDS Localization Codes window opens.
4 Click **New**. A row of empty fields appears for the new localization code.
5 Enter information as described in Localization Code Settings.
6 Click **Save**. The system saves the localization code information in the ISDS database and the ISDS Localization Codes window updates to include the new code.
7 Add the new localization code to your network map.
8 Do you need to add another localization code?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to close the ISDS Localization Codes window.

Modify a Localization Code

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Localization

After a localization code has been saved in the ISDS, you can modify all of the parameters except the localization code ID.

Note: To change the localization code ID, you must delete the localization code, and re-add it to the ISDS using the new ID.

Follow these instructions to modify a localization code.

1 On the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **Localization**. The ISDS Localization Codes window opens.
4 Select the localization code that you want to modify. A check mark appears in the Select box and the row is highlighted.

   Note: You can also click in the exact field you wish to modify. The row for that localization code becomes highlighted and a check mark appears in the Select box for that localization code.
5 Change the information as described in Localization Code Settings.
6 Click **Save**. The ISDS Localization Codes window updates to include the new information. Set-tops receive updates within a few minutes to an hour, depending on the size of your system. Rebooting a set-top causes it to apply updates immediately.
7 Update your network map to reflect these changes.
8 Click **Cancel** to close the ISDS Localization Codes window.

Delete a Localization Code

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > Localization

You may need to delete a localization code because you are no longer using it or because you need to redefine the headend or ID.

Follow these instructions to delete a localization code.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Localization**. The ISDS Localization Codes window opens.
4. Select the localization code that you want to delete. A check mark appears in the Select box and the row is highlighted.
5. Click **Delete**. A confirmation message opens.
6. Click **OK**. The message closes. The system removes the localization code information from the ISDS database and from the ISDS Localization Codes window.
7. Remove the localization code from your network map.
8. Do you need to delete another localization code?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Cancel** to close the ISDS Localization Codes window.

55-1 QPSK

The 55-1 QPSK configuration allows you to use third-party QPSK devices to send command and control data to set-tops using the SCTE55-1 protocol.

This section describes the procedures you need to configure the 55-1 QPSK.

55-1 QPSK Settings

Use the following fields when you manage 55-1 QPSKs in the ISDS.

Field	Description
Bridge ID	Type a unique number that identifies the QPSK bridge you are setting up.
Hub Name	Select the hub associated with the QPSK from the list.
Name	Type a unique name for the QPSK.
IP Address	The IP address of the QPSK.
Return Path IP	If not specified on the QPSK, type the ISDS public IP address.
DHCT Reboot Log Server IP	The IP address of an archive log server. When the set-top reboots, it sends log files to this server.
Frequency	Type the frequency that this QPSK uses to distribute the command and control data.
DCM	Select the DCM associated with this QPSK (if applicable).

Add a 55-1 QPSK

Quick Path: ISDS Administrative Console > Network Element Provisioning tab > 55-1 QPSK > File > New > 55-1 QPSK

Follow these instructions to add a 55-1 QPSK.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **55-1 QPSK**. The 55-1 QPSK List window opens.
4. Select **File > New > 55-1 QPSK**. The Add 55-1 QPSK window opens.
5. Complete the fields on the screen as described in 55-1 QPSK Settings.
6. Click **Save**. The 55-1 QPSK List window updates to show the new QPSK.
7. Add the QPSK to your network map.

Modify a 55-1 QPSK

Quick Path: ISDS Administrative Console > Network Element Provisioning tab > 55-1 QPSK > [select QPSK] > File > Open

After you add a 55-1 QPSK, you can modify all parameters of the QPSK except its bridge number. To change the bridge number of the 55-1 QPSK, you must delete the QPSK and re-add it.

Follow these instructions to modify a 55-1 QPSK.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **55-1 QPSK**. The 55-1 QPSK List window opens.
4. Select a QPSK in the list and select **File > Open**. The Add 55-1 QPSK window opens.
5. Complete the fields on the screen as described in 55-1 QPSK Settings.
6. Click **Save**.
7. Make any pertinent changes to your network map.

Delete a 55-1 QPSK

Quick Path: ISDS Administrative Console > Network Element Provisioning tab > 55-1 QPSK > [select QPSK] > File > Delete

Follow these instructions to delete a 55-1 QPSK.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **55-1 QPSK**. The 55-1 QPSK List window opens.
4. Select the QPSK you want to delete.
5. Select **File > Delete Bridge**. A confirmation window opens.
6. Click **OK**. The QPSK is deleted from the ISDS database.
7. Remove the QPSK from your network map.

VQE

This section contains procedures for setting up the VQE in the ISDS.

There are procedures you need to complete (setting up the VQE server and setting up network connectivity) before starting this process in the ISDS. Refer to the documentation you received with your VQE server before proceeding with these steps.

Overview

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE

Visual Quality Experience (VQE) is a real-time error repair and quick-channel change system for system providers delivering broadcast data over DSL in an network.

The equipment used to provide VQE in a system includes the following:

- VQE Server at the Edge Router
- VQE Server in the headend (provisioned through the ISDS)
- Digital Content Manager (DCM) in the headend
- VQE Client on the set-tops

VQE uses the following advanced techniques to provide this quality assurance:

- Edge-optimized solution with application level Forward Error Correction (FEC) and selective RTP retransmission
- Monitoring and reporting per subscriber

You can configure VQE on a per-channel basis. For example, FEC can be turned off for HD channels to conserve bandwidth.

Error Correction

The VQE provides error correction of broadcast data over DSL.

If the set-top client receives a transmission packet with errors, or misses a packet entirely, it notifies the VQE server. The VQE server transmits the missed packet to the set-top, where it is assembled in its original order to be viewed by the subscriber.

Quick Channel Change

The VQE also provides a method of speeding up channel change requests of broadcast data over DSL. When the subscriber changes the set-top channel to a VQE channel, the set-top requests a unicast from the VQE server. The VQE server then streams the new channel to the set-top as a unicast until the set-top buffer catches up to the multicast stream of the channel. The set-top then switches to the multicast channel stream.

For more information on the theory and operation of the VQE, refer to the documentation provided with your VQE server.

VQE Settings

This section contains the settings you need to consider when you manage VQEs in the ISDS.

VQE Global Parameter Settings

Use the following fields when you manage VQE global parameters in the ISDS.

Field	Description
Report Interval	Defines how often (in seconds) the VQE client sends an RTCP report to the server. ■ The default value is **5**.
Maximum Receivers	Total number of VQE clients expected to tune to this channel. The server uses this number to determine how often it transmits the RTCP report to the video source for this channel.
Original Stream Average Packet Size	Average size of the packets in the original video source as determined by the program distributor.
Repair Stream Average Packet Size	Average size of the packets in the repair stream.

VQE Server Settings

Use the following fields when you manage VQE servers in the ISDS.

Field	Description
Server ID	A unique ID that identifies this VQE server. **Note:** If you do not enter a Server ID, the system will assign the next available number. Be sure to use an ID that is consistent with the naming conventions of your network map. You will not be able to change the ID later.
Name	Unique name for the VQE server. You can use up to 15 alphanumeric characters. Be sure to use a name that is consistent with the naming conventions of your network map.
IP Address	The management IP address of this VQE server. This IP address is the virtual IP address that works to load balance the VQE interfaces.
Admin Status	Determines whether the VQE server is active.

VQE Channel Settings

Use the following fields when you manage VQE servers in the ISDS.

Field	Description
Original Stream	
Server Mode	Defines where the VQE server resides in the video path: ■ **Lookaside** - Select when the VQE server is not in the direct video path. ■ **Source** - Select when the VQE server is directly in the video path.
IP Source	Select the original video stream from the IP Source drop-down menu.
Error Correction?	Determines whether the VQE server provides error correction for this channel. Select the **Error Correction?** option to have the VQE server process this channel for error correction.
Fast Channel Change?	Determines whether the VQE server provides fast channel change service for this channel. Select the **Fast Channel Change?** option to have the VQE server process this channel for fast channel change.
Retransmission Stream	
Feedback Address	A unique IP address for each VQE channel.
RTP Port	The RTP port on the VQE server that accepts receiver reports (RRs). RRs contain information about UDP packet loss and delay variation (jitter).

RTCP Port	The RTCP port on the VQE server that accepts negative acknowledgement (NAK) messages that identify missing or corrupted packets from the VQE client on the set-top. Can be unique or you can use the same port number across all the feedback addresses.
Unicast Mode	Select one of the following options: ■ Summary ■ Reflect
Summary Mode	Only displays if Summary is selected as the Unicast Feedback Mode. Select one of the following options: ■ None ■ Aggregate ■ Forward ■ Term
Retransmit Time	Leave at the default value.

Add a VQE

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE

This section contains procedures for setting up the VQE in the ISDS.

Important: These procedures are for setting up the VQE in the ISDS. There are procedures you need to complete (setting up the VQE server and setting up network connectivity) before starting this process in the ISDS. Refer to the documentation you received with your VQE server before proceeding with these steps.

Complete these steps to set up the VQE in the ISDS.

1. ***Verify the Network Connection*** (on page 37) from the ISDS to the VQE server.
2. ***Set Up VQE Global Parameters*** (on page 38).
3. ***Add a VQE Server*** (on page 38).
4. ***Add a VQE Channel*** (on page 39).
5. ***Associate VQE Channels with VQE Servers*** (on page 39).
6. ***Provisioning the VQE Configuration*** (on page 40)

Verify the Network Connection

Before you begin adding the information for the VQE server to the ISDS, you should verify that the ISDS can communicate with the VQE server over the network.

1. Open an xterm window on the ISDS.
2. Type **ping [IP address of the VQE server]** and press **Enter**.

Example: Type **ping 10.253.2.1** and press **Enter**. Do not type the brackets **[ ]** in the command.

3 Does the VQE server respond as **alive**?

- If **yes**, you have network connectivity with the VQE server. You are finished with this procedure.
- If **no**, check with your system administrator to make sure you have the correct IP address for the VQE server.

4 Is the IP address for the VQE server correct?

- If **yes**, verify that the VQE is physically connected to the correct network.
- If **no**, correct the IP address and repeat this procedure from step 2.

Set Up VQE Global Parameters

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Parameters > Global Parameters Screen

This section contains the information you need to add the global VQE parameters to the ISDS.

1 From the ISDS Administrative Console, click the **ISDS** tab.

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

3 Click **VQE**. The VQE Channels screen opens.

4 Click **Parameters**. The Global Parameters screen opens.

5 Complete the fields as described in VQE Global Parameter Settings.

6 When you are finished, click **Save**.

Add a VQE Server

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Servers > Add > Add Server Screen

Before you add a VQE server, you need the following information:

- Name and ID for the server that is compatible with your naming convention (check your network map or network administrator for more information)
- IP address of the VQE server

Follow these instructions to add a VQE server.

1 From the ISDS Administrative Console, click the **ISDS** tab.

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

3 Click **VQE**. The VQE Channels screen opens.

4 Click **Servers**. The VQE Servers screen opens.

5 Click **Add**. The Add Server screen opens.

6 Complete the fields as described in VQE Server Settings.

7 When you are finished, click **Save**.

8 Do you need to add another VQE server to the ISDS?

- If **yes**, repeat this procedure from step 5.
- If **no**, go to ***Add a VQE Channel*** (on page 39).

Add a VQE Channel

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Channels > Add > Add Channel Screen

Before you add a VQE channel to the ISDS, you need the following information:

- VQE server mode
- IP source
- Whether this channel will use error correction or fast channel change, or both
- Feedback address for retransmission
- RTP and RTCP ports for retransmission
- Unicast feedback mode (summary or reflect)
- Summary feedback mode (aggregate, forward, or term)
- Retransmit time

You also need to make sure the following prerequisites are met:

- The Output Protocol of the transport stream must be set to RTP on the DCM.
- The video source must exist in the IP Source Definition section of the ISDS and be set to RTP.

Follow these instructions to add a VQE channel.

1 From the ISDS Administrative Console, click the **ISDS** tab.

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

3 Click **VQE**. The VQE Channel screen opens.

4 Click **Add**. The Add Channel screen opens.

5 Complete the fields as described in VQE Channel Settings.

6 Click **Save**.

7 Do you need to add another channel?

- If **yes**, repeat this procedure from step 4.
- If **no**, go to ***Associate VQE Channels with VQE Servers*** (on page 39).

Associate VQE Channels with VQE Servers

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Associations > Associate

VQE Channels with Servers Screen

This section contains the information you need to associate a VQE channel with a VQE server in the ISDS

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VQE**. The VQE Channels window opens.
4. Click **Associations**. The Associate VQE Channels with Servers screen opens.
5. Select a server from the Servers list. The Available Channels and Selected Channels lists open.
6. Select a channel from the Available Channels list and click **Add**. The channel moves to the Selected Channels list and is now associated with this server.

   Note: To select all the Available Channels, select the box next to Available Channels.
7. When you are finished selecting channels, click **Save**.
8. Provision the configuration changes. See ***Provisioning the VQE Configuration*** (on page 40) for more information.

Provisioning the VQE Configuration

Provisioning the VQE configuration sends the ISDS configuration information to the VQE server.

1. From any VQE screen, click **Provisioning**. The Provisioning screen opens.
2. Click **Send** to provision the VQE configuration. The status of each channel updates and displays in the Status column.

   Note: Click **Refresh** to view the status message changes.

VQE Log Locations

The VQE creates several logs as it repairs errors and facilitates quick-channel changes. These logs and their locations on the VQE are as follows:

- VQE-S log: **/var/log/vqe/vqe.log**
- System messages log: **/var/log/messages**
- HTTPD error log: **/var/log/httpd/error_log**
- SSL error log: **/var/log/httpd/ssl_error_log**
- Tomcat log: **/usr/share/tomcat5/logs/catalina.out**

VQE Fast-Fill

VQE Fast-Fill reduces the video decoder buffering delay when you tune to a new multicast stream.

You can dedicate a customizable amount of bandwidth for allowing the VQE Server to fast-fill the video decoder buffer. This bandwidth can and should be configured for your site to achieve optimal performance.

Enable Fast-Fill on the VQE

Follow these instructions to enable fast-fill on the VQE server.

1. From an xterm window on the ISDS, ssh to the VQE server.
2. Log into the VQE server as root user.
3. Type **cd /etc/opt/vqes** and press **Enter**. The vqes directory becomes the working directory.
4. In a UNIX text editor, open the **vcdb.comf** file for editing.
5. Add the following line to the vcdb.conf file:

   vqe.vqes.fastfill_enable="true";
6. Save and close the vcdb.conf file.
7. Type **vqe_cfgtool -apply** and press **Enter**. The system sources the vcdb.conf file.

Modify the Excess Bandwidth Fraction for Fast-Fill

Follow these directions to modify the excess bandwidth fraction.

1. From an xterm window on the ISDS, ssh to the VQE server.
2. Log into the VQE server as root user.
3. Type **cd /etc/opt/vqes** and press **Enter**. The vqes directory becomes the working directory.
4. In a UNIX text editor, open the **vcdb.comf** file for editing.
5. Add the following lines to the vcdb.conf file:

   vqe.vqes.excess_bw_fraction="100";

   vqe.vqes.excess_bw_fraction_high_def="100";
6. Save and close the vcdb.conf file.
7. Type **vqe_cfgtool -apply** and press **Enter**. The system sources the vcdb.conf file.

Add the vqec.conf File to the BFS Carousel on the ISDS

Follow these instructions to add the vqec.conf file to the BFS carousel.

1. FTP the **vqec.cfg** file to the ISDS.
2. Copy the file to the **/dvs/dvsFiles/VQE directory** on the ISDS.
3. From the ISDS Administration Console, click the **Application Interface Modules** tab.
4. Click **BFS Client**. One of the following windows opens:
   - **If you are using an RCS,** the BFS Client Sites opens. Go to step 5.

- **If you are not using an RCS,** the Site [site name] Broadcast File Server list opens. Go to step 6.

5 Select **File > All Sites**.The Site AllSites Broadcast File Server list opens.

6 Select **VQEC** from the list and click **File > New Link**. The Set Up Link window opens.

7 Enter the following options in the Set Up Link window:

- Link Name: **vqec.cfg**
- Source Name: **VQE Client**

8 Click **Select** to browse to the **vqec.cfg** file you copied to the **/dvs/dvsFiles/VQE** directory.

9 Click **Save**.

Example vqec.cfg File

The following is an example of a vqec.cfg file for your reference.

Important: Your exact vqec.cfg file will likely have different configuration parameters.

```
 * Copyright (c) 2007 by Cisco Systems, Inc.

 * All rights reserved.

 */

channel_lineup = "/var/vqe_channels.cfg"; /* an SDP configuration file. Will
be empty in non-standalone mode */

vqe.vqes.fastfill_enable="true";

vqe.vqes.excess_bw_fraction="100";

vqe.vqes.excess_bw_fraction_high_def="100";

sig_mode = "NAT";

input_ifname = "eth0";

output_ifname = "eth0";

max_tuners = 4;

libcli_telnet_port = 8182;

pakpool_size = 3600;

so_rcvbuf = 524288;

jitter_buff-size = 500;

repair_trigger_point_abs = 20;

reorder_delay_abs = 20;

max_paksize = 1344;

cli_ifname = "*";

vcds_server_ip = "172.16.10.2";
```

```
cdi_enable = true;
output_pakq_limit = 2000
```

Modify a VQE

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > [Select VQE] > File > Open

This section contains details about modifying a VQE in the ISDS.

Modifying VQE Global Parameters

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Parameters

Follow these instructions to modify a VQE's global parameters.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VQE**. The VQE Channels window opens.
4. Click **Parameters**. The Global Parameters screen opens.
5. Change the global parameters as described in VQE Global Parameter Settings.
6. When you finish making changes, click **Save**.
7. Provision the configuration changes. See ***Provisioning the VQE Configuration*** (on page 40) for more information.

Modifying VQE Servers

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Servers > [Select Server] > Details

Follow these instructions to modify a VQE server.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **VQE**. The VQE Channels window opens.
4. Click **Servers**. The VQE Servers screen opens.
5. Select the server you want to modify and click **Details**. The View Server screen opens.
6. Change the server parameters as described in VQE Server Settings.
7. When you are finished, click **Save**.
8. Provision the configuration changes. See ***Provisioning the VQE Configuration*** (on page 40) for more information.

Modifying VQE Channels

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > [Select Channel] > Details

Follow these instructions to modify a VQE channel.

1 From the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **VQE**. The VQE Channels window opens.
4 Select the channel you want to modify and click **Details**. The View Channel screen opens.
5 Change the channel parameters as described in VQE Channel Settings.
6 When you are finished, click **Save**.
7 Provision the configuration changes. See ***Provisioning the VQE Configuration*** (on page 40) for more information.

Delete a VQE

This section contains details about removing associations from VQE servers and about deleting a VQE in the ISDS.

Removing Associations from VQE Servers

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Associations > Associate VQE Channels with Servers Screen > [Select Server] > [Select Channel] > Remove

Follow these instructions to remove associations from a VQE server.

1 From the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **VQE**. The VQE Channels window opens.
4 Click **Associations**. The Associate VQE Channels with Servers screen opens.
5 Select a server from the Servers list. The Available Channels and Selected Channels lists open.
6 Select a channel from the Selected Channels list and click **Remove**. The channel moves to the Available Channels list and is no longer associated with this server.

   Note: To remove all of the Selected Channels, select the box next to Selected Channels and click **Remove**.
7 When you are finished selecting channels, click **Save Changes**.
8 Provision the configuration changes. See ***Provisioning the VQE Configuration*** (on page 40) for more information.

Deleting VQE Channels

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > [Select Channel] > Delete

You do not need to remove the channel associations before you delete a channel from the VQE configuration.

Follow these instructions to delete a VQE channel.

1 From the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **VQE**. The VQE Channels window opens.
4 Select the channel you want to delete and click **Delete**. A confirmation window opens.

   Note: If the channel has associations with servers, the confirmation will ask if you want to continue with the deletion.
5 Click **OK**. The ISDS removes the channel from the VQE Channels list.
6 Provision the configuration changes. See ***Provisioning the VQE Configuration*** (on page 40) for more information.

Deleting VQE Servers

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VQE > Servers >[Select Server] > Delete

Before you delete a VQE server, you must remove all associations from that server. See ***Removing Associations from VQE Servers*** (on page 44) for more information.

Follow these instructions to delete a VQE server.

1 From the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **VQE**. The VQE Channels window opens.
4 Click **Servers**. The VQE Servers screen opens.
5 Select the server you want to delete and click **Delete**. A confirmation window opens.
6 Click **OK**. The ISDS removes the server from the VQE Servers list.

PCG

This section provides an overview of the PowerKEY® Conditional Access System (CAS) and describes the PowerKEY CAS Gateway (PCG). It also contains provisioning procedures for the PCG.

PowerKEY Conditional Access System (CAS)

PowerKEY CAS is a flexible, secure Digital Rights Management (DRM) system for supporting digital services. The PowerKEY CAS system offers software-based encryption and decryption and uses a combination of symmetric and asymmetric keys to secure the Entitlement Control Message (ECM).

PowerKEY CAS can be configured within cable-based networks, IP networks, and hybrid IP/RF networks. This section only covers the North American configuration. For information on the International configuration, refer to *PowerKEY CAS Gateway (PCG) Installation and Operation Guide* (part number 4017672).

PowerKEY CAS Gateway (PCG) Overview

The PCG can be integrated with a DVB SCS-compliant scrambler through the ECMG-to-Simulcrypt Synchronizer (SCS) interface to function as an ECM Generator (ECMG). In an IPTV and Broadband Delivery System (IBDS) network, PCGs can be deployed in a redundant server farm configuration as subordinates to an SCS, such as the Motorola SmartStream Encryptor/Modulator (SEM). The SCS/SEM is assigned the role of both managing redundancy (that is, PCG impairment) as well as load-balancing ECM request traffic between the PCGs within a given PCG server farm.

You can access the PCG interface and configure the PCG in two ways: use the PCG serial console or login through Secure Shell (SSH) from your network-control platform.

The ISDS manages (creates and deletes) PCG sessions, which deliver the attributes of an MPEG program (e.g., access criteria, ECM format, session ID, etc.) to the PCG.

PCG Settings

There are tabs that provide access to the different PCG settings areas. Click one of the tabs to set up the parameters.

Primary PCG Settings

Use the following fields when you manage a primary PCG in the ISDS.

Field	Description
	PCG Identification
ID	A unique value belonging to a PCG device on the ISDS.
Headend	The name of the headend at the site where the PCG is used.
Name	The name of the PCG.
Status	Indicates that the pkeManager process in the ISDS is now communicating with this particular PCG.
	PCG Network Parameters
PCG IP Address	IP address of the PCG interface that communicates with the ISDS.
PCG MAC Address	MAC Address of the PCG Ethernet port that communicates with the ISDS.
PCG IP Subnet Mask	Subnet mask of the PCG interface that communicates with the ISDS.
PCG IP Default Gateway	IP address of the gateway the PCG uses to communicate with the ISDS.
SCS Interface IP Address	The IP address of the interface the PCG uses to communicate with the SCS on a private network.
SCS Interface Subnet Mask	The subnet mask of the interface the PCG uses to communicate with the SCS on a private network.
SCS Interface Default Gateway	The gateway the PCG uses to communicate with the SCS on a private network.

Secondary PCG Settings

Use the following fields when you manage a secondary PCG in the ISDS.

Field	Description
	PCG Identification
Secondary PCG	Check this box to identify this PCG as a secondary PCG device.
ID	A unique value identifying the secondary PCG device on the ISDS.
Name	The name of the secondary PCG.
Status	Indicates whether the secondary PCG is active (online) or inactive (offline).
	PCG Network Parameters
PCG IP Address	IP address of the secondary PCG interface that communicates with the ISDS.
PCG MAC Address	MAC Address of the secondary PCG Ethernet port that communicates with the ISDS.

PCG IP Subnet Mask	Subnet mask of the secondary PCG interface that communicates with the ISDS.
PCG IP Default Gateway	IP address of the gateway the secondary PCG uses to communicate with the ISDS.
SCS Interface IP Address	The IP address of the interface the secondary PCG uses to communicate with the SCS on a private network.
SCS Interface Subnet Mask	The subnet mask of the interface the secondary PCG uses to communicate with the SCS on a private network.
SCS Interface Default Gateway	The gateway the secondary PCG uses to communicate with the SCS on a private network.

Additional Parameters Settings

Use the following fields when you manage additional parameters for a PCG in the ISDS.

Field	Description
SCS Interface Parameters	
Leave all these fields at their default values.	
DNCS Parameters	
Max PCG Sessions	The maximum number of sessions for the PCG. This value is based on network traffic. Determine how many sessions the network is likely to run and set your value to a number 2% higher than the likely number of sessions. **Valid values:** Any number from 1 to 1000 inclusive.
PCG Msg Timeout (seconds)	The pkeManager manages PCG provisioning and sessions. This timeout indicates the period that the pkeManager process will wait for any communication with the PCG before timing out. **Valid values:** 5 to 60 (seconds).
Default Scrambling mode	Leave at default value.
PCG Settings	
Config File	The configuration file (pcg.cfg) that is downloaded at power up by the "bootup" software and contains the name of the pcg software executable.
SCS Test Timeout (seconds)	Leave at default value.
Support External Access Criteria	Leave at default value.
External_AC_Length	Leave at default value.

Enforce DVB Control Word Conformance	Leave at default value.

SCS Devices Settings

Use the following fields when you manage SCS devices for a PCG in the ISDS.

Field	Description
SCS Device Name	The name of the SCS device.
SCS Device Type	The type of SCS device. Select one of the following: ■ Encrypting ■ Clear
Linked SCS Device	Indentifies the pair of SCS devices that act as redundant devices. ■ If this SCS device is a primary device, select **None**. ■ If this SCS device is a secondary device, select the primary SCS device from the list.

Add a PCG

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > PCG > PowerKEY CAS Gateway screen > Add

Follow these instructions to add a PCG to the ISDS.

Important: If you are running PowerKEY MediaCypher ServCrypt, see Appendix A in the *PowerKEY CAS Gateway (PCG) Installation and Operation Guide* (part number 4017672) for installation instructions.

Adding a Primary PCG

1. Obtain the first MAC address from the label on the PCG.

   Note: To find the PCG MAC address, open an xterm window, type **/sbin/ifconfig eth0** and press **Enter.**
2. From the ISDS Administrative Console, select the **Network Element Provisioning** tab.
3. Click **PCG**. The PowerKEY CAS Generators window opens.
4. Click **Add**. The Update PowerKEY CAS Gateway window opens.
5. Click the **Primary PCG** tab.
6. Complete the fields on the interface as described in Primary PCG Settings.
7. Are you adding a secondary PCG at the same time as the primary PCG?

- If **yes**, click the **Secondary PCG** tab and complete the fields on the interface as described in Secondary PCG Settings.

  Note: Several of the fields are required to remain at their default values. Do not change those values unless instructed to by Cisco® Services.

- If **no**, continue with the next step in this procedure.

8 Click the **Additional Parameters** tab.

9 Complete the fields on the interface as described in Additional Parameters Settings.

  Note: Several of the fields are required to remain at their default values. Do not change those values unless instructed to by Cisco® Services.

10 Click the **SCS Devices** tab.

11 Complete the fields on the interface as described in SCS Devices Settings.

12 Click **Save**. The record is saved to the database and the provisioning information is sent to the PCG.

  Important: Make sure the physical connection of this interface is connected to the ISDS VLAN on the router.

13 Power on the PCG. The PCG software should run. If it does not, contact Cisco Services.

Adding a Secondary PCG

1 From the ISDS Administrative Console, select the **Network Element Provisioning** tab.

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

3 Click **Add**. The Update PowerKEY CAS Gateway window opens.

4 Click the **Secondary PCG** tab.

5 Complete the fields on the interface as described in Secondary PCG Settings.

  Note: Several of the fields are required to remain at their default values. Do not change those values unless instructed to by Cisco® Services.

6 Click **Save**. The record is saved to the database and the provisioning information is sent to the PCG.

Adding SCS Devices

SimulCrypt Synchronizer (SCS) devices are the MPEG Elementary Stream (Video/Audio) scrambling devices. The SCS Device interacts with the ECM Generator (ECMG), in this case the PCG, to generate ECMs.

Follow these instructions to add SCS devices to the PCG.

1 From the ISDS Administrative Console, select the **Network Element Provisioning** tab.

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

3 Select a PCG from the list and click **Edit**.

4 Click the **SCS Devices** tab.
5 Complete the fields on the interface as described inSCS Devices Settings.
6 Click **Save**. The record is saved to the database and the provisioning information is sent to the PCG.

Modify a PCG

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > PCG > PowerKEY CAS Gateway screen > [select PCG] > Edit

Follow these instructions to modify a PCG in the ISDS.

Modifying a Primary PCG

1 From the ISDS Administrative Console, select the **Network Element Provisioning** tab.
2 Click **PCG**. The PowerKEY CAS Generators window opens.
3 Select a PCG in the list and click **Edit**. The Update PowerKEY CAS Gateway window opens.
4 Modify the fields on the interface as described in Primary PCG Settings.
5 Click the Additional Parameters tab.
6 Modify the fields on the interface as described in Additional Parameters Settings.

   Note: Several of the fields are required to remain at their default values. Do not change those values unless instructed to by Cisco Services.
7 Click **Save**. The record is saved to the database and the updated provisioning information is sent to the PCG.

Modifying a Secondary PCG

1 From the ISDS Administrative Console, select the **Network Element Provisioning** tab.
2 Click **PCG**. The PowerKEY CAS Generators window opens.
3 Select a PCG in the list and click **Edit**. The Update PowerKEY CAS Gateway window opens.
4 Click the **Secondary PCG** tab.
5 Modify the fields on the interface as described in Secondary PCG Settings.

   Note: Several of the fields are required to remain at their default values. Do not change those values unless instructed to by Cisco Services.
6 Click **Save**. The record is saved to the database and the updated provisioning information is sent to the PCG.

Modifying an SCS Device

1. From the ISDS Administrative Console, select the **Network Element Provisioning** tab.
2. Click **PCG**. The PowerKEY CAS Generators window opens.
3. Select the PCG associated with the SCS device you want to modify in the list and click **Edit**. The Update PowerKEY CAS Gateway window opens.
4. Click the **SCS Devices** tab.
5. Modify the fields on the interface as described in SCS Devices Settings.

   Note: Several of the fields are required to remain at their default values. Do not change those values unless instructed to by Cisco Services.
6. Click **Save**. The record is saved to the database and the updated provisioning information is sent to the PCG.

Reset a PCG

Quick Path: DNCS Administrative Console > ISDS tab > Network Element Provisioning tab > PCG > PowerKEY CAS Gateway screen > [select PCG] > Reset Device

Resetting a PCG from the ISDS reboots the PCG. Follow these steps to reboot a PCG from the ISDS.

1. From the ISDS Administrative Console, select the **Network Element Provisioning** tab.
2. Click **PCG**. The PowerKEY CAS Generators window opens.
3. Select a PCG in the list and click **Reset Device**. A confirmation message appears.
4. Click **Yes**. The PCG resets.

Delete a PCG

Quick Path: DNCS Administrative Console > ISDS tab > Network Element Provisioning tab > PCG > PowerKEY CAS Gateway screen > [select PCG] > Delete

Follow these instructions to delete a PCG from the ISDS.

Deleting a PCG

1. From the ISDS Administrative Console, select the **Network Element Provisioning** tab.
2. Click **PCG**. The PowerKEY CAS Generators window opens.
3. Select a PCG in the list and click **Delete**. A confirmation window opens.
4. Click **OK**. The PCG is removed from the ISDS database.

Deleting an SCS Device

1. From the ISDS Administrative Console, select the **Network Element Provisioning** tab.

2 Click **PCG**. The PowerKEY CAS Generators window opens.
3 Select the PCG associated with the SCS device you want to delete and click **Edit**.
4 Click the **SCS Devices** tab.
5 Select an SCS device in the list and click **Delete SCS**. A confirmation window opens.
6 Click **OK**. The device is removed from the database and the updated provisioning information is sent to the PCG.

Download Server

The download server is an optional setup that allows you to have a secondary server to push device images to network devices, such as set-tops and CableCARD modules.

Important: This section only contains procedures to configure the ISDS to use a download server. Before you begin these procedures, you must have already installed and configured the server itself. For more information on installing and configuring the download server, refer to *Download Server Upgrade Guide* (part number 4026602).

Settings

There are two sets of settings you need to know about to configure the download server in the ISDS: the download server settings, and the settings for the BFS carousel.

Download Server Settings

Use the following fields when you manage download servers in the ISDS.

Field	Description
Device ID	The ISDS will automatically assign an ID to the download server.
Device Name	Type a unique name for this download server.
Device IP	Type the IP address of the download server you are adding.
Device Type	The type of download server you are adding. Select **HTTP**.
Site ID	Select the site associated with this download server.
Enabled	Determines whether the download server is enabled. Check the **Enabled** box to enable the device.

BFS Carousel Settings for Download Server

Use the following fields when you manage BFS carousels for download servers in the ISDS.

Field	Description
Server Name	Type a unique name that corresponds to the download server this BFS carousel is associated with.
Unicast Download	Enable this option for the download server carousel.
Sources	From the Available Sources list, select the download server this carousel is associated with. Click **Add** to move that server to the Selected Sources list.

Add a Download Server

Quick Path: ISDS Administration Console > ISDS tab > Network Element Provisioning tab > Download Server > New

You Need to Know

Process Overview

Follow these instructions to add a download server to the ISDS.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Download Server**. The Download Servers window opens and displays any current download servers in your network.
4. Click **New**. A blank line appears at the top of the list.
5. Complete the fields as described in Download Server Settings.
6. Click **Save**. The list updates to include your new download server.
7. Add the new download server to your network map.

Add a BFS Carousel for the Download Server

Quick Path with RCS: ISDS Administrative Console > Application Interface Modules > BFS Admin > [select site] > File > Select > Servers tab > File > New

Quick Path without RCS: ISDS Administrative Console > Application Interface Modules > BFS Admin > Servers tab > File > New

Follow these instructions to add a BFS carousel for the donwload server.

1. From the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. One of the following occurs:
   - **For systems using RCS**, the BFS Admin Site window opens. Go to step 3.
   - **For systems not using RCS**, the BFS Administration window opens. Go to step 4.
3. Choose one of the following options:
   - If the download server provides images to a **specific site**, select that site and click **File > Select**.
   - If the download server provides images to the **entire network**, click **File > All Sites**.

   Result: The Site BFS Administration window opens.
4. Click the **Servers** tab. The list of BFS carousels opens.

5 Click **File > New**. The Authorize BFS Server window opens.
6 Complete the fields as described in BFS Carousel Settings for Download Server.
7 Click **Save**. The Site BFS Administration window updates to show your new carousel.
8 Add the carousel to your network map.

Activate a Download Server

Quick Path: ISDS Administration Console > ISDS tab > Network Element Provisioning tab > Download Server > [select server] > Enabled

Follow these instructions to activate a download server.

1 From the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **Download Server**. The Download Servers window opens and displays any current download servers in your network.
4 Select the download server you want to activate.
5 Click the **Enabled** box (so that a check displays).
6 Click **Save**.

Modify a Download Server

Quick Path: ISDS Administration Console > ISDS tab > Network Element Provisioning tab > Download Server > [select server]

Follow these instructions to modify a download server.

1 From the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **Network Element Provisioning** tab.
3 Click **Download Server**. The Download Servers window opens and displays any current download servers in your network.
4 Select the download server you want to modify.
5 Modify the fields as described in Download Server Settings.
6 Click **Save**.

Delete a Download Server

Quick Path: ISDS Administration Console > ISDS tab > Network Element Provisioning tab > Download Server > [select server > Delete

You Need to Know

Before You Begin

Follow these instructions to delete a download server.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **Download Server**. The Download Servers window opens and displays any current download servers in your network.
4. Select the download server you want to delete.
5. Click **Delete**. The list updates to remove the download server.
6. Remove the download server from your network map.

5

Content Element Configuration

Introduction

The following elements process content, such as audio/video programming and Web services:

- **GbE element** - Connects the ISDS to the Digital Content Manager (DCM). A GbE element is a logical concept (not a physical device) used to specify the DCM that receives encrypted content from the ISDS.
- **Digital Content Managers (DCMs)** - Used to stream multicast content.

In This Chapter

GbE Elements

The GbE transport network is a logical concept, not a physical device. Creating a GbE transport network allows you to specify and limit connectivity between the ISDS and DCMs. This is done by creating GbE transport networks with arbitrary numbers of connection “ports” and indicating the DCMs and sources that are connected to those networks.

Digital Content Manager (DCM)

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > DCM

The DCM is a device that provides enhanced MPEG processing capabilities for IP multicast content.

Note: As a pre-requisite for creating source definitions, you must build a multicast session/source on a DCM device. Refer to the documentation that you received with your DCM for more information.

DCM Settings

Use the following fields when you manage DCMs in the ISDS.

Field	Description
Name	Name of the DCM. Use a name for the device that is consistent with the naming scheme used on your network map.
Source IP	Output IP address of the DCM that is streaming the multicast content when that multicast content is not encrypted by the Netcrypt.
Enabled	Determines whether the DCM is active.

Add a DCM

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > DCM > New

Follow these instructions to add a DCM.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **DCM**. The ISDS DCM Parameters window opens.
4. Click **New**. A new line opens on the ISDS DCM Parameters window.
5. Enter information as described in DCM Settings.
6. Click **Save**. The ISDS saves the information you entered and updates the window to display the current list of DCMs.

Modify a DCM

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > DCM > [select DCM]

After a DCM has been saved in the ISDS, you can modify only the following parameters for that cluster:

- Source IP
- Enabled

Note: To change the Name parameter, you must delete the DCM and re-add it to the ISDS, using the new information.

Follow these instructions to modify a DCM.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **DCM**. The ISDS DCM Parameters window opens.
4. Click a check mark into the Select box adjacent to the row for the cluster you want to modify. The row becomes highlighted.

   Note: You can also click in the exact field you wish to modify. The row for that cluster becomes highlighted and a check mark is inserted in the Select box for that cluster.
5. Change information for **Source IP** and **Enabled** as described in DCM Settings.
6. Do you need to modify another DCM?
   - If **yes**, repeats this procedure from step 3.
   - If **no**, go to step 7.
7. Click **Save**. The ISDS DCM Parameters window updates to include the new information for the DCM. set-tops receive updates within a few minutes to an hour, depending on the size of your system. Rebooting a set-top causes it to apply updates immediately.
8. Change your network map to reflect these changes.
9. Click **Cancel** to exit the ISDS DCM Parameters window.

Delete a DCM

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > DCM > [select DCM] > Delete

You might need to delete a DCM because you are no longer using it or because you need to redefine the headend or ID.

Follow these instructions to delete a DCM.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Network Element Provisioning** tab.
3. Click **DCM**. The ISDS DCM Parameters window opens.
4. Click a check mark into the Select box adjacent to the row for the cluster you want to delete. The row becomes highlighted.
5. Click **Delete**. A confirmation message opens.

6 Click **OK**. The message closes. The system removes the DCM information from the ISDS database and from the ISDS DCM Parameters window.

7 Delete the DCM from your network map.

8 Do you need to delete another DCM?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **Cancel** to close the ISDS DCM Parameters window.

6

Broadcast File System (BFS) Host

Introduction

After you set up your network logical elements, you need to set up a BFS host. The BFS host is the primary interface (means of communication) between the Application Server and the set-tops that are connected to the network.

This section describes how to configure the BFS host.

In This Chapter

Adding an ISDS BFS Host

Quick Path: ISDS Administrative Console > Application Interface Modules tab > BFS Admin > File > New

Follow these instructions to add a BFS host to the ISDS.

1. From the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Administration window opens.
3. Click **File > New**. The Set Up BFS Host window opens.
4. Enter **dncsatm** in the **Host Name** field.
5. Click **Save** and close the Set Up BFS Host window and the BFS Administration window.

BFS IP Sources

Quick Path: ISDS Administrative Console > Application Interface Modules tab > BFS Admin > IP Sources tab

The first step in setting up a clear, secure, or PPV service is to add information to the ISDS database about the original content source. After the source has been added to the ISDS, 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.

BFS IP Source Settings

Use the following fields when you manage BFS IP sources in the ISDS.

Field	Description
Source Name	Name of the BFS IP source.
Source ID	ID of the BFS IP source. ■ You can use up to eight numerical characters. ■ Be sure to use an ID number that is consistent with the numbering scheme used on your network map. **Important:** You will not be able to modify this field later.
Source Type	Type of information this BFS IP source transmits. ■ Select **BFS** unless this source carries Bootloader information.
Transport Type	Describes the type of transport mechanism for the source. ■ Select the **Multicast** option for the ISDS source.
Data Rate	The maximum data rate (in Mbps) the ISDS will allocate for this source. Use the following guidelines for your sources: ■ **BFS sources:** Type **3** (Mbps) ■ **OOB, MMM OOB, or IPG OOB:** Type **0.01** (Mbps) ■ **For most other sources:** Type **1** (Mbps)

Block Size	The block size of the data the source transmits. Type one of the following values: ■ For Bootloader, type **1304** ■ For all others, type **1300**
Indication Interval	Determines how often Download Indication messages are transmitted. ■ Type **100** for the Indication Interval.
Multicast IP Address	A unique multicast IP address for this BFS IP source from the SSM range (232.0.0.0 - 232.255.255.255), unless this source carries Bootloader, which must use an IP address **not in** the SSM range. This IP address must conform to your network map and must be unique for each BFS IP source.
Source	Determines if the source is active.
Hosts	Determines which hosts will have access to the source.

Building a BFS IP Source

Quick Path: ISDS Administrative Console > Application Interface Modules tab > BFS Admin > IP Sources tab > Source > Set Up BFS Source window

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

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Admin**. The BFS Administration window opens.
3. Click the **IP Sources** tab.

   Note: If the sources do not build automatically, close and re-open the window.
4. Double-click a source. The Set Up BFS Source window opens.
5. Enter information as described in BFS IP Source Settings.
6. Click **Save**. The Set Up BFS Source window closes.
7. Do you need to build another source?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File > Close** to close the BFS Administration window.
8. Are you setting up an RCS for your network?
   - If **yes**, go to ***Add a Remote Site to an RCS*** (on page 253).
   - If **no**, go to ***BFS Services*** (on page 69).

BFS Services

After you build your BFS IP sources and save the configuration, you need to confirm that the BFS client built the SAM services for those IP sources.

Confirming that the BFS Client Built a SAM Service

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **BFS Client**. The Broadcast File Server window opens.
3. Does the sam cabinet exist?
   - If **yes**, close the Broadcast File Server and go to ***Bouncing the bfsServer Process*** (on page 69).
   - If **no**, go to step 4.
4. On the Broadcast File Server window, click **File > New Server**. The Set Up Server window opens.
5. In the **Server Name** field, type **sam**.
6. In the **Mode** field, click **1-way**.
7. Highlight SAM in the Available Sources column and click **Add**. The SAM services moves to the Selected Sources column.
8. Click **Save**.
9. Click **File > Close** to close the Set Up Server window.
10. Click **File > Close** to close the Broadcast File Server window.

Bouncing the bfsServer Process

To populate the SAM folder, you need to bounce (stop and restart) the bfsServer process.

Complete the following steps to bounce the bfsServer process.

1. On the ISDS Administrative Console Status window, click **Control**. The ISDS Control window opens.
2. On the ISDS Control window, click to highlight the **bfsServer** process.
3. Click **Process > Stop Process**. In a few minutes, the indicator for the bfsServer process changes from green to red.

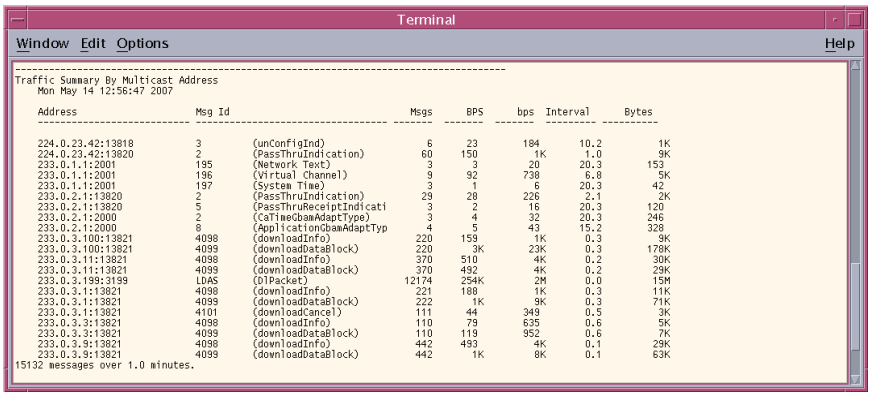
   Important: Do not go to the next step until the indicator has changed to red.
4. Click to highlight the **bfsServer** process again.
5. Click **Process > Start Process**. In a few minutes, the indicator for the bfsServer process changes from red to green.

6 Confirm that the system is transmitting BFS transactions. See ***Confirming That the System Transmits BFS Transactions*** (on page 70) for more information.

Confirming That the System Transmits BFS Transactions

1 Open an xterm window on the ISDS server.

2 Type **/dvs/dncs/etc/isdsDumper.pl** and press **Enter**. The system should display output similar to the following example:



```
Terminal
Window  Edit  Options                                                                    Help
-----------------------------------------------------------------------------------------------
Traffic Summary By Multicast Address
    Mon May 14 12:56:47 2007

    Address                     Msg Id                                  Msgs     BPS      bps  Interval     Bytes
    ------------------------- ---------------------------------------- -------  -------  -------  -------- ----------

    224.0.23.42:13818           3         (unConfigInd)                     6      23      184      10.2         1K
    224.0.23.42:13820           2         (PassThruIndication)             60     150       1K       1.0        9K
    233.0.1.1:2001              195       (Network Text)                    3       3       20      20.3       153
    233.0.1.1:2001              196       (Virtual Channel)                 9      92      738       6.8        5K
    233.0.1.1:2001              197       (System Time)                     3       1        6      20.3        42
    233.0.2.1:13820             2         (PassThruIndication)             29      28      226       2.1        2K
    233.0.2.1:13820             5         (PassThruReceiptIndicati          3       2       16      20.3       120
    233.0.2.1:2000              2         (CaTimeQbamAdaptType)             3       4       32      20.3       246
    233.0.2.1:2000              8         (ApplicationQbamAdaptTyp          4       5       43      15.2       328
    233.0.3.100:13821           4098      (downloadInfo)                  220     159       1K       0.3        9K
    233.0.3.100:13821           4099      (downloadDataBlock)             220      3K      23K       0.3      178K
    233.0.3.11:13821            4098      (downloadInfo)                  370     510       4K       0.2       30K
    233.0.3.11:13821            4099      (downloadDataBlock)             370     492       4K       0.2       29K
    233.0.3.199:3199            LDAS      (DTPacket)                    12174     254K      2M       0.0       15M
    233.0.3.1:13821             4098      (downloadInfo)                  221     188       1K       0.3       11K
    233.0.3.1:13821             4099      (downloadDataBlock)             222      1K       9K       0.3       71K
    233.0.3.1:13821             4101      (downloadCancel)                111      44      349       0.5        3K
    233.0.3.3:13821             4098      (downloadInfo)                  110      79      635       0.6        5K
    233.0.3.3:13821             4099      (downloadDataBlock)             110     119      952       0.6        7K
    233.0.3.9:13821             4098      (downloadInfo)                  442     493       4K       0.1       29K
    233.0.3.9:13821             4099      (downloadDataBlock)             442      1K       8K       0.1       63K
15132 messages over 1.0 minutes.
```

3 If the system does not display a similar output, contact Cisco Services.

Adding the ClusterID Field to the Database

Until the ISDS user interface is modified to support the cluster ID when configuring set-tops, you need to manually add this record to the database.

Complete the following steps to add the clusterID field to the hct_profile table in the database.

Follow these instructions to add the cluster ID field to the ISDS database.

1 Open an xterm window on the ISDS server.

2 Type **dbaccess dncsdb -** and press **Enter**. The system opens the database.

3 Type the following and press **Enter**:

update hct_profile set hct_qpsk_mod_id='< clusterID value >' where hct_mac_address='<DHCT MAC address >'

4 Repeat step 3 for as many set-top records that apply.

5 Press the **Ctrl** and **C** (**Ctrl + C**) keys simultaneously to close the database.

7

CSM Services

Introduction

Channel Service Manager (CSM) services associate a specific service with an application that defines the medium to be used for that service.

For example, to access a standard audio/video program service, a set-top must download the **WatchTV** application. The WatchTV application contains the operation attributes that tell the set-top how to tune to and display a standard audio/video program service so that subscribers can hear and view the service.

This section describes how to create, test, and delete CSM services.

In This Chapter

CSM Services Settings

Use the following fields when you manage CSM services.

Field	Description
Service Name	The name you want to use to identify this service. ■ You can use up to 20 alphanumeric characters. **Example: Discovery Kids**.
Short Description	A brief description of this service. ■ This description will appear on the IPG and on the channel banner on the subscriber's television screen. ■ You can use up to 5 alphanumeric characters. **Example:** For the Discovery Kids service, you might type **DSCK**.
Long Description	A detailed description of this service. ■ You can use up to 32 alphanumeric characters. ■ This information is for your benefit only. Subscribers will not see this information.
Application URL	Select the path on the BFS where the software file resides.
Logo	The number for the logo associated with this service.
Parameter	Allows you to define the type of service. ■ **VOD service:** Select number and type **0** ■ **Clear or secure service:** Select number and type the **service source ID** that you assigned when you added the service source to the ISDS

Add CSM Services

Quick Path: ISDS Administrative Console > Application Interface Modules tab > CSM Service > File > New

Creating a CSM service achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's set-top.
- Communicates the operation attributes to the set-tops in your network.
- If the service is to be included as part of a package, creating the service associates it with the specified package.

Note: This procedure does not apply to PPV services.

You Need to Know

Before You Begin

Follow these instructions to add a CSM service to the ISDS.

1. From the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **CSM Service**. The CSM Service List window opens.
3. Click **File > New**. The Set Up CSM Service window opens.
4. Enter information as described in CSM Services Settings.
5. Click **Save**.
6. Repeat this procedure from step 3 to create additional CSM services.
7. Close the CSM Service List window when you are finished.

Test a Service

Note: Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the ISDS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops 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 set-top and a television.

Is the new service packaged?

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

Authorize a Set-Top or CableCARD Module for a Service

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

You Need to Know

Before You Begin

Time To Complete

Performance Impact

Follow these instructions to authorize a set-top for a service.

Complete these steps to authorize a set-top for a service.

1. Make sure the test set-top is connected to a television, and to an Ethernet feed into your network.
2. Make sure both the set-top and television are plugged into a power source.
3. On the ISDS Administrative Console, click the **ISDS** 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 set-top you are testing.

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

7 Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.

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 set-top 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 set-top must be authorized for that package as well. This should have been done when the set-top 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:

- **DMS Enable** - Enable this option to allow the set-top to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Fast Refresh Enable** - This option is used to send EMMs to set-tops during staging. For more information, refer to the Explorer Digital Home Communications Terminal Staging Guide.
- **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 set-top.

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

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. Go to ***Verify a Successful Service Setup*** (on page 75).

Verify a Successful Service Setup

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

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Follow these instructions to verify a successful service setup.

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

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
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 Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. 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 Cisco Services.

Locating a Set-Top MAC Address

To locate the MAC address of a set-top, do one of the following:

- Display the set-top diagnostic screens.
- Look on the back of the set-top for a label with the MAC address recorded on it.

Modify CSM Services

Quick Path: ISDS Administrative Console > Application Interface Modules tab > CSM Service > [select service] > File > Open

Follow these instructions to modify a CSM service.

1. From the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **CSM Service**. The CSM Service List window opens.
3. Select the service you want to modify.
4. Click **File > Open**. The Set Up CSM Service window opens.
5. Edit the service information as described in CSM Services Settings.
6. Click **Save**.
7. Repeat this procedure from step 3 to modify additional CSM services.
8. Close the CSM Service List window when you are finished.

Remove Services from a Channel Map

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Channel Maps > [Select Service] > File > Delete

When a service is no longer needed for a particular channel map, delete the service from the channel map.

You Need to Know

Performance Impact

Follow these instructions to remove a service from a channel map.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select that service in the channel slot column.
6. Click **Remove**. The service is now listed under Available Services and no longer displays in the Channel Slot column.
7. If you are removing this service from your system, select one of the following:
   - If you are using CSM services, go to ***Delete CSM Services*** (on page 79).
   - If you are using SAM services, go to ***Delete SAM Services*** (on page 88).

Delete CSM Services

Quick Path: ISDS Administrative Console > Application Interface Modules tab > CSM Service > [select service] > File > Delete

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Follow these instructions to delete a CSM service.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **CSM Service**. The CSM Service List window opens.
3. Select the service you want to delete.
4. Click **File > Delete**. A confirmation window opens.
5. Click **Yes** to delete the service. The service is removed from the system and no longer displays in the Available Services list for any channel maps.
6. Clean up sources, sessions, and segments associated with the deleted service as needed. Any sources, sessions, and segments associated with a deleted service remain active unless you manually delete the source, session, or segment. In addition, any package that contains a segment associated with the deleted service continues to contain that segment unless you manually delete the segment from the package.

8

SAM Services

Introduction

Service Application Manager (SAM) services associate a specific service with an application that defines the medium to be used for that service.

For example, to access a standard audio/video program service, a set-top must download the **WatchTV** application. The WatchTV application contains the operation attributes that tell the set-top how to tune to and display a standard audio/video program service so that subscribers can hear and view the service.

This section describes how to create, test, and delete SAM services.

In This Chapter

SAM Service Settings

Use the following fields when you manage SAM services.

Field	Description
Service Name	The name you want to use to identify this service. ■ You can use up to 20 alphanumeric characters. **Example: Discovery Kids**.
Short Description	A brief description of this service. ■ This description will appear on the IPG and on the channel banner on the subscriber's television screen. ■ You can use up to 5 alphanumeric characters. **Example:** For the Discovery Kids service, you might type **DSCK**.
Long Description	A detailed description of this service. ■ You can use up to 32 alphanumeric characters. ■ This information is for your benefit only. Subscribers will not see this information.
Application URL	Path on the BFS where the software file resides.
Logo	The number for the logo associated with this service.
Parameter	Allows you to define the type of service. ■ **VOD service:** Type **0** ■ **Clear or secure service:** Type the **service source ID** that you assigned when you added the service source to the ISDS

Create SAM Services

Quick Path: ISDS Administrative Console > Application Interface Modules tab > SAM Service > File > New

Creating a SAM service achieves the following objectives:

- Associates the service with the software application that contains the attributes that define how the service operates when it gets to a subscriber's set-top.
- Communicates the operation attributes to the set-tops in your network.
- If the service is to be included as part of a package, creating the service associates it with the specified package.

Notes:

- If you want to adjust how often the SAM communicates service operation attributes to the set-tops in your network, go to ***Schedule Service Updates*** (on page 390).
- This procedure does not apply to PPV services.

You Need to Know

Before You Begin

Follow these instructions to create a SAM service.

1. From the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens.
3. Click **File > New**. The Set Up SAM Service window opens.
4. Enter information as described in SAM Service Settings.
5. Click **Save**.

   Note: Write down the Service ID that is automatically generated. You will need this number later.
6. Repeat this procedure from step 3 to create additional SAM services.
7. Close the SAM Service List window when you are finished.

Test a Service

Note: Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the ISDS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops 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 set-top and a television.

Is the new service packaged?

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

Authorize a Set-Top or CableCARD Module for a Service

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

You Need to Know

Before You Begin

Time To Complete

Performance Impact

Follow these instructions to authorize a set-top for a service.

Complete these steps to authorize a set-top for a service.

1. Make sure the test set-top is connected to a television, and to an Ethernet feed into your network.
2. Make sure both the set-top and television are plugged into a power source.
3. On the ISDS Administrative Console, click the **ISDS** 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 set-top you are testing.

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

7 Click **Continue**. The Set Up DHCT window opens with the Communications tab in the forefront.

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 set-top 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 set-top must be authorized for that package as well. This should have been done when the set-top 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:

- **DMS Enable** - Enable this option to allow the set-top to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **Fast Refresh Enable** - This option is used to send EMMs to set-tops during staging. For more information, refer to the Explorer Digital Home Communications Terminal Staging Guide.
- **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 set-top.

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

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. Go to ***Verify a Successful Service Setup*** (on page 75).

Verify a Successful Service Setup

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

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Follow these instructions to verify a successful service setup.

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

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
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 Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. 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 Cisco Services.

Locating a Set-Top MAC Address

To locate the MAC address of a set-top, do one of the following:

- Display the set-top diagnostic screens.
- Look on the back of the set-top for a label with the MAC address recorded on it.

Remove Services from a Channel Map

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Channel Maps > [Select Service] > File > Delete

When a service is no longer needed for a particular channel map, delete the service from the channel map.

You Need to Know

Performance Impact

Follow these instructions to remove a service from a channel map.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select that service in the channel slot column.
6. Click **Remove**. The service is now listed under Available Services and no longer displays in the Channel Slot column.
7. If you are removing this service from your system, select one of the following:
   - If you are using CSM services, go to ***Delete CSM Services*** (on page 79).
   - If you are using SAM services, go to ***Delete SAM Services*** (on page 88).

Delete SAM Services

Quick Path: ISDS 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.

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Follow these instructions to delete a service from a SAM.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **SAM Service**. The SAM Service List window opens.
3. Select the service you want to delete.
4. Click **File > Delete**. A confirmation window opens.
5. Click **Yes** to delete the service from the SAM. The service is removed from the system and no longer displays in the Available Services list for any channel maps.
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.

9

Video Sources and Definitions

Introduction

The first step in setting up a clear, secure, or PPV service is to add information to the ISDS database about the original content source. After the source has been added to the ISDS, 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.

In This Chapter

Set Up IP Video Sources

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

This procedure applies to clear, secure, and PPV services. It does not apply to VOD services.

1. From the ISDS Administrative Console, click the **System Provisioning** tab.
2. Click **Source**. The Source List window opens.
3. Click **File > New**. The Set Up Source window opens.
4. Type the **Source Name**.

   Note: The Source Name is typically the Short Description.
5. Type the **Source ID**.

   Important: The Source ID must be greater than 200. IDs 200 or less are reserved for BFS sources.
6. Click **Save**.
7. Repeat this procedure from step 3 for all channels.
8. Go to ***Complete the Source Definition*** (on page 91).

Complete the Source Definition

After you build an IP source and set up the video sources in the ISDS database for a clear or secure service, define the parameters for the source so that the system knows how to process the service content.

Source Definition Settings

Use the following fields when you complete the source definition.

Field	Description
	Provision IP Multicast Content Source
Source Name	Name of this source.
MPEG Program Number	Program number of the MPEG transport stream that feeds this source.
Effective Time	The month, day, year and hour, minute, second 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. For example, you would type July 4, 2008, as **07/04/2008**. ■ You must type two digits for each time value. Enter the time in 24-hour format For example, you would type eight o'clock AM as **08:00:00**. You would type eight o'clock PM as **20:00:00**. **Example:** If you want the source to be effective starting July 4, 2008 at eight o'clock in the morning, type: **07/04/2008 08:00:00**
Description	Description of this source.
	Source Device
Source Device	Device associated with this source.
Name, Port, IP	Name, port and IP address of the Netcrypt associated with this source. ■ This field only displays if you select **Netcrypt** as the Source Device.
DCM IP	IP address of the DCM associated with this source. ■ This field only displays if you select **DCM** as the Source Device.
IP	IP address of the device associated with this source. ■ This field only displays if you select **Other** as the Source device.
	Stream Data
Multicast Destination IP	Multicast stream that receives the output of this source.

Video Encoding	Video encoding method for this source: ■ MPEG-2 ■ H.264 ■ VC-1 ■ Other
Data Rate	Maximum data rate for the source.
Encapsulation	Encapsulation method for this source: ■ IP/UDP/MPEG-TS ■ IP.UDP/RTP/MPEG-TS ■ Undefined
Audio Encoding	Audio encoding method for this source: ■ AC-3 ■ MPEG-2, 2-Channel ■ MPEG-1, Layer 1 ■ MPEG-1, Layer 2 ■ MPEG-1, Layer 3 ■ AC-3 Plus ■ AAC ■ AAC-HE ■ Unknown
Frame Rate	Video frame rate for this source: ■ FR_Undefined ■ FR_24E ■ FR_24 ■ FR_25 ■ FR_30E ■ FR_30 ■ FR_50 ■ FR_60E ■ FR_60
UDP Port	UDP port associated with this source. ■ This field only displays if you select either IP/UDP/MPEG-TS or Undefined as the Encapsulation type.

RTP Port	RTP port associated with this source. ■ This field only displays if you select IP/UDP/RTP/MPEG-TS as the Encapsulation type.
RTCP Port	RTCP port associated with this source. ■ This field only displays if you select IP/UDP/RTP/MPEG-TS as the Encapsulation type.
Resolution	Resolution of the video portion of the source.
Hub	Hub associated with this source.

Completing the Source Definition

1. From the ISDS Administrative Console, click the **System Provisioning** tab.
2. Click **IP Source Definitions**. The IP Source Definitions window opens.
3. Click **New**. The ISDS Multicast Source Parameters window opens.
4. Select the previously created source from the **Source Name** drop-down list.
5. Enter information as described in Source Definition Settings.
6. Click **Save**.
7. Click **File > Quit**.
8. Repeat the procedures in ***Set Up IP Video Sources*** (on page 90) and this procedure for any other sources you want to configure.

Content Sources and Sessions

This section discusses defining sources and setting up sessions.

A source is the actual program or data that is made available to the set-top as a service to the subscriber. Sources can include any of the following:

- MPEG digital broadcast services that are non-secure, non-encrypted, audio/video programs
- Internet connections from an Internet service provider (ISP)
- Digital PPVs that are secure, encrypted, digital MPEG programs
- Digital music services

Sessions are the logical elements that define and allocate the resources that the network uses to deliver source content.

Source and Session Settings

Use this section to learn about the settings required for adding or editing sources and sessions in the ISDS.

Add and Edit Source Settings

Use the following fields when you add sources to the ISDS.

Field	Description
Source Name	The name of the source you are adding. 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.

Source ID	The number you will use to identify this source. Typically, the source ID is 1000 plus the number of the channel offering the service. For example, the source ID for a service appearing on channel 2 would be **1002**. You can use up to 5 numeric characters. **Notes:** ■ 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. ■ Remember the content source ID. You will need it as you continue to set up the service. ■ You cannot edit the Source ID field. To change the source ID of an existing source, you must delete the source and add it again.
Enable EAS Channel Suppression	Select this option to enable EAS channel suppression on this source. For more information on this options, see Suppress EAS Information on Digital Channels. **WARNING:** **Use this feature at your own risk. It is imperative that service providers use this feature carefully so as not to suppress EAS messages on services that do not already provide EAS information. We do not take responsibility for the incorrect use of this feature.**

Digital Source and Session Settings

Use the following fields when you manage digital sources and sessions in the ISDS.

Field	Description
Source Definition Type	Defines the type of source definition. Select **Digital** from the drop-down list. Updated fields display based on your selection.
Source Name	Name of the source you are adding the session to.
Date/Time	Allows you to define when subscribers can start viewing content from this source. If left unselected, subscribers can start viewing content immediately.

Effective Date	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. **Example:** For July 4, 2010, type **07042010**. The system inputs the slashes for you and displays **07/04/2010**. This option is only activated if you select the **Select effective date and time** option.
Effective Time	The hour, minute, second, and half-day (AM or PM) you want subscribers to be able to start seeing content from this source. You must type two digits for each value. **Example:** For eight o'clock, type **080000**. The system inputs the colons for you and displays **08:00:00**. This option is only activated if you select the **Select effective date and time** option.
Hex Session	Select this option to display the session ID in a hexadecimal format.
Session ID	**Site/ISSDS ID** - The site ID associated with this source.
	Hub ID - The hub associated with this source.
	PCG ID - The PCG associated with this source.
	Rsv - Reserved. Leave blank.
	MPEG PN - The MPEG stream ID for this source.
	Source ID - The source ID you used when you added the content source.
High Definition	Select this option if the source is a high-definition source.
PCG Device	Select the PCG device associated with this source from the drop-down list.
External Access Criteria 1	If the PCG supports external access criteria, enter the first third-party SCS access criteria parameter here.
External Access Criteria 2	If the PCG supports external access criteria, enter the second third-party SCS access criteria parameter here.
Scrambling Mode	Select the scrambling mode from the drop-down list.

Third-Party Content Source Settings

Use the following fields when you manage a third-party content source in the ISDS.

Field	Description
Distribution	Defines how the source is distributed: ■ **All Hubs** - Distributes the source to all hubs. ■ **Single Hub** - Distributes the source to the specific hub defined in Hub Name.

Hub Name	The hub name that receives content. This option is only activated if you selected the **Single Hub** option in the Distribution field.
MPEG Program Number	The MPEG program being fed into the transport stream. This number must match the program number of the MPEG source as defined by your content provider.
Channel Center Frequency	The channel frequency of the channel you will use to send data from this modulator to the hubs on your system. You can enter a value in 6 MHz increments from 91 to 867. Click for a table of recommended QAM frequencies.
Modulation Type	The type of modulation this modulator uses. **Example:** If this modulator uses ITU J.83 Annex B modulation, select **ITU J.83 Annex B (6 MHz)**.
Modulation	The modulation method this modulator uses. **Example:** If this modulator uses 256 QAM, select **256-QAM**.
High Definition	Select this option if the source contains high-definition content.
PCG Session ID	Select the appropriate PCG session ID for this source, if any.

Service Package Settings

Use the following fields when you manage a service package in the ISDS.

Field	Description
Package Name	The name that identifies 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. Default packages (those used for InstaStaging) are the only exception. **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 Cisco Services. ■ Do not select the **PPV**, **IPPV**, or **Allow Event Extension** options. The ISDS does not support these options at this time.
Duration	Allows subscribers to have unlimited access to the package. 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 Cisco Services.
Pay Per View	Not supported at this time.

Allow Event Extension	Not supported at this time.
Impulse Pay Per View	Not supported at this time.

Service Registration Settings

Use the following fields when you register a service in the ISDS.

Field	Description
Service Name	The name you want to use to identify this service. You can use up to 20 alphanumeric characters.
Short Description	A brief description of this service. You can use up to 5 alphanumeric characters. This description will appear on the IPG and on the channel banner on the subscriber's television screen.
Long Description	A detailed description of this service. You can use up to 32 alphanumeric characters. This information is for your benefit only. Subscribers will not see this information.
Logo	The number for the logo associated with this service, if required.
Parameter	Define the type of service: ■ For a VOD service, type **0**. ■ For a clear or secure service, type the **service source ID** that you assigned when you added the service source.

Add a Content Source

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

The first step in setting up a clear, secure, or PPV service is to add information to the ISDS database about the original content source. After the source has been added to the ISDS, 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.

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Complete these steps to add a source for a service.

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

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click **Add**. The Set Up Source window opens.
5. Complete the fields on the screen as described in Add and Edit Source Settings.
6. Click **Save**. The system saves the source information in the ISDS database and closes the Set Up Source window. The Source List window updates to include the new source.
7. You are ready to define the source that you just added. Go to ***Define a Content Source*** (on page 99).

Define a Content Source

Note: These procedures do not apply to VOD services.

After you add a content source to the ISDS database for a clear, secure, or PPV service, define parameters for the source so that the system knows how to process the service content.

After you add a content source to the ISDS for a clear, secure, or PPV service, define parameters for that source. Then build a session from the source definition. You do not need to define a source and session for a VOD service.

You Need to Know

Before You Begin

Time To Complete

Performance Impact

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.

4 Select the service source you need to define and click **File > Source Definition**. The Source Definition List window opens for the source you selected.

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

6 Complete the field information for **Hex Session**, **Session ID**, and **High Definition** as described in Digital Source and Session Settings.

7 Click **Next**. The Session Setup window opens.

8 Select the **PCG Device** from the drop-down list.

9 Click **Next**. The Wrap-Up window opens.

10 Enter the values for the **External Access Criteria** and the **Scrambling Mode** as described in Digital Source and Session Settings.

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

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

13 Do you need to define another digital source for this service?

- If **yes**, repeat this procedure.
- If **no**, click **File > Close** to close the Source Definition List window and return to the Source List window.

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.

14 Do you want to offer the clear service to only specifically authorized subscribers?

- If **yes**, go to the next step.
- If **no**, your next step is to register the clear service. Go to ***Register a Service*** (see "***Registering a Service***" on page 102).

15 Your next step is to add the clear service to a package. Does a package already exist to which you want to add this service?

- If **yes**, go to ***Determine and Convert a Package EID*** (on page 103).
- If **no**, go to ***Add a Service Package*** (on page 101).

Define a Third-Party Content Source

This procedure describes how to configure a system to carry clear (unencrypted) MPEG content that delivers unmodified Program and System Information Protocol (PSIP) in a bandwidth-efficient manner configured on the ISDS as a third-party source.

You Need to Know

Before You Begin

Time to Complete

Performance Impact

1. On the DNCS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Select the source you need to define.
5. Click **Source Definition**. The Source Definition List window opens for the source you selected.
6. Click **File > New non-SA Digital**. The Set Up Non-SA Digital Source Definition window opens.
7. Complete the fields on the screen as described in Third-Party Content Source Settings.
8. Click **Save**. The system closes the Set Up Non-SA Digital Source Definition window and the Source Definition List window updates to include the new third-party source.
9. Repeat this procedure for each third-party source you need to add.
10. From the Source Definition List window, select **Exit**.

Add a Service Package

Notes:

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

Important: If you are using our RCS solution, create a package for each site that will receive the service this package provides.

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 set-top to receive the package. When you authorize the set-top to receive the package, you enable the set-top to decrypt the secure service.

VOD services are similar to secure services in that you must add a service package for each VOD service before a subscriber can access the service. Then, you authorize the subscriber's set-top to receive the package, etc., just as you would for a 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 set-tops that cannot descramble or decrypt services. Some examples of clear services that you might want to offer on a subscription basis include the following:

- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and Web browsing

You Need to Know

Time to Complete

Performance Impact

1. On the ISDS Administrative Console, click the **ISDS** 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 > New**. The Set Up Package window opens.
5. Complete the fields on the screen as described in Service Package Settings.
6. Click **Save**. The system saves the package information in the ISDS database and closes the Set Up Package window. The Package List window updates to include the new package.
7. Are you using our RCS solution?
   - If **yes**, go to step 8.
   - If **no**, go to step 9.
8. Are there other RCS sites that will use the third-party application that this package provides?
   - If **yes**, repeat this procedure from step 4 to add a package to another site.
   - If **no**, go to step 9.
9. Do you need to add a VOD or clear service to this package?
   - If **yes**, go to ***Determine and Convert a Package EID*** (on page 103).
   - If **no**, go to step 10.
10. Click **File > Close** to close the Package List window.
11. Go to ***Register a Service*** (see "***Registering a Service***" on page 102).

Registering a Service

Complete these steps to register a service.

Note: This procedure does not apply to PPV services.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **CSM Service**. The CSM Service List window opens.
3. Click **File > New**. The Add CSM Service window opens.
4. Complete the fields on the screen as described in Service Registration Settings.
5. Click **Save**. The system saves the service information in the ISDS database, registers the service with the BFS, and closes the Add CSM Service window. The CSM Service List window updates to include the new service with its Service ID.
6. Do you need to register another service with the CSM?
   - If **yes**, repeat this procedure.
   - If **no**, click **File > Close** to close the CSM Service List window and return to the ISDS Administrative Console.
7. Your next step is to add the service to a channel map. Does a channel map already exist to which you want to add this service?
   - If **yes**, go to ***Add a Service to a Channel Map*** (on page 110).
   - If **no**, go to ***Add a Channel Map*** (on page 109).

Determine and Convert a Package EID

Important:

- This procedure applies to VOD services. It also applies to clear services that you want to package. It does not apply to secure, PPV, or unpackaged clear services.
- Because clear services are not encrypted, packaging a clear service does not protect it from being accessed (stolen) by unauthorized users.

When you add a service package to your system, the ISDS automatically assigns an Entitlement Identifier (EID) to the package. To package a VOD or clear service, you must first determine the package EID, and then convert it from a hexadecimal value to a decimal value. Then, you use the decimal value when you register the service. Among other things, registering the service associates it with the specified package.

By making this association, set-tops are able to use data from the CSM Service List to link the service with a particular package. If you do not make this association, all set-tops will receive the service — even those set-tops that are not authorized to receive it.

You must add a VOD service to a package to make it available to your authorized subscribers. Each VOD service must have its own package.

You can also add a clear service to a package to make it available only to specifically authorized subscribers. You may want to do this if you have set-tops that cannot descramble (or decrypt) services. Some examples of clear services that you might want to offer on a package basis include the following:

- Clear digital video
- Clear digital audio
- Other channel-based services, such as email and web browsing

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Determining a Package EID

Important: This procedure applies to VOD services and clear services that you want to package. It does not apply to secure, PPV, or unpackaged clear services.

1. On the ISDS Administrative Console, click the **ISDS** 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. Select the package to which you want to add the service.
5. Click **Edit**. The Edit Package window opens for the package you selected.
6. Record the number shown in the EID field.
7. Click **Cancel** to close the Edit Package window and return to the Package List window.
8. Click **Exit** to close the Package List window and return to the Administrative Console.
9. Your next step is to convert the EID from hexadecimal value to a decimal value. Go to ***Converting a Package EID to Decimal*** (on page 104).

Converting a Package EID to Decimal

Important: This procedure applies to VOD services and clear services that you want to package. It does not apply to secure, PPV, or unpackaged clear services.

The CSM Service List recognizes only decimal formats. However, the Set Up Package window displays the package EID in hexadecimal format. After you determine the package EID, for the CSM Service List to be able to link a VOD or a clear service with a particular package, you must convert the EID to decimal format.

Hexadecimal values derive from the base-16 number system, which consists of 16 unique symbols: the numbers 0 to 9, followed by the letters a to f. Once you reach the letter f, you continue counting with 1a, 1b, 1c, and so on until you reach 1f. Then, you continue with 2a, 2b, 2c, and so on.

In contrast, decimal values derive from the base-10 number system, which consists only of the numbers 0 to 9. Once you reach the number 9, you continue counting with 10, 11, 12, and so on until you reach 19. Then, you continue with 20, 21, 22, and so on.

Each hexadecimal number corresponds to a decimal number. For example, in the following tables, the hexadecimal (HEX) 53 corresponds with the decimal (DEC) 83. You would use the number 83 to associate the service with the package when you register the service.

Use the following procedure to convert a package EID to a decimal value.

1. After you determine the ISDS package EID, use the following table to locate the EID in the **HEX** column.
2. Then, locate the corresponding decimal value in the **DEC** column.

   For example, if the package EID is **1f**, the decimal value is **31**.

HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC
0	0	20	32	40	64	60	96	80	128	a0	160	c0	192	e0	224
1	1	21	33	41	65	61	97	81	129	a1	161	c1	193	e1	225
2	2	22	34	42	66	62	98	82	130	a2	162	c2	194	e2	226
3	3	23	35	43	67	63	99	83	131	a3	163	c3	195	e3	227
4	4	24	36	44	68	64	100	84	132	a4	164	c4	196	e4	228
5	5	25	37	45	69	65	101	85	133	a5	165	c5	197	e5	229
6	6	26	38	46	70	66	102	86	134	a6	166	c6	198	e6	230
7	7	27	39	47	71	67	103	87	135	a7	167	c7	199	e7	231
8	8	28	40	48	72	68	104	88	136	a8	168	c8	200	e8	232
9	9	29	41	49	73	69	105	89	137	a9	169	c9	201	e9	233
a	10	2a	42	4a	74	6a	106	8a	138	aa	170	ca	202	ea	234
b	11	2b	43	4b	75	6b	107	8b	139	ab	171	cb	203	eb	235
c	12	2c	44	4c	76	6c	108	8c	140	ac	172	cc	204	ec	236
d	13	2d	45	4d	77	6d	109	8d	141	ad	173	cd	205	ed	237
e	14	2e	46	4e	78	6e	110	8e	142	ae	174	ce	206	ee	238
f	15	2f	47	4f	79	6f	111	8f	143	af	175	cf	207	ef	239
10	16	30	48	50	80	70	112	90	144	b0	176	d0	208	f0	240
11	17	31	49	51	81	71	113	91	145	b1	177	d1	209	f1	241
12	18	32	50	52	82	72	114	92	146	b2	178	d2	210	f2	242
13	19	33	51	53	83	73	115	93	147	b3	179	d3	211	f3	243
14	20	34	52	54	84	74	116	94	148	b4	180	d4	212	f4	244
15	21	35	53	55	85	75	117	95	149	b5	181	d5	213	f5	245

HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC	HEX	DEC
16	22	36	54	56	86	76	118	96	150	b6	182	d6	214	f6	246
17	23	37	55	57	87	77	119	97	151	b7	183	d7	215	f7	247
18	24	38	56	58	88	78	120	98	152	b8	184	d8	216	f8	248
19	25	39	57	59	89	79	121	99	153	b9	185	d9	217	f9	249
1a	26	3a	58	5a	90	7a	122	9a	154	ba	186	da	218	fa	250
1b	27	3b	59	5b	91	7b	123	9b	155	bb	187	db	219	fb	251
1c	28	3c	60	5c	92	7c	124	9c	156	bc	188	dc	220	fc	252
1d	29	3d	61	5d	93	7d	125	9d	157	bd	189	dd	221	fd	253
1e	30	3e	62	5e	94	7e	126	9e	158	be	190	de	222	fe	254
1f	31	3f	63	5f	95	7f	127	9f	159	bf	191	df	223	ff	255

10

Channel Maps

Introduction

The set of channels that subscribers can tune in through their set-tops is called a "channel map." This section describes how to add channel maps and how to add and remove services from channel maps.

In This Chapter

Channel Map Settings

Use the following fields when you manage channel maps in the ISDS.

Field	Description
Name	Name of the channel map. You can use up to 20 alphanumeric characters.
VCT ID	Virtual channel table identifier. During set-top provisioning, each set-top is assigned a VCT ID. The set-top uses the VCT ID to retrieve its associated SI data among other sets of data that might be available on its hub.
Copy channel map from:	Copy an existing channel map. 1 Select the **Copy channel map from:** option. 2 Click the arrow to select the channel map you want to copy. 3 Click **Continue** to view and amend the channel setup for that channel map.
Channels	Assign services to channels. 1 Select a service in the Available Services column then click a Channel Slot. 2 Click **Add** to move that service to that Channel Slot.

Add a Channel Map

Quick Path: DNCS Administrative Console > Application Interface Modules tab > Channel Maps > File > New

You must add a service to a channel map so that your subscribers can access it by tuning to a particular channel.

You Need to Know

Time to Complete

Performance Impact

Follow these instructions to add a channel map.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click **File > New**. The Set Up Channel Map window opens.
4. Enter information as described in Channel Map Settings.
5. Click **Continue**. The Set Up Display Channel Map window opens.
6. Do you need to add a service to this channel map?
   - If **yes**, go to ***Add a Service to a Channel Map*** (on page 110).
   - If **no**, click **Save**. The system saves the channel map information in the database, closes the Set Up Display Channel Map window, and returns you to the Display Channel Map List window.
7. Do you need to add another channel map?
   - If **yes**, repeat this procedure from step 3.
   - If **no**, click **File > Close** to close the Display Channel Map List window and return to the ISDS Administrative Console.

Add a Service to a Channel Map

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Channel Maps > [Channel Map Name] > File > Open

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Important: If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they tune to the channel.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Click once on the row containing the channel map to which you want to add this service.

   Note: If you select the Default channel map, this service will be available to all hubs.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the Available Services field until you see the service you want to add, and then click to select that service.

   Important: If this is a PPV service, add only the PPV service to the channel map. If you add the Event Use Service to the channel map, you will have an encrypted service occupying a tunable channel. Instead of the PPV event barker, subscribers would see a blank screen when they to the channel.
6. Scroll through the **Channel Slot** field until you see the channel to which you want to assign the service, and then click to select that channel slot.
7. Click **Add**. The service name moves from the Available Services field to the Channel Slot field.
8. Do you need to add another service to this channel map?
   - If **yes**, repeat this procedure from step 5.
   - If **no**, click **Save**. The system saves the channel map information in the DNCS database, closes the Set Up Display Channel Map window, and returns to the Display Channel Map List window.
9. Do you need to add a service to another channel map?
   - If **yes**, repeat this procedure from step 3.

- If **no**, click **File > Close** to close the Display Channel Map List window and return to the DNCS Administrative Console.

10 Is this is a VOD service?

- If **yes**, complete any additional procedures required by the vendor of your VOD server.
- If **no**, go to step 11.

11 Your next step is to test the new service on a DHCT to verify that it has been set up successfully. Go to ***Test a Service*** (on page 84).

Remove Services from a Channel Map

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Channel Maps > [Select Service] > File > Delete

When a service is no longer needed for a particular channel map, delete the service from the channel map.

You Need to Know

Performance Impact

Follow these instructions to remove a service from a channel map.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Channel Maps**. The Display Channel Map List window opens.
3. Select the channel map containing the service you want to remove.
4. Click **File > Open**. The Set Up Display Channel Map window opens for the channel map you selected.
5. Scroll through the services under **Channel Slot** until you see the service you want to remove, and then select that service in the channel slot column.
6. Click **Remove**. The service is now listed under Available Services and no longer displays in the Channel Slot column.
7. If you are removing this service from your system, select one of the following:
   - If you are using CSM services, go to ***Delete CSM Services*** (on page 79).
   - If you are using SAM services, go to ***Delete SAM Services*** (on page 88).

Enhanced Channel Maps

The Enhanced Channel Maps feature frees you from the restriction of hub-based channel maps. This gives you greater flexibility in assigning channel maps. For example, this feature allows you to add a channel that is visible to all high-definition (HD) DHCTs but does not appear on standard-definition (SD) DHCTs.

Note: For additional information, refer to the *Enhanced Channel Maps User's Guide* (part number 4011413). To obtain this guide, refer to ***Printed Resources*** (on page 8).

Verify That Your System Is Enabled for Enhanced Channel Maps

The Enhanced Channel Maps feature remains inactive until installers enable a setting on the ISDS. After this setting is enabled, the Set Up Display Channel Map window allows you to associate channel maps with a Lineup Group Identifier (LUG ID).

1. On the ISDS Administrative Console, click **Application Interface Modules** tab.
2. Click **BFS Client**. The Broadcast File List window opens.

   Note: For multi-site systems (those with the RCS option enabled), the Please Select a Site window opens. From this window, click **All Sites** to open the Site All Sites Broadcast File List window.
3. Click the **sam** cabinet. The cabinet opens and displays its contents.
4. Is a folder named **lug** contained in the sam cabinet?
   - If **yes**, the Enhanced Channel Maps feature is enabled on your system.
   - If **no**, the Enhanced Channel Maps feature is not enabled. Contact Cisco Services for assistance.

Special Requirements for SSC DHCTs

When you create group definition rules for SSC DHCTs, create rules based only one of the following attributes:

- DHCT attributes
- CableCARD module attributes

Note: An SSC DHCT includes the functionality of the stand-alone DHCT, but adds the convenience of a factory-installed PowerKEY Multi-Stream CableCARD module (or M-Card). The M-Card module is mounted in the rear of the DHCT and is secured with a cover plate to deter tampering. A label provides the bar codes for the serial number and MAC address of the M-Card module is also provided on the rear panel of the DHCT.

Rules for SSC DHCTs

Group Definition rules should use DHCT attributes for the following conditions:

- Model number
- Version number
- Physical hub where the SSC DHCT resides
- OUI

Rules for CableCARD Modules

Group Definition rules should use CableCARD attributes for the following conditions:

- CableCARD MAC address
- PowerKEY package authorization
- Physical hub where the module resides

Set Up Enhanced Channel Maps

As part of setting up enhanced channel maps for your facility, you build a set of group definition rules. This page describes how to create an enhanced channel map and build a set of group definition rules.

You Need to Know

Before You Begin

Follow these instructions to set up an enhanced channel map:

1. Add a custom channel map to the ISDS and determine its LUG ID.

   Example: You might create a channel map that contains only high-definition (HD) channels. When giving a name to the channel map, we suggest that you use a name that identifies the lineup group function. For example, you might name a lug-based channel map that contains only HD channels **HD_LUG**.

   Note: Add a customized channel map the same way you would add a typical hub-based channel map to the ISDS. See ***Add a Channel Map*** (on page 109) for assistance.

2. Determine the LUG ID of the custom channel map that you created in step 1: Open the Display Channel Map window for the channel map you just created and write down the Lug ID (lineup group ID) that the ISDS assigned to the new channel map.
3. Repeat steps 1 and 2 to create other custom channel maps.

Note: Several minutes after creating a new channel map, the channel map file can be viewed in the sam cabinet on the BFS Client window. New channel map files are listed under the lug folder in order by lug ID. If a channel map is associated with a hub, then the channel map file will also appear in the sam cabinet by hub ID.

4 ***Create a set of group definition rules*** (see "***Add a Group Definition Rule***" on page 117) that a DHCT must meet in order to receive a custom channel map (Lug ID) that you have created. The ISDS places these rules on the BFS as a file for distribution to DHCTs. DHCTs use the file to determine their Lug ID assignment and download the appropriate channel map.

Note: As the last step in creating a set of group definition rules, click **Write File** to update the group_defs.txt file on the BFS with the rules you have created. After clicking Write File, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

Important: The order in which you create group definition rules is very important: the DHCT stops searching as soon as it finds a matching group definition rule.

Group Definition Rule Settings

Use the following fields when you manage a group definition rule in the ISDS.

Field	Description	
lug_id	The number of the Lug ID that you want to assign to these rules. This is the number that the ISDS assigned when you created the channel map	Do **only one** of these.
virtual_hub	The number of the virtual hub that you want to assign to these rules	
Conditions	Set the criteria fields that a DHCT must satisfy to receive this channel map.	

PowerKEY Package Authorization - This field specifies the Entitlement ID (EID).

You can obtain this value by opening a package in the Package List window and displaying the Set Up Package List window.

When entering this value, you must use a four-digit hexadecimal EID format.

Example: 0x01BD.

Set-Top Hardware Model - You can obtain this value from the Type column in the DHCT Type List window or from the label on the DHCT.

When entering this value, you must use a four-digit model number format.

Example: 4200 or **8300**.

Set-Top Hardware Version - You can obtain this value from the version number listed in the Name column on the DHCT Type List window.

When entering this value, you must use the major #.minor # version string format.

Example: 1.0, **1.2**, or **2.1**.

MAC Address - You can obtain this number by displaying page 3 of the DHCT diagnostic screen or by looking on the back of the DHCT for a label with the MAC address on it.

Physical Hub - You can obtain this value from the Hub List window.

When entering this value you must use a whole number.

Example: 1, **13**, or **44**.

- To exclude any criteria, check the box labeled not.

  Example: If you want a channel map to be used by every DHCT model except for the Explorer 2000, set the DHCT Hardware Model to **2000** and select the box labeled **not**.
- Two or more sets of rules can use the same Lug ID.
- If a DHCT meets more than one set of criteria (and is eligible for more than one Lug ID), the DHCT will be assigned to the first Lug ID for which it meets the conditions.
- A rule must have at least one condition and only one action.

	OUI - This field specifies the organizationally unique identifier (OUI), which is the first six digits of a DHCT MAC address. The OUI is sometimes called the "company ID" portion of the MAC Address. **Example:** Our MAC Addresses currently use an OUI of **00:14:F8**.	
	Bouquet Assignment - Systems that use Digital Video Broadcast-Service Information (DVB-SI), instead of ATSC-SI use bouquets.	
	Service Group ID - Specifies the Service Group ID for this LUG.	

Add a Group Definition Rule

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Group Definitions > Add

After you create channel maps and determine the Lug ID that was assigned to the channel map, define a set of group definition rules that a DHCT must meet to download the appropriate channel map.

The ISDS places these rules on the out-of-band BFS carousel as a file for distribution to DHCTs. A DHCT receives and parses the file to determine the Lug ID for the channel map that the DHCT should use, based on the first rule that the DHCT matches. The DHCT then downloads the appropriate channel map for its Lug ID.

1. In the ISDSAdministrative Console, click the **Applications Interface Modules** tab.
2. Click **Group Definitions**. The Group Definitions Rules window opens.
3. Click **Add**. The Add Group Definition Rules window opens.
4. Complete the fields on the screen as described in Group Definition Rule Settings.
5. Click **Save**. The ISDS saves this rule in the Enhanced Channel Maps Group Definition Rules window.

   Notes:

   - A DHCT must meet all criteria in a rule to receive this channel map.
   - If a DHCT meets more than one set of criteria and is eligible for more than one channel map, the DHCT will be assigned to the first channel map for which it meets conditions.

- Verify that you have entered each value correctly and that the rules are listed in the correct order. Otherwise, DHCTs may download the wrong channel map.

6 Click **Write**. The ISDS updates the **group_defs.txt** file on the BFS with the rules you have created. You can verify the update by viewing the time stamp of the file /dvs/dvsFiles/BFS/osm/group_defs.txt, or by viewing the contents of the file.

Important: Until you click **Write**, the group definition rules are not placed on the BFS for distribution to DHCTs. After you click Write, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

7 Click **Exit** to close the Enhanced Channel Map Group Definition Rules window.

Note: If you forget to click **Write** and click **Exit**, a message window opens and prompts you to save the changes you made to the Enhanced Channel Map Group Definition Rules window. Click **Save** to save your changes, or click **Cancel** to close the window without saving changes.

Modify a Group Definition Rule

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Group Definitions > [Select Rule] > Edit

Complete these steps to change an existing rule.

1 In the ISDS Administrative Console, click the **Application Interface Modules** tab.

2 Click **Group Definitions**. The Group Definitions Rules window opens.

3 Select the check box beside the rule that you want to change.

4 Click **Edit**. Edit Group Definition Rules window opens.

5 Edit the fields based on Group Definition Rule Settings. When making changes, keep the following information in mind:

- To exclude any criteria, check the box labeled **not**. For example, if you want a channel map to be used by every DHCT model except for the Explorer 2000, set the DHCT Hardware Model to 2000 and select the box labeled **not**.
- Two or more sets of rules can use the same Lug ID.
- A rule must contain at least one condition and only one action.

6 Verify that you have entered each value correctly and that the rules are listed in the correct order. Otherwise, DHCTs may download the wrong channel map.

7 Click **Save.** The ISDS saves these changes in the Enhanced Channel Maps Group Definition Rules window.

8 Click **Write**. The ISDS updates the **group_defs.txt** file on the BFS with your changes. You can verify the update by viewing the contents of the file /dvs/dvsFiles/BFS/osm/group_defs.txt.

Important: Until you click **Write**, the group definition rules are not placed on the BFS for distribution to DHCTs. After you click Write, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.

9 Click **Exit** to close the Enhanced Channel Map Group Definition Rules window.

Note: If you forget to click **Write** and click **Exit**, a message window opens and prompts you to save the changes you made to the Enhanced Channel Map Group Definition Rules window. Click **Save** to save your changes, or click **Cancel** to close the window without saving changes.

Troubleshooting Enhanced Channel Maps

There are a few quick checks you can make from the ISDS to troubleshoot enhanced channel maps. In addition, if you have access to a local DHCT that matches a set of rules you have defined, you can use the SAM EDCT (Enhanced Display Channel Table) Information diagnostic screen to troubleshoot Enhanced Channel Maps.

Note: For assistance using the **SAM EDCT Information** screen to troubleshoot Enhanced Channel Map errors, refer to *Enhanced Channel Maps User's Guide* (part number 4011413). To obtain a copy of this publication, see ***Printed Resources*** (on page 8).

The following checks can help you troubleshoot errors that may have occurred when creating enhanced channel maps:

- **Look for Lug Files in the SAM cabinet** - View the contents of the SAM cabinet in the BFS Client window to ensure that new Lug files appear there. Several minutes after creating a new Lug-based channel map, the channel map file can be viewed in the SAM cabinet on the BFS Client window. New Lug-based channel map files are listed beneath the lug folder in order by lug ID. If a channel map is associated with a hub, then the channel map file will also appear in the SAM cabinet by hub ID.

- **Look for updates to the group_defs.txt file** - View the time stamp of the /dvs/dvsFiles/BFS/DNCS/osm/group_defs.txt file to determine if it was updated after you clicked **Write** in the Enhanced Channel Map Group Definition Rules window. If the time stamp is correct, you may also want to view the contents of the group_defs.txt file to ensure that the data is correct.

- **Verify Lug ID numbers assigned to lug- based channel maps** - Open the channel map that is expected to be assigned to a DHCT, or group of DHCTs, and

verify its Lug ID. Also verify that the channel slot assignments are correct.

- **Contact Cisco Services for assistance** - If you determine that the Lug files are not in the SAM cabinet or the group_defs.txt file was not updated.

Delete a Group Definition Rule

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Group Definitions > [Select Rule] > Delete

Complete these steps to delete an existing rule.

1. In the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Group Definitions**. The Group Definitions Rules window opens.
3. Select the check box beside the rule that you want to delete.
4. Click **Delete**. A confirmation window opens.
5. Click **OK**. The rule is removed from the Group Definitions Rules window.
6. Click **Write**. The ISDS updates the **group_defs.txt** file on the BFS with your changes. You can verify the update by viewing the contents of the file /dvs/dvsFiles/BFS/osm/group_defs.txt.

   Important: Until you click **Write**, the group definition rules are not placed on the BFS for distribution to DHCTs. After you click Write, affected DHCTs implement Enhanced Channel Map changes within the hour or following any changes to traditional channel maps. For example, saving a channel map from the Set Up Display Channel Map window would cause affected DHCTs to implement Enhanced Channel Map changes following the setting for the SAM Config Update Timer.
7. Click **Exit** to close the Enhanced Channel Map Group Definition Rules window.

   Note: If you forget to click **Write** and click **Exit**, a message window opens and prompts you to save the changes you made to the Enhanced Channel Map Group Definition Rules window. Click **Save** to save your changes, or click **Cancel** to close the window without saving changes.

11

Set-Tops

Introduction

This section contains procedures for adding set-tops to your network, customizing set-tops for subscribers, authorizing set-tops for a service, and for creating and updating CVT groups.

In This Chapter

Set-Top Provisioning

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

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

The DHCT Provisioning area has five buttons that allow you to work with the set-tops in your system as described in the following table.

This button...	Allows you to perform these tasks...
Type	■ View a list of the set-top types contained in your ISDS database, along with the revision level and OUI for each. ■ Add, modify, or delete a set-top type. ■ Associate software TOC files with or unassociate them from older set-tops that use the OSM method to download software. ■ Download specific operating systems to the set-tops in your network.
DHCT	■ Add, modify, or delete an individual set-top. ■ Send service or system information to an individual set-top within a few minutes. ■ Assign service packages to an individual set-top. ■ Enable an individual set-top to display secure analog, PPV, and VOD services. ■ Authorize a set-top for service. **Note:** Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the ISDS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described in ***Authorize a Set-Top for a Service*** (see "***Authorize a Set-Top or CableCARD Module for a Service***" on page 74, "***Authorize a Device for a Service***" on page 136), you should coordinate the authorization of set-tops for services with your billing system vendor.
Boot Page	This feature is reserved for future use.
OS	View the names of files that currently reside on the BFS.

Image	■ Load the set-top resource file (settop.res) into the ISDS database. ■ View a list of the current set of image files on your system. ■ Load new image files for CVT downloads onto the BFS or remove old image files that are no longer used. ■ Create test groups of set-tops. ■ Set up and download client software to set-tops on your system.

Set-Top Settings

There are a number of settings you need to be aware of when you manage set-tops in the ISDS: ***Set-Top Settings*** (see "***Device Settings***" on page 124), ***Set-Top Type Settings*** (on page 126), and ***Set-Top Image File Settings*** (on page 126).

Device Settings

Use the following fields when you manage devices in the ISDS.

Field	Description
Communications tab	
Admin Status	Defines the administration status of the DHCT. Click the arrow to select one of the following options from the Admin Status list: ■ Out of Service ■ In Service One Way ■ In Service Two Way—select for CableCARD modules ■ Deployed
DHCT Type	Defines the device type you are adding. Select the device type from the drop-down list.
Boot Page	Boot page for this device (if used). Leave blank if you are using bootloader
Primary VASP Name	Primary VASP for this device. Click the arrow to select the Primary VASP Name from the drop-down list (leave blank if you are using bootloader).
S/W Table of Contents	The TOC file specific to this device type. Click **Select** to browse to the correct toc file for this device (leave blank if you are using bootloader). When you load the EMMs into the ISDS for a shipment of devices, a table of contents file (TOC file) is created and is available to your billing system. The TOC file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all devices in the shipment.
Billing ID	Billing ID of the device.
IP Address	IP address of the DNCS server.

IPV6 Address	If you have the IPv6 feature enabled, this field displays the IPv6 address of the DHCT. It is a read-only field.
DHCT Serial Number	Serial number of the device.
Secure Services tab	
Key Certificate	Select the key certificate you are using (if any) with this device. To load the certificates from a batch file or CD, click **Load from batch CD...**.
Packages	Select the packages you want to add to the device from the **Available** list. Click **Add** to move the packages to the **Selected** list. **Notes:** ■ For a description of the available packages, click **Package Descriptions** at the bottom of the window. ■ 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 device must be authorized for that package as well. This should have been done when the device was staged.
IPPV Enable	Select this option to enable this device to receive IPPV events.
IPPV Credit Limit	Active only if you select the **IPPV Enable** option. Enter the number of IPPV credits available to the device.
Max. IPPV Events	Active only if you select the **IPPV Enable** option. Enter the maximum number of IPPV events the device is allowed to view.
DMS Enable	Select this option to allow the device to receive secure services.
DIS Enable	Select this option to help generate VOD purchases.
Analog Enable	Select this option if this device needs to display secure analog services.
Fast Refresh Enable	This option is used to send EMMs to devices during staging. For more information, refer to
Location X	Leave these fields blank or enter a **0** (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.
Location Y	

Set-Top Type Settings

Use the following fields when you manage set-top types in the ISDS.

Field	Description
DHCT Type Number	The type of set-top you are linking.
Revision	The software revision represented by the CVT files. **Example:** Type **10**.
Org. Unit ID	The OUI portion of the set-top MAC address. Type **00:02:DE**.
Name	The name of the set-top type. **Example:** Type **IPN430MC**.
Vendor	The manufacturer of the set-top. **Example:** For the **IPN430MC**, type **Scientific Atlanta**.
S/W Table of Contents	Not used in ISDS.
Boot Page Name	Not used in ISDS.

Set-Top Image File Settings

Use the following fields when you manage set-top image files in the ISDS.

Field	Description
Downloadable Files tab	
Image ID	Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID. **Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends.
File	The name of the image file. Click **Browse** and select the appropriate set-top image file.
Description	A description of the image file.
DHCT Groups tab	
Group ID	The group associated with this image file. Type **20** for the group ID.
Group Name	The name of the group associated with this image file.

DHCT MAC Address	Type the MAC address of a set-top you want to add to the group and click **Add**. That set-top is added to the group list. Remove set-tops from the group by highlighting the set-top in the group list (**Ctrl + click** to select mutliple set-tops) and clicking **Remove**.
DHCT Downloads tab	
View	Determines whether the image is delivered intact or broken into multiple components. Select one of the following options: ■ **Simple** - Use if the image file is small and can be delivered intact. ■ **Component** - Use for large image files that must be delivered in multiple components.
DHCT Type	Select the type of set-top you are downloading the image to.
Group	If you want to narrow the download to a specific group, select the group from the drop-down list.
Carousel	If you want to download the image using a specific carousel, highlight the carousel in the list. **Note:** To select multiple carousels for the download, use **Ctrl + click** to select the carousels you want to use.
Download Scheduling	Determines when the download is issued. Select one of the following options: ■ **Normal** - The set-tops download software based on the following criteria: – Set-top is on: Downloads software at 2:00 a.m. – Set-top is off (standby): Downloads software immediately – Set-top is powered off (unplugged): Downloads software when it is powered on (plugged in) ■ **Immediate** - The set-tops display a notification barker and download software based on the following criteria: – Set-top is on or in standby mode: Downloads software immediately and in a relatively short period of time, but interrupts watching TV, PPV, VOD, and other services (unless the ISDS is in standby mode) – Set-top is powered off (unplugged): Downloads software when it is powered on (plugged in) ■ **Emergency** - The set-tops begin downloading instantaneously and no notification barker is displayed. This method interrupts watching TV, PPV, VOD, and other services (unless the set-tops are in standby mode). **Note:** This method also reboots the set-tops. We recommend that you use this method only in the early morning hours or late at night when viewership is lower.

File Description	Select the file you are downloading from the drop-down list.
Recovery Download Mode	Select this option to allow the bootloader to take control of the set-top and perform the download. Certain set-tops do not support background downloads and all downloads to these set-tops must be performed by the bootloader.

ISDS Manually Add Devices to the ISDS

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > DHCT > Select Option > New

Devices (DHCTs and CableCARD modules) are normally added to the database through CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to add devices to the database.

Follow these instructions to manually add a device to the ISDS database.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Click **Add**. The Add DHCT window opens.
5. Enter information as described in Device Settings.
6. Click **Save**.
7. Do you need to add other devices?
   - If **yes**, repeat this procedure from step 4 for every device you need to add to the database.
   - If **no**, go to the next step.
8. Close the Set Up DHCT window and the DHCT Provisioning window.
9. Your next step is to link the devices to CVT files. Go to ***Link Devices to CVT Files*** (on page 131).

Adding Devices

Follow these instructions to manually add a device to the ISDS database.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Click **Add**. The Add DHCT window opens.
5. Enter information as described in Device Settings.
6. Click **Save**.
7. Do you need to add other devices?
   - If **yes**, repeat this procedure from step 4 for every device you need to add to the database.
   - If **no**, go to the next step.
8. Close the Set Up DHCT window and the DHCT Provisioning window.

9 Your next step is to link the devices to CVT files. Go to ***Link Devices to CVT Files*** (on page 131).

Link Devices to CVT Files

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > Type > Add

Devices (DHCTs and CableCARD modules) are normally linked to their CVT files using the CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to link the devices to their CVT files.

CVT File Settings

Use the following fields when you link devices to CVT files in the ISDS.

Field	Description
DHCT Type Number	The DHCT Type number of the device that you are linking to the CVT file.
Revision	Software revision represented by the CVT files.
Org. Unit ID	The OUI portion of the device MAC address. Type **00:02:DE**.
Name	The name representing the type of device you are linking.
Vendor	Manufacturer of this device. Type **Cisco**.
S/W Table of Contents	Table of contents (TOC) file related to the CVT file. Click **Select** to browse to the correct TOC file (leave blank if you are using bootloader).
Boot Page Name	The name of the boot page associated with this device. Click the arrow to select the boot page from the drop-down list (leave blank if you are using bootloader).

Linking Devices to CVT Files

Follow these instructions to link devices to CVT files.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens.
4. Click **Add**. The Add DHCT Type window opens.

5 Enter information as described in CVT File Settings.

6 Click **Save**. The Add DHCT Type window closes.

7 Click **Exit** to close the DHCT Type List window.

8 Your next step is to configure the device image file. Go to ***Configure the Device Image File*** (on page 133).

Configure the Device Image File

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > Image > Downloadable Files tab > Add

After you link the devices (DHCTs and CableCARD modules) to their image files, you need to configure the image files.

Device Image File Settings

Use the following fields when you configure device image files in the ISDS.

Field	Description
Downloadable Files Tab	
Image ID	Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID. **Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends.
File	The name of the image file. Click **Browse** to select the appropriate set-top image file.
Description	Description of the image file.
DHCT Groups Tab	
Group ID	The group ID associated with this image file (if any).
Group Name	The name of the group associated with this image.
DHCT Downloads Tab	
DHCT Resource File	The resource file (settop.res) associated with this image. Click **Browse** to locate the /dvs/resapp/settop.res file.

Configuring the Device Image File

Follow these instructions to configure the device image file.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.

5 Click **Add**. The Add Downloadable File window opens.

6 Enter information as described in Device Image File Settings.

7 Click **Save**.

8 On the Image List window, click the **Device Groups** tab. The window updates to display device groups.

9 Click **Add**. The Add Device Group window opens.

10 Enter information as described in the Device Group section of Device Image File Settings.

11 Click **Save** and close the Set Up DHCT Group window.

12 On the Image List window, click the **Device Downloads** tab. The window updates to display device downloads configured with the appropriate type and group.

13 Click **Load DHCT Resource File**. The Load DHCT Resource File window opens.

14 Click **Browse** and select the **/dvs/resapp/settop.res** file.

15 Click **Save**.

16 Click **Add**.

17 Change the group to the Group Name assigned to this image, if necessary.

18 Click **Save**.

Customize for Subscribers

Special software on each of our set-top allows you to customize how a set-top functions so that you can customize set-tops to meet the needs of your subscribers.

Ways to Customize Set-Top Behavior

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

- Allow subscribers to skip unauthorized channels.
- Allow subscribers to select which channel the set-top 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 set-top's wireless keyboard.
- Allow subscribers to choose a color scheme for the set-top user screens, or select a color scheme for subscribers.

Ways to Send Customized Behavior to Set-Tops

After you have customized how you want the set-top to function, you can send this configuration to the set-tops in your system in any of the following ways:

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

Authorize a Device for a Service

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

You Need to Know

Before You Begin

Time To Complete

Performance Impact

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

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the ISDS Administrative Console, click the **ISDS** 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 or CableCARD module you are testing.

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

   Tip: When entering IP addresses, type a period to move from octet to octet. Do *not* press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
7. Select the device you want to authorize and click **Edit**. The Edit DHCT window opens with the Communications tab in the forefront.
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 or CableCARD module 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 or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module 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 or CableCARD module 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 to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **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 *Analog Descrambling Support for the Digital Broadband Delivery System Application Guide* (part number 716370) for details. To obtain a copy of this publication, see .
- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375).
- **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 or CableCARD module.

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

15 Click **Exit** to close the Edit DHCT window and return to the DHCT Provisioning window.

16 Click **Exit** 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.

Verify a Successful Service Setup

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

You Need to Know

Before You Begin

Time to Complete

Performance Impact

Follow these instructions to verify a successful service setup.

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

1. Make sure the set-top is connected to a television and to an RF feed into your network.
2. Make sure the set-top and television are powered on.
3. Tune to the channel you selected when you added the service to a channel map.
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 Cisco Services.
5. Is this a PPV or VOD service?
   - If **yes**, attempt to purchase an event, go to step 6.
   - If **no**, you are finished testing the service.
6. 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 Cisco Services.

Create and Update CVT Groups

CVT groups allow you to separate certain devices in your service network from the general population. These devices can then receive software downloads apart from the general device population.

This section provides instructions to create CVT groups.

CVT Test Group Settings

Use the following fields when you manage CVT test groups in the ISDS.

Field	Description
Group ID	The group ID for this CVT test group. Type a unique group ID number (other than zero).
Group Name	The name of this CVT test group.
DHCT MAC Address	The MAC address of a device you want to add to the group. **Note:** Before you add a CableCARD module to the group, the module must be installed in a host and functioning correctly.

Create CVT Groups

Quick Path: ISDS tab > Home Element Provisioning tab > Image > File > New

CVT groups allow you to separate certain devices in your service network from the general population. These devices can then receive software downloads apart from the general device population.

Complete the following steps to create CVT groups for devices in the network. If you already created CVT test groups, do not complete this procedure; go to ***Update CVT Groups*** (on page 140).

Important: A device should be connected to the network within 2 hours of creating or adding it to a group. If the device is not connected within 2 hours, then the device does not receive a group assignment until the ISDS database cycles through all in-service devices. Depending on the number of devices in your system, this process could take a significant amount of time.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.

4 Click the **DHCT Groups** tab. The DHCT Groups tab opens.
5 Select **File > New**. The Set Up DHCT Group window opens.
6 Enter information as described in CVT Group Settings.
7 Click **Add**. The MAC Address of the device moves to the Associated DHCTs column.
8 Repeat steps 6 and 7 for each device you want to add to the group.
9 Click **Save**. The new group appears in the list of group descriptions on the DHCT Groups tab.

Update CVT Groups

Quick Path: ISDS tab > Home Element Provisioning > Image > DHCT Groups tab > [Group name] > File > Open

Complete the following steps to update test groups for devices in the network. If you need to add CVT groups to the ISDS, use the procedure in ***Create CVT Groups*** (on page 139).

Important: A device should be connected to the network within 2 hours of creating or adding it to a group. If the device is not connected within 2 hours, then the device does not receive a group assignment until the ISDS database cycles through all in-service devices. Depending on the number of devices in your system, this process could take a significant amount of time.

1 On the ISDS Administrative Console, select the **ISDS** tab.
2 Select the **Home Element Provisioning** tab.
3 Click **Image**. The Image List window opens.
4 Click the **DHCT Groups** tab. The DHCT Groups tab opens.
5 Select the group you want to update from the list.
6 Click **File > Open**. The Set Up DHCT Group window for the group you selected opens.
7 Evaluate the list in the Associated DHCTs list. Are the Associated devices listed correct?
   - If **yes**, click Cancel.
   - If **no**, add or remove MAC addresses of the devices (as needed), then click **Save**.

Load New Image Files onto the BFS

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > Image > Downloadable Files tab > Add

The next step is to load the image files onto the BFS. Load only the image files for the devices that you have in your system.

Important:

- If a file is used by more than one device type or device revision, you only need to add that file once.
- Unnecessary files will slow the software download. Be careful to load only those files currently required by your system. Refer to ***Delete Unused Device Types from the Database*** (on page 143) for more information.

Follow these instructions to load a new image file onto the BFS.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. On the Image List window, click **Add**. The Add Downloadable File window opens.
6. Do you want to specify an image ID?
   - If **yes**, type a unique **Image ID**.
   - If **no**, leave the Image ID field blank, and the DNCS will automatically assign an Image ID.

   Note: Typing a specific image ID allows you to use the same name for the image ID across multiple headends.
7. In the **File** field, click **Select**. The File Chooser window opens.
8. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
9. Choose one of the following options for the Filter field:
   - **DHCTs:** Type **/dvs/resapp/xxx*rom**
   - **CableCARD modules:** Type **/dvs/cablecard/xxx*rom**

   Note: The "xxx" is part of the file name provided in the software release notes document.

   Example: For a DHCT, type **/dvs/resapp/141*rom**.
10. Click **Filter**. The directory entered becomes the working directory and a filters file list opens.

11 In the **Files** column, select the ROM file that you want to add to the list of downloadable files.

   Example: 1419pe4a7.rom

12 Click **OK**. The file path for the ROM file opens on the Add Downloadable File window.

13 In the **Downloadable File** window, copy or type the file name without the path in the **Description** field.

   Example: 1419pe4a7.rom

14 Click **Save**. The new file and file description appear in the Image List window.

   Note: If the save fails, the file may already exist in the list.

Manage Device Images

This section is an overview of configuring and downloading client software to test groups or to your device population. For a full discussion of the procedures, including all the prerequisites required before your software download, refer to *Downloading Client Application Software to ISDP Set-Tops Installation Instructions* (part number 4021172).

Note: You will need a secure GUI password to set up the image files. Obtain a secure GUI password from Cisco Services. This provides Cisco Services the opportunity to communicate known issues about the software as well as other information that may be needed before loading the software onto your network.

Delete Unused Device Types from the Database

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning > Type > [select type] > Delete

Follow these instructions to delete an unused device type from the ISDS database.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens, listing the device type, revision, OUI, and name.
4. Look at each entry in the list. Is the entry used in your system?
   - If **yes**, there is no need to delete this entry. Look at the next entry.
   - If **no**, or if you are not certain, continue with this procedure.
5. Select the device type you want to delete and click **Delete**. The following message appears:

   Are you sure you want to delete the current item?
6. Click **OK**.
7. Did an **Unspecified Error** message appear?
   - If **yes**, the selected device type is used in your system and you cannot delete it.
   - If **no**, the selected device type is not used in your system, and the ISDS deletes it from the database.
8. Repeat steps 4 through 7 for each device type in the DHCT Type List.
9. From the DHCT Type List window, click **Exit**. The DHCT Type List closes.

Load the settop.res File into the Database

For CVT downloads, you must install the set-top resource file (settop.vxx) that contains the device types installed in your network. The system refers to this data during the image file download assignment process to verify software compatibility with the selected device type.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List opens.
4. Click **Load Device Resource File**. The Load DHCT Resource File window opens.

   Note: Though the screen only mentions DHCTs, you can load CableCARD module software using this screen.
5. Click **Select**. The File Chooser window opens.
6. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
7. Choose one of the following options:
   - If you are installing the resource file from an FTP server, type **/export/home/dncs/download/settop*** in the Filter field.
   - If you are installing the resource file from a CD, complete the following steps.

     a. Insert the CD containing the resource file into the CD drive of the ISDS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.

     b. Type **/cdrom/cdrom0/settop*** in the Filter field.
8. Click **Filter**. The Selection field updates with the directory from which you selected the resource file.
9. Click **settop.vxx** in the Files column.

   Note: This file is named settop.v followed by a version number (for example, **settop.v62**). Be sure that you select the latest version of this file.
10. Click **OK**. The DHCT Resource File field in the Load DHCT Resource File window updates to display the resource file path.
11. Click **Save**. A 'Process Control file saved' message appears on the Image List window.
12. On the Image List window, click **Exit**.
13. Did you install the resource file from a CD?
    - If **yes**, type **eject cdrom** (in either the CD window or in an xterm window on the ISDS) and press **Enter**. The ISDS ejects the CD from the CD drive.
    - If **no**, you are finished with this procedure.

Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

Important: You will need a SW TOC Verification password (or secure GUI password) to complete the following steps. Contact Cisco Services to obtain a SW TOC Verification password.

1 Open an xterm window on the ISDS.

2 Type **cd /export/home/dncs/doctor** and press **Enter**.

3 Type **doctor -q** and press **Enter**. Initially, this command sends a ping command to the QAM to ensure the QAM is communicating with the DNCS. Then, a remote procedure call (RPC) request is sent to each QAM to validate that the higher-level functions in the QAM are working correctly.

4 Are all of the QAMs active in the network?

- If **yes**, go to step 5.
- If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

Example: The following is an example list of network elements that has a non-responding QAM.

```
OK:    QAM BCASTQAM1     172.16.4.201    is alive.
OK:    QAM BCASTQAM1     172.16.4.201    RPC working.
Error: QAM VODMBQAM1      172.16.4.210    is not pingable.
OK:    QAM BCASTQAM2     172.16.4.202    is alive.
OK:    QAM BCASTQAM2     172.16.4.202    RPC working.
OK:    QAM BCASTQAM3     172.16.4.203    is alive.
OK:    QAM BCASTQAM3     172.16.4.203    RPC working.
OK:    QAM VODMQAM2      172.16.4.212    is alive.
OK:    QAM VODMQAM2      172.16.4.212    RPC working.
OK:    BIG    CVLab      172.16.4.101    is alive.
OK:    TED   dncsted     192.168.1.2     is alive.
```

Important: Non-responding QAMs may have an old CVT table retained in memory. If the non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from the non-responding QAMs.

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

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

7 Click **Image**. The Image List window opens.

8 On the Image List window, click the **Device Downloads** tab. The Device Downloads window displays the different devices that have already been configured for a CVT download.

9 Click on the top of the **Group** column to sort the list of device types by group.

10 Does a configured download already exist for the device type, revision, and group that you are testing?

- If **yes**, click to highlight the download and select **Edit**.
- If **no**, go to the next step.

11 At the **File Description** field, click the down arrow and choose the new software. Go to step 12.

12 Select **Add**. The Add Device Download window opens.

13 Complete the following steps to configure the Add Device Download window for the test download.

   a Click the **Device Type** arrow and select a device that needs to receive the new software.

   b Click the **Group** arrow and select the test group.

   c Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

   Note: Unless you have old or test versions still posted, there should be only one choice.

   d Click the **Download Scheduling** arrow and select **Emergency**.

   e If you are using multiple download carousels, select the appropriate **Carousel** for the image download.

14 Click **Save**.

   Note: An emergency download begins instantaneously and no barker opens to the subscriber.

   Result: The Association Verification window opens.

15 Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.

16 Configure the following fields on the Association Verification window:

   - **Are you SURE you want to do this?:** Type **yes**.
   - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
   - **Password:** Type the password you received from Cisco Services.

17 Click **OK**.

   Results:

   - The Association Verification window closes.
   - The Image List window is updated with the newly defined test download schedule.
   - The software download to the device test groups begins.

18 Do you have more devices or groups to test?

   - If **yes**, repeat steps 8 through 17 for each group being tested.

     Note: Since a group can contain multiple device types, you might have multiple downloads to the same device group.

   - If **no**, in the Image List window, click **Exit** to return to the Admin Console window.

19 Open an xterm window on the DNCS.

20 Type **cd /export/home/dncs/doctor** and press **Enter**.

21 Type **doctor -q** and press **Enter**.

22 Are all of the QAMs still active in the network?

- If **yes**, go to step 21.
- If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

23 Your next step is to verify that the test device or devices downloaded software and operate as expected. Go to ***Verify that Test Devices Downloaded Software*** (on page 148) for more information.

Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

Important: You will need a SW TOC Verification password (or secure GUI password) to complete the following steps.

1 On the <product_name_common Administrative Console, select the **ISDS** tab and select the **Home Element Provisioning** tab.

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

3 On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.

4 Does the DHCT type, revision, and group that you are testing already exist?

- If **yes**, select the appropriate row and select **File > Open.** Go to step 6.
- If **no**, go to step 5.

5 At the **File Description** field, click the down arrow choose the new software and select Immediate in the Download Scheduling field. Then, go to step 8.

6 Select **File > New**. The Set Up DHCT Download window opens.

7 Complete the following steps to configure the Set Up DHCT Download window for the test download.

   a Click the **DHCT Type** field arrow and select a device that needs to receive the new software.

   b Click the **Group** field arrow and select the test group you created in Create and Update CVT Test Groups.

   c Click the **File Description** field arrow and select the file that corresponds to the new application platform release that you want to download.

   Note: Unless you have old or test versions still posted, there should be only one choice.

   d Click the **Download Scheduling** field arrow and select **Immediate**.

8 On the Set Up DHCT Download window, click **Save**.

Note: An emergency download begins instantaneously and no barker opens to the subscriber.

Result: The Association Verification window opens.

9 Verify that the DHCT Type, Group, and Image File versions shown on the Association Verification window are correct.

10 Configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?:** Type **yes**.
- **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password:** Type the password you received from Cisco Services.

11 Click **OK**.

Results:

- The Association Verification window closes.
- The Image List window is updated with the newly defined test download schedule.
- The software download to the ISDS test groups begins.

12 Do you have more devices or groups to test?

- If **yes**, repeat steps 3 through 11 for each group being tested.

  Note: Since a group can contain multiple DHCT types, you might have multiple downloads to the same DHCT group.
- If **no**, in the Image List window, select **File > Close** to return to the Admin Console window.

13 Your next step is to verify that the test device or devices downloaded software and operate as expected. Go to ***Verify that Test Devices Downloaded Software*** (on page 148).

Verify that Test Devices Downloaded Software

Verify that the test devices operate as expected by checking the following items.

Verify that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-

top.

Verify that CableCARD Modules Downloaded Software

- Verify that each host can display all authorized services.

Download Client Software to Devices

The instructions in this section provide the steps to prepare and download the application platform software release to devices using the CVT method.

Notes:

- This procedure is for downloading client software to your entire population of devices (set-tops and CableCARD modules). If you need the procedure to download only to a specific CVT group, follow the procedure in ***Download Images to CVT Test Groups*** (on page 144, on page 147).
- The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

1. On the ISDS Administrative Console, select the **ISDS** tab and select the **Home Element Provisioning** tab.
2. Click **Image**. The Image List window opens.
3. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.
4. In the DHCT Type column, select the DHCT type that will receive the new software where the value in the Group column is labeled **Default**.
5. Click **File > Delete**.
6. Repeat steps 4 and 5 for each DHCT type that will receive new software.

   Note: Do *not* remove the download entries for your test groups. Leave the download entries for your test groups configured.
7. In an xterm window, type **listCVT** and press **Enter**. The listCVT report displays. Look for unused files in the report.

   Example:

```
Model Rev        OUI    IMG# Grp  Download Group  Image
Mode   DHCTs
----- ---   ----  ----  --- --------------  ------------
-----   ----

430   1.1   02DE    10       Default
VALINOR_02.02.29.00_ Emerg   -
                    9   .. (not being used)
VALINOR_02.01.25.00_
                    8   .. (not being used)
VALINOR_02.00.92.00_
```

```
-------------------------------------------------------------
--------------
Total image files being downloaded = 1
```

8 Select the **Downloadable Files** tab on the Image List window and compare the list of files displayed with the list of unused files listed in the listCVT report.

9 Select any unused file on the **Downloadable Files** tab.

Note: The new software should not be listed as unused because it is associated with a test group.

10 Click **File > Delete**.

Note: The ISDS will not allow you to delete a file that is already associated with a download.

11 Repeat steps 9 and 10 until you have deleted all unused files.

12 Select the **DHCT Downloads** tab.

13 Click **File > New**. The Set Up DHCT Download window opens.

14 Complete the following steps to configure the Set Up DHCT Download window.

a Click the **DHCT Type** field arrow and select a device that needs to receive the new software.

b Click the **Group** field arrow and select **Default**.

c Click the **File Description** field arrow and select the file that corresponds to the new application platform release that you want to download.

Note: Unless you have old or test versions still posted, there should be only one choice.

d Click the **Download Scheduling** field arrow and select either **Normal** or **Immediate**.

15 Click **Save**. The Association Verification window opens.

16 Verify that the DHCT Type, Group, and Image File versions shown on the Association Verification window are correct.

17 Configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?:** Type **yes**.
- **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password:** Type the password you received from Cisco Services.

18 Click **OK**. The system schedules the software download according to the schedule you configured earlier in this section.

19 Repeat steps 13 through 18 for each DHCT type that you want to receive the software using the CVT method.

UN-Config

The UN-Config (user-to-network configuration) sends messages from the ISDS to set-tops and CableCARD modules that configure or reboot the set-tops or CableCARD modules.

This section describes the functions and procedures that allow you to maintain a single device or population of devices.

Initiate UN-Config for a Single Set-Top or CableCARD Module

ISDS Administrative Console > ISDS tab > System Provisioning tab > System Management > UN-Config > Initiate UN-Config for single DHCT

To send UN-Config messages to a single set-top or CableCARD module, use the following procedure.

WARNING:

Before initiating a software download for a set-top or a CableCARD module using UN-Config, you must make sure that the corresponding image is on the BFS carousel (or on the appropriate download server, if applicable). Otherwise, the device will stall and become unusable.

Follow these instructions to initiate a UN-Config for a single set-top or CableCARD module.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. In the System Management section, click the **UN-Config** tab. The UN-Config window opens.
4. Select the **Initiate UN-Config for single DHCT** option.
5. Enter the **MAC Address** for the set-top or CableCARD module that will receive the UN-Config messages.
6. Select one of the following **Reason Codes**:
   - **Normal** - For a normal UN-Config indication message. The set-top or CableCARD module should send a reply.
   - **No Reply** - For an unsolicited UN-Config indication message. No reply is expected from the set-top or CableCARD module.
   - **Download Now No Reply** - Requests the set-top or CableCARD module download a new OS image immediately. No reply is expected.
   - **Download Now With Reply** - Requests the set-top or CableCARD module download a new OS image immediately. A reply is expected from the set-top or CableCARD module before the download begins.

- **Download No Reply** - Requests the set-top or CableCARD module download a new OS image when convenient. No reply is expected.
- **Download With Reply** - Requests the set-top or CableCARD module download a new OS image when convenient. A reply is expected from the set-top or CableCARD module before the download begins.

7 Click **Send**. The ISDS sends the UN-Config messages to the selected set-top or CableCARD module.

Initiate UN-Config for a DHCT Type

ISDS Administrative Console > ISDS tab > System Provisioning tab > System Management > UN-Config > Initiate UN-Config for DHCT Type

To send the UN-Config messages to an entire population of set-tops or CableCARD modules based on type, use the following procedure.

WARNING:

Before initiating a software download for a DHCT type using UN-Config, you must make sure that the corresponding image is on the BFS carousel (or on the appropriate download server, if applicable). Otherwise, the device will stall and become unusable.

Follow these instructions to initiate a UN-Config for a set-top type.

1 From the ISDS Administrative Console, click the **ISDS** tab.

2 Click the **System Provisioning** tab.

3 In the System Management section, click the **UN-Config** tab. The UN-Config window opens.

4 Select the **Initiate UN-Config for DHCT Type** option.

5 Select the **DHCT Type Name** from the list for the population of set-tops or CableCARD modules.

6 Select one of the following **Reason Codes**:

- **No Reply** - For an unsolicited UN-Config indication message. No reply is expected from the population defined by the DHCT type.
- **Download Now No Reply** - Requests the population defined by the DHCT type download a new OS image immediately. No reply is expected.
- **Download No Reply** - Requests the population defined by the DHCT type download a new OS image when convenient. A reply is expected from the population before the download begins.

7 Click **Send**. The ISDS sends the UN-Config messages to the selected set-top or CableCARD module population defined by the type you selected.

Reboot a DHCT or CableCARD Module

ISDS Administrative Console > ISDS tab > System Provisioning tab > System Management > UN-Config > Reboot DHCT

Follow these instructions to reboot a single set-top or CableCARD module using UN-Config messages.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. In the System Management section, click the **UN-Config** tab. The UN-Config window opens.
4. Select the **Reboot DHCT** option.
5. Enter the **MAC Address** for the set-top or CableCARD module you want to reboot.
6. Click **Send**. The ISDS sends the reboot UN-Config command to the selected set-top or CableCARD module.

MoCA

Quick Path: Global Parameters: ISDS tab > Sys Config > MoCA Parameters tab

Quick Path: Set-Top Parameters: ISDS tab > Home Element Provisioning tab > DHCT > [Enter Set-Top MAC/IP/SN] > Continue > MoCA Parameters tab

MoCA (Multimedia Over Coax Alliance) technology allows a set-top to establish IP connectivity using the in-home coax cable. The set-top uses MoCA to both send and receive IP messages, thus providing 2-way IP connectivity.

MoCA Parameter Priority Implementation on the STB

Cisco set-tops support three levels of MoCA parameter set priority. These are described in the following table.

Priority	Name	Description
Lowest	Built-In	These parameters are built into the platform software.
Medium	Default	These parameters are received from the ISDS using a broadcast 55-1 message.
Highest	Set-Top Specific	These parameters are assigned to an individual set-top from the ISDS using a unicast 55-1 message.

Because MoCA parameter sets can be received by different methods with different priority levels, the MoCA subsystem follows the rules specified in the following table when deciding whether to accept or ignore new MoCA parameters.

		Current Parameters		
		Built-In	**Default**	**Set-Top Specific**
New Parameters	**Built-In**	Always use	Ignore	Ignore
	Default	Always use	Always use	Ignore
	Set-Top Specific	Always use	Always use	Always use

MoCA Parameter Priority Examples

When the set-top receives and accepts an updated parameter set, the MoCA operation is reconfigured to use the updated parameters. The set-top leaves the MoCA network and re-joins the network without rebooting.

If the new parameter set is the same as the existing parameter set, the priority of the parameter set is recorded but MoCA network connectivity will not be interrupted.

All MoCA parameter sets, once accepted by the set-top, are persistent when the set-top reboots.

Examples of MoCA parameter configuration are as follows:

- If the set-top has no or limited ISDS connectivity and is booted for the first time, the set-top uses the built-in MoCA parameters. If the software on this set-top is later updated (with at least partial ISDS connectivity), the set-top uses any revised built-in MoCA parameters contained in the new image when the set-top reboots to use the new software.
- If the set-top has no ISDS connectivity when booted for the first time, the set-top uses the built-in MoCA parameters. If ISDS connectivity is later established and the set-top receives updated default MoCA parameters from the ISDS, the set-top stores and uses these updated parameters.
- If the set-top previously booted with ISDS connectivity and received default parameters from the ISDS, a platform code upgrade with new built-in parameters will not affect the MoCA operational parameters that are stored in the set-top.

MoCA Settings

The settings for MoCA have specific defaults. The global settings can be overridden by the individual set-top settings.

Global MoCA Settings

Use the following fields when you manage global MoCA settings in the ISDS.

Field	Description
Specify NC Mode	Network Coordinator setting. Select one of the following options: ■ **Master:** The master is the network coordinator (NC). It sends the beacon, sets the system clock, and performs bandwidth allocation. The NC must have the best RF modulation profiles compared to the non-NC devices. ■ **Slave:** Non-NC role. Non-NC devices only need to send and receive to the NC to join a MoCA network. They do not need to be able to send and receive to all MoCA devices in the network. ■ **Auto (default):** If no other NC is detected in the network, assumes the role of Master (NC). If an NC is detected in the network, assumes the role of Slave (non-MC).
Security Password	Determines if you use a security password for MoCA. To set a password, check the box and enter the security password in the space provided. ■ **Default:** Unchecked with no password **Important:** If you set the security password, all nodes on the network must be set to use the same password.
Manual Transmit Power	Allows you to set the transmit power of the MoCA gateway. To set the transmit power manually, check the box and enter the transmit power in the space provided. ■ **Default:** Unchecked (auto) with no power setting
Frequency Scan Mode Auto	Determines whether you use a fixed frequency or allow the set-top to scan frequencies for the MoCA signal. ■ **For scan:** Check the box and select a set of frequencies in Frequency Plan (optional) ■ **For fixed frequency:** Uncheck the box, and select the fixed frequency from the list ■ **Default:** Unchecked and 1150 MHz
Frequency Plan	The set of frequencies to scan when Frequency Scan Mode Auto is selected. Select the set of frequencies by checking the box next to the frequency. **Default:** N/A

Set-Top MoCA Settings

Use the following fields when you manage set-top MoCA settings in the ISDS.

Note: Set-top MoCA settings override the global settings.

Field	Description
Specify NC Mode	Network Coordinator setting. Select one of the following options: ■ **Master:** The master is the network coordinator (NC). It sends the beacon, sets the system clock, and performs bandwidth allocation. The NC must have the best RF modulation profiles compared to the non-NC devices. ■ **Slave:** Non-NC role. Non-NC devices only need to send and receive to the NC to join a MoCA network. They do not need to be able to send and receive to all MoCA devices in the network. ■ **Auto (default):** If no other NC is detected in the network, assumes the role of Master (NC). If an NC is detected in the network, assumes the role of Slave (non-MC).
Security Password	Determines if you use a security password for MoCA. To set a password, check the box and enter the security password in the space provided. ■ **Default:** Unchecked with no password **Important:** If you set the security password, all nodes on the network must be set to use the same password.
Manual Transmit Power	Allows you to set the transmit power of the MoCA gateway. To set the transmit power manually, check the box and enter the transmit power in the space provided. ■ **Default:** Unchecked (auto) with no power setting
Frequency Scan Mode Auto	Determines whether you use a fixed frequency or allow the set-top to scan frequencies for the MoCA signal. ■ **For scan:** Check the box and select a set of frequencies in Frequency Plan (optional) ■ **For fixed frequency:** Uncheck the box, and select the fixed frequency from the list ■ **Default:** Unchecked and 1150 MHz
Frequency Plan	The set of frequencies to scan when Frequency Scan Mode Auto is selected. Select the set of frequencies by checking the box next to the frequency. **Default:** N/A

Change MoCA Parameters

The MoCA parameters for the ISDS system are typically set up during initial installation. However, you can change these parameters as your network and requirements change.

Note: Changing the MoCA parameters for an individual set-top overrides the global MoCA parameters setup at the system level.

Changing Global MoCA Parameters

Follow these instructions to change the global MoCA parameters.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Under System Management, click **Sys Config**. The ISDS System Configuration window opens.
4. Click the **MoCA Parameters** tab.
5. Change the information you need by using the information in Global MoCA Settings.
6. When you are finished, click **Save**.

Changing Set-Top MoCA Parameters

Follow these instructions to change the MoCA parameters for an individual set-top.

Note: Changing the MoCA parameters for an individual set-top overrides the global MoCA parameters set up at the system level.

1. On the ISDS Administration Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Enter one of the following for the set-top you want to edit.
   - MAC address
   - IP address
   - Serial number
5. Click **Continue**. The Set Up DHCT window opens.
6. Click the **MoCA Parameters** tab.
7. Change the information you need by using the information in Set-Top MoCA Settings.
8. When you are finished, click **Save**.

Reset Set-Tops

This section details the steps you need to reset set-tops, including resetting the set-top NVM, resetting the set-top PIN, and resetting the set-top itself.

Resetting the Set-Top PIN

1. From the ISDS Administrative Console, click the **Home Element Provisioning** tab.
2. Click **DHCT**. The DHCT Provisioning window opens.
3. Enter the **MAC Address**, **IP Address**, or **Serial Number** of the DHCT you want to edit and click **Continue**. The Set Up DHCT window opens.
4. Enter a new **PIN Value** and click **Send**. The ISDS sends the reset PIN message to the set-top.

Resetting the Set-Top

1. From the ISDS Administrative Console, click the **Home Element Provisioning** tab.
2. Click **DHCT**. The DHCT Provisioning window opens.
3. Enter the **MAC Address**, **IP Address**, or **Serial Number** of the DHCT you want to edit and click **Continue**. The Set Up DHCT window opens.
4. Click **Reset HCT Resources**. The Reset HCT Resources window opens.
5. Click **HCT** and click **Send Reset**. The ISDS sends the reset set-top message to the set-top.

Resetting the CableCARD Module

1. From the ISDS Administrative Console, click the **Home Element Provisioning** tab.
2. Click **DHCT**. The DHCT Provisioning window opens.
3. Enter the **MAC Address**, **IP Address**, or **Serial Number** of the DHCT you want to edit and click **Continue**. The Set Up DHCT window opens.
4. Click **Reset HCT Resources**. The Reset HCT Resources window opens.
5. Click **CableCARD** and click **Send Reset**. The ISDS sends the reset CableCARD module message to the set-top.

Resetting the Set-Top NVM

Follow these instructions to reset the non-volatile memory of a set-top.

1. From the ISDS Administrative Console, click the **Home Element Provisioning** tab.
2. Click **DHCT**. The DHCT Provisioning window opens.
3. Enter the **MAC Address**, **IP Address**, or **Serial Number** of the DHCT you want to edit and click **Continue**. The Set Up DHCT window opens.
4. Click **Reset HCT Resources**. The Reset HCT Resources window opens.
5. Click **NVM** and click **Send Reset**. The ISDS sends the reset NVM message to the set-top.

Resetting the Set-Top Disk

1. From the ISDS Administrative Console, click the **Home Element Provisioning** tab.
2. Click **DHCT**. The DHCT Provisioning window opens.
3. Enter the **MAC Address**, **IP Address**, or **Serial Number** of the DHCT you want to edit and click **Continue**. The Set Up DHCT window opens.
4. Click **Reset HCT Resources**. The Reset HCT Resources window opens.
5. Click **Disk** and click **Send Reset**. The ISDS sends the reset disk message to the set-top.

Resetting the Set-Top Flash Memory

1. From the ISDS Administrative Console, click the **Home Element Provisioning** tab.
2. Click **DHCT**. The DHCT Provisioning window opens.
3. Enter the **MAC Address**, **IP Address**, or **Serial Number** of the DHCT you want to edit and click **Continue**. The Set Up DHCT window opens.
4. Click **Reset HCT Resources**. The Reset HCT Resources window opens.
5. Click **Flash** and click **Send Reset**. The ISDS sends the reset flash memory message to the set-top.

Using the IIH Utility to Reset Set-Tops

The IIH utility can be configured to send certain billing transactions to set-tops.

Each transaction is identified by the system through specific parameters that are used in conjunction with the IIH utility. See ***IIH*** (on page 472) for information on the parameters used with IIH.

Using IIH with a List of Set-Tops

Each of the transactions listed in ***IIH*** (on page 472) can be run using a list of set-tops.

Each set-top in the list is identified by MAC address. You typically prepare the list of set-tops, identified by MAC address, before using the utility by using a text editor, such as vi. Instructions for preparing the list of set-tops are found in ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396).

Note: When the IIH utility processes a list of set-tops, the transaction processes 10 set-tops at a time, by default. The reason 10 set-tops are processed at a time is to avoid monopolizing the bossServer process of the ISDS. If you have an urgent need to process more set-tops than ten at a time, you can override the default value through use of the **-C** parameter.

Refresh Set-Top EMMs with the dhctInstantHit Transaction

The dhctInstantHit transaction refreshes set-tops with EMMs from the database.

The following procedures provide detailed instructions for sending a dhctInstantHit transaction to an individual set-top, set-tops contained in a list, or set-tops of a specific model type.

Refreshing the EMMs of an Individual Set-Top

Follow these instructions to refresh the EMMs of an individual set-top.

1. Open an xterm window on the ISDS.
2. Type **IIH -i [set-top MAC address]** and press **Enter**. The system refreshes the specified set-top with its EMMs.

   Notes:

   - Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets [ ] in the command.
   - The MAC address can be formatted with or without colons (:).

   Examples:

   IIH -i 00:02:DE:A6:45:92

   IIH -i 0002DEA64592

Refreshing the EMMs of a List of Set-Tops

Follow these instructions to refresh the EMMs of a list of set-tops.

1. Open an xterm window on the ISDS.
2. Do you want to force the system to process more than ten set-tops at a time?
   - If **yes**, go to step 3.
   - If **no**, go to step 4.
3. Type **IIH -i -C[# of set-tops] [text file name]** and press **Enter**. Go to step 5.

Notes:

- Substitute the number of set-tops you want to process at once for [# of set-tops]. Do not type the brackets **[ ]** in the command.
- Substitute the name (including path) of the text file for [text file name]. Do not type the brackets in the command.

  Example: IIH -i -C50 /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

4 Type **IIH -i [text file name]** and press **Enter**.

  Note: Substitute the name (including path) of the text file for [text file name]. Do not type the brackets **[ ]** in the command.

  Example: IIH -i /tmp/iih-in_11.31.02

  Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

5 Type **y** and press **Enter**. The system lists the MAC addresses of the set-tops as it sends a dhctInstantHit transaction to each one.

Refreshing the EMMs of Set-Tops with a Specific Model Number

The dhctInstantHit transaction can be configured to refresh the EMMs of a specific model number of set-top. Follow these instructions to refresh the EMMs of set-tops of a specific model number.

1 Open an xterm window on the ISDS.

2 Type **IIH -i -M[model number]** and press **Enter**.

  Note: Substitute the model number of DHCT for [model number]. Do not type the brackets **[ ]** in the command.

  Example: IIH -i -M2100

  Result: A confirmation message similar to the following appears:

```
DHCTs with DHCT Model=[model number] will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

3 Type **y** and press **Enter**. The system sends a dhctInstantHit transaction to each set-top of the specified model number.

Reset Set-Top NVM with the resetClientNvm Transaction

The resetClientNvm transaction resets the non-volatile memory (NVM) of a set-top to default settings established at the factory.

The procedures in this section provide detailed instructions on resetting the NVM of an individual set-top, a list of set-tops, or DHCTs of a specific model number.

Note: The **-r** option, which is used to reset the NVM, is only a valid option at sites that use the SARA Application Server. When the -r option is used at a site that does not use the SARA Application Server, the system displays an error message.

Resetting the NVM of an Individual Set-Top

Follow these instructions to reset the NVM of an individual set-top.

1. Open an xterm window on the ISDS.
2. Type **IIH -r [set-top MAC address]** and press **Enter**. The system resets the NVM of the specified set-top.

   Notes:

   - Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets [ ] in the command.
   - The MAC address can be formatted with or without colons (:).

   Examples:

   IIH -r 00:02:DE:A6:45:92

   IIH -r 0002DEA64592

Resetting the NVM of a List of Set-Tops

Follow these instructions to reset the NVM of a list of set-tops.

1. Open an xterm window on the ISDS.
2. Do you want to force the system to process more than ten set-tops at a time?
   - If yes, go to step 3.
   - If no, go to step 4.
3. Type **IIH -r -C[# of set-tops] [text file name]** and press **Enter**. Go to step 5.

   Notes:

   - Substitute the number of set-tops you want to process at once for [# of set-tops]. Do not type the brackets **[ ]** in the command.
   - Substitute the name (including path) of the text file for [text file name]. Do not type the brackets in the command.

   Example: IIH -r -C50 /tmp/iih-in_11.31.02

   Result: A confirmation message, similar to the following, appears:

   ```
   DHCTs listed in file "[filename]" will be NVM reset …
   [#] MAC addresses will be involved.
   Do you want to continue? (Y/N)
   ```

4. Type **IIH -r [text file name]** and press **Enter**.

Note: Substitute the name (including path) of the text file for [text file name]. Do not type the brackets **[ ]** in the command.

Example: IIH -r /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be NVM reset …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

5 Type **y** and press **Enter**. The system lists the MAC addresses of the set-tops as it sends a resetClientNvm transaction to each.

Resetting the NVM of Set-Tops of a Specific Model Number

The resetClientNvm transaction can be configured to reset the NVM of a specific model number of set-top.

Follow these instructions to reset the NVM of set-tops of a specific model number.

1 Open an xterm window on the ISDS.

2 Type **IIH -r -M[model number]** and press **Enter**.

Note: Substitute the model number of set-top for [model number]. Do not type the brackets **[ ]** in the command.

Example: IIH -r -M2100

Result: A confirmation message, similar to the following, appears:

```
saManager is running
DHCTs with DHCT model=[model number] will be NVM-Reset
# MAC addresses will be involved.
Do you want to continue (Y/N)?
```

3 Type **y** and press **Enter**. The system resets the NVM of the specified set-tops.

Reboot a Set-Top with the bootDhct Transaction

The bootDhct transaction reboots a single set-top, a list of set-tops, or set-tops of a specific model number.

Follow the instructions in this section to configure the IIH utility to send a bootDhct transaction.

Rebooting an Individual Set-Top

Follow these instructions to reboot an individual set-top.

1 Open an xterm window on the ISDS.

2 Type **IIH -b [set-top MAC address]** and press **Enter**. The system reboots the specified set-top.

Notes:

- Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets **[ ]** in the command.
- The MAC address can be formatted with or without colons (:).

Examples:

IIH -b 00:02:DE:A6:45:92

IIH -b 0002DEA64592

Rebooting a List of Set-Tops

Follow these instructions to reboot a list of set-tops.

1. Open an xterm window on the ISDS.
2. Do you want to force the system to process more than ten set-tops at a time?
   - If **yes**, go to step 3.
   - If **no**, go to step 4.
3. Type **IIH -b -C[# of set-tops] [text file name]** and press **Enter**. Go to step 5.

   Notes:
   - Substitute the number of set-tops you want to process at once for [# of set-tops]. Do not type the brackets **[ ]** in the command.
   - Substitute the name (including path) of the text file for [text file name]. Do not type the brackets in the command.

   Example: IIH -b -C50 /tmp/iih-in_11.31.02

   Result: A confirmation message, similar to the following, appears:

   ```
   DHCTs listed in file "[filename]" will be Rebooted …
   [#] MAC addresses will be involved.
   Do you want to continue? (Y/N)
   ```
4. Type **IIH -b [text file name]** and press **Enter**.

   Note: Substitute the name (including path) of the text file for [text file name]. Do not type the brackets **[ ]** in the command.

   Example: IIH -b /tmp/iih-in_11.31.02

   Result: A confirmation message, similar to the following, appears:

   ```
   DHCTs listed in file "[filename]" will be Rebooted …
   [#] MAC addresses will be involved.
   Do you want to continue? (Y/N)
   ```
5. Type **y** and press **Enter**. The system lists the MAC addresses of the set-tops as it sends a bootDhct transaction to each.

Rebooting Set-Tops of a Specific Model Number

Follow these instructions to reboot set-tops of a specific model number.

1. Open an xterm window on the ISDS.

2 Type **IIH -b -M[model number]** and press **Enter**.

Note: Substitute the model number of set-top for [model number]. Do not type the brackets **[ ]** in the command.

Example: IIH -b -M2100

Result: A confirmation message, similar to the following, appears:

```
saManager is running
DHCTs with DHCT model=[model number] will be Rebooted
# MAC addresses will be involved.
Do you want to continue (Y/N)?
```

3 Type **y** and **press** Enter. The system reboots the specified set-tops.

12

PowerKEY CableCARD Modules

tiIntroduction

This section contains procedures you can use to display and manage the CableCARD modules in your system.

In This Chapter

About CableCARD Modules

The PowerKEY CableCARD module complies with the OpenCable specification for a removable security device that separates a retail device from a provider's conditional access system.

A CableCARD module inserts into a slot on a host device, such as a set-top or a digital television. Once inserted, the CableCARD module controls access to secure digital content so that authorized host devices can receive this content according to the CCI data for the program or event.

The host device, which can be purchased from a retail store or elsewhere, supplies all other basic tuning, navigation, and video display capabilities. If the host device is capable of receiving clear digital content, and the subscriber does not want to receive secure digital content, a CableCARD module is not required. However, if the subscriber wants to receive secure digital content, a CableCARD module is required.

The CableCARD module uses the PowerKEY Conditional Access System in the same manner as an Explorer DHCT to decrypt secure digital content. In fact, you authorize CableCARD modules for services in the same way that you authorize Explorer DHCTs.

M-Card Modules and SSC DHCTs

In addition to CableCARD modules, Separable Security Hosts with CableCARD Modules (SSC) set-tops also comply with the OpenCable specification for a removable security device.

An SSC set-top includes the functionality of the stand-alone set-top, but adds the convenience of a factory-installed PowerKEY Multi-Stream CableCARD module (or M-Card).

The M-Card module is mounted in the rear of the set-top and is secured with a cover plate to deter tampering. A label on the rear panel of the set-top provides the bar codes for the serial number and MAC address of the M-Card module.

Service providers should make every effort to ensure that the SSC combination (of the set-top and the CableCARD or M-Card module) remains together. If this combination is separated, the convenience of having the combination is lost, and you must either implement manual processes to redeploy either unit or return the set-top to us for repair.

Binding CableCARD Modules and Hosts

For hosts to provide the high-value, copy-protected services authorized by a conditional access system, a CableCARD module and host must be *bound*.

Binding is a ISDS function that matches the MAC address of the CableCARD to the host ID of the host.

You must bind a CableCARD module to its host to authorize the bound pair to present "high-value" copy-protected services (services with copy protection settings of either *copy one generation* or *copy never*). However, services that are copy protected with the copy-protection setting of *copy freely* can be viewed by an unbound CableCARD and host pair.

SSC set-tops and M-Card modules use the combo-binding method. With this method, the SSC set-top downloads its EMMs during staging and the ISDS populates its database with the SSC pairing information from the staging inventory file.

The ISDS then sends pairing information (as a file named podData) to the BFS, which allows the SSC set-tops and M-Card modules to bind. This file contains two lists: an authorized list and an unauthorized list. Each list contains information on the SSC DHCT and its paired M-Card module.

The M-Card module reads the pairing information from the file. If the M-Card module finds its SSC pairing in the authorized list, it authorizes the binding between it and the SSC set-top. If it finds its SSC pairing in the unauthorized list, or if it does not find its SSC pairing in either list, it does not authorize the binding.

CableCARD Module Binding Methods

Binding is a ISDS function that matches the MAC address of the CableCARD to the host ID of the host. You must bind a CableCARD module to its host before the CableCARD module can receive "high-value" copy-protected services (services with copy protection settings of either copy once or copy never). Services that are copy protected with the copy protection setting of copy freely can be viewed by an unbound host.

Important: Until you bind the SSC set-top and the CableCARD module, the set-top will not be able to display high-value, copy-protected services—even if the set-top is authorized to receive these services.

You can choose to use one of the following copy protection binding methods:

- **Combo-binding** occurs when the SSC set-top downloads EMMs during staging. Sending the EMMs to the SSC set-top starts a process that adds the CableCARD module/host pair to a file (podData) on the BFS. After the pair is added to the file, the SSC set-top receives the podData file that authorizes the CableCARD module and the set-top to be bound.
- **Autobinding** matches a CableCARD module and host when the CableCARD module is inserted into the host and the host goes into two-way mode. Autobinding is available for two-way hosts only if **all** of the following conditions are met:

- The ISDS is set up for autobinding.
- The CableCARD module and host can be staged in a one-way or two-way environment.

  Note: To use autobinding, the CableCARD module and host must be bound in a two-way environment to view high-value content. Once bound, they can be used in a one-way environment.
- The host is **not** on the certificate revocation list (CRL).

- **Manual binding** allows binding of the CableCARD module and host from either the ISDS or the billing system. From the ISDS, the CableCARD module ID and host ID are added to the ISDS through the CableCARD interface.
- **Billing-transaction** binding occurs from the billing system interface using the RegisterHost command. Contact your billing vendor to see if they support this option.

CableCARD Filter

From the Filter area on the CableCARD Summary window, you can quickly retrieve information about the PowerKEY® CableCARD™ modules in your system. The Filter allows you to select CableCARD attributes, such as CableCARD ID or Host MAC address, and find the CableCARD modules in your system that meet your search criteria.

CableCARD Filter Settings

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > Filter

This section describes CableCARD Filter options and provides examples to show how the Filter searches for CableCARD data based on your selections.

The following table describes the Filter options for searching CableCARD modules.

By Field	By Value	Examples
CCard MAC Address	Enter any part of a CableCARD MAC address in the By Value field to have the filter display CableCARD modules with MAC addresses that match any portion of the text entered in this field. **Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons.	If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules with any of the following MAC addresses: ■ **AA:BB**:CC:EE:DD:FF ■ CC:**AA:BB**:CC:DD:EE ■ CC:FF:FF:DD:**AA:BB** **Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above.
Host MAC Address	Enter any part of a Host MAC address in the By Value field to have the filter display CableCARD modules paired with hosts whose MAC addresses match any portion of the text entered in this field. **Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons.	If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts that have any of the following MAC addresses: ■ **AA:BB**:CC:EE:DD:FF ■ CC:**AA:BB**:CC:DD:EE ■ CC:FF:FF:DD:**AA:BB** **Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above.

Vendor ID **Note:** The Vendor ID consists of the first three digits of a Host ID. These first three digits are used to identify the manufacturer (or vendor) of the host device.	Enter the Vendor ID for a host device in the By Value field to have the filter display CableCARD modules whose hosts have the same vendor ID. **Note:** Enter only numbers in this field.	If you enter **0-38** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts whose Host IDs begin with 0-38. Example: Any of the following Host IDs might be found: ■ **0-38**0-000-022-331 ■ **0-38**0-000-022-141

CCard Binding	■ **Active Binding** - Only those CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the ISDS. ■ **Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast by the ISDS. ■ **Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content. ■ **Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content. ■ **Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content. **Note:** For more information on revoked hosts, see ***Certification Revocation List*** (see "***Maintain CRL***" on page 211).	

CCard ID	Enter any part of a CableCARD ID in the By Value field to have the filter display CableCARD modules with IDs that match any portion of the text entered in this field.	If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with CableCARD IDs that contain this number. Example: The Filter would find any of the following CableCARD IDs: ■ **0-010**-670-850-691 ■ 0-011-028-3**00-10**8 ■ 0-011-039-01**0-010**
Host ID	Enter any part of a Host ID in the By Value field to have the filter display CableCARD modules with Host IDs that contain the number you have entered. **Note:** Enter only numbers in this field.	If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with Host IDs that contain this number. Example: The Filter would find any of the following Host IDs: ■ **0-010**-670-186-813 ■ 0-380-0**00-10**0-251 ■ 0-380-0**00-10**8-460

■

CableCARD Filter Options

The following table describes the Filter options for searching CableCARD modules.

By Field	By Value	Examples
CCard MAC Address	Enter any part of a CableCARD MAC address in the By Value field to have the filter display CableCARD modules with MAC addresses that match any portion of the text entered in this field. **Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons.	If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules with any of the following MAC addresses: ■ **AA:BB**:CC:EE:DD:FF ■ CC:**AA:BB**:CC:DD:EE ■ CC:FF:FF:DD:**AA:BB** **Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above.

Host MAC Address	Enter any part of a Host MAC address in the By Value field to have the filter display CableCARD modules paired with hosts whose MAC addresses match any portion of the text entered in this field. **Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons.	If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts that have any of the following MAC addresses: ■ **AA:BB**:CC:EE:DD:FF ■ CC:**AA:BB**:CC:DD:EE ■ CC:FF:FF:DD:**AA:BB** **Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above.
Vendor ID **Note:** The Vendor ID consists of the first three digits of a Host ID. These first three digits are used to identify the manufacturer (or vendor) of the host device.	Enter the Vendor ID for a host device in the By Value field to have the filter display CableCARD modules whose hosts have the same vendor ID. **Note:** Enter only numbers in this field.	If you enter **0-38** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts whose Host IDs begin with 0-38. Example: Any of the following Host IDs might be found: ■ **0-38**0-000-022-331 ■ **0-38**0-000-022-141

CCard Binding	■ **Active Binding** - Only those CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the ISDS. ■ **Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast by the ISDS. ■ **Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content. ■ **Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content. ■ **Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content. **Note:** For more information on revoked hosts, see ***Certification Revocation List*** (see "***Maintain CRL***" on page 211).	

CCard ID	Enter any part of a CableCARD ID in the By Value field to have the filter display CableCARD modules with IDs that match any portion of the text entered in this field.	If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with CableCARD IDs that contain this number. Example: The Filter would find any of the following CableCARD IDs: ■ **0-010**-670-850-691 ■ 0-011-028-3**00-10**8 ■ 0-011-039-01**0-010**
Host ID	Enter any part of a Host ID in the By Value field to have the filter display CableCARD modules with Host IDs that contain the number you have entered. **Note:** Enter only numbers in this field.	If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with Host IDs that contain this number. Example: The Filter would find any of the following Host IDs: ■ **0-010**-670-186-813 ■ 0-380-0**00-10**0-251 ■ 0-380-0**00-10**8-460

Information Needed to Filter

The data you need depends on the type of search you want the Filter to perform. The Filter can search for any of the following CableCARD module/host pair parameters:

- CableCARD MAC address
- Host MAC address
- Vendor ID (The prefix consists of the first three digits of the Host ID. However,you can enter up to 13 digits and the system will search for hosts with IDs that match the digits that begin with the digits you entered.)
- CableCARD ID
- Host ID
- CableCARD binding status
  - **Active Binding** - Only those CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the DNCS.
  - **Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast

by the DNCS.

- **Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content.
- **Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content (that is, unprovisioned), or have been deauthorized for copy-protected content.
- **Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content.

Filter CableCARD Modules

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > Filter

Follow these instructions to use the Filter to display specific CableCARD modules in your system.

1. Click the **By Field** arrow and select one of the following options:
   - CCard MAC Address
   - Host MAC Address
   - Vendor ID
   - CCard Binding
   - CCard ID
   - Host ID

   Note: For a description of these options, see ***CableCARD Filter Settings*** (on page 171).
2. Information in the By Value field varies according to the selection you made in step 1. Perform one of the following actions as appropriate:
   - Click in the **By Value** field and enter data in this field.
   - Click the **By Value** arrow and select the appropriate value.

   Note: For examples of how By Value data affects searches, see ***CableCARD Filter Settings*** (on page 171).
3. Click **Show**. The Filter searches the database for the parameters you selected and displays any matches in the CableCARD Summary window.

   Notes:
   - For information about the data displayed in the CableCARD Summary window, see CableCARD Summary Data.

- You can sort the data to organize it and display exactly what you need. To sort the data, click any of these column headings and the Filter will reorder the data in ascending order according to the heading you clicked: CableCARD ID, CableCARD MAC Address, Host ID, Host MAC Address, or Host Change Count. Clicking the same heading again displays the column in descending order.

PowerKEY CableCARD Module Settings

There are a number of settings you need to be aware of when you manage CableCARD modules in the ISDS.

CableCARD Module and Host Pair Settings

Use the following fields when you manage CableCARD modules and host pairs in the ISDS.

Field	Description
CableCARD ID	The ID for the CableCARD module.
CableCARD MAC Address	The MAC address of the CableCARD module. The ISDS automatically completes this field based on the CableCARD ID you enter.
Host ID	The ID for the host associated with the CableCARD module.
Host MAC Address	The MAC address of the CableCARD host. For example, an SSC set-top or a CableCARD-ready TV. For best results, enter the **Host ID** and not the Host MAC Address.
Host Bound (Yes or No)	Determines whether the host and CableCARD module are unbound Select one of the following options: ■ **Yes:** The host is authorized to receive high-value copy-protected content. ■ **No:** The host is not authorized to receive high-value copy-protected content.

Modify CableCARD Module and Host Pair Settings

Use the following fields when you modify a CableCARD module and host pair in the ISDS.

Field	Description	Notes
Host ID	The ID for the host associated with the CableCARD module	Enter the ID for the host associated with the CableCARD module you are adding to the ISDS.
Host MAC Address	The MAC address of the CableCARD host	For example, an SSC set-top or a CableCARD-ready TV. For best results, enter the **Host ID** and not the Host MAC Address.

Host Bound (Yes or No)	Determines whether the host and CableCARD module are unbound	Select one of the following options: ■ **Yes:** The host is authorized to receive high-value copy-protected content. ■ **No:** The host is not authorized to receive high-value copy-protected content.

CableCARD Server Settings

Use the following fields when you manage a CableCARD server in the ISDS.

Field	Description
	CableCARD Server Address
IP Address	The IP address of the server that is running the CableCARD Server. Typically, this is the IP address on the ISDS that connects to the QPSKs. For example, 10.253.0.1. **Notes:** ■ Autobinding on: **IP address** ■ Autobinding off: **0.0.0.0** **Tip:** When entering IP addresses, type a period to move from octet to octet. Do *not* press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
Port Number	The port number on the ISDS that the CableCARD server will monitor for incoming CableCARD module requests. **Notes:** ■ Autobinding on: 13830 ■ Autobinding off: 0
	CableCARD Module Parameters

Authorization Time-Out Period (Hours)	The length of time the Host-CableCARD pair copy-protection authorization data is kept in the file on the BFS. Enter **2** in this field. **Notes:** ■ Negative values are not permitted in this field. ■ If you define a value greater than 2, be aware of the following issues: – The podData file can contain no more than 1500 authorization entries. During staging, a pod/host pair is added to the podData file for the amount of time defined in this field. When the Authorization Time-out Period is reached, the pod/host pair is removed from the file. – If you attempt to exceed 1500 entries during the timeout period you have defined, then pod/host pairs will be unable to bind.
DeAuthorization Time-Out Period (Days)	The number of days that the copy-protection deauthorization message for the CableCARD module/host pair is kept in the file on the BFS. Enter **30** in this field.
Maximum Key Session Period (Decaseconds)	The rate (in decaseconds for single-stream capable mode and minutes for multi-stream capable mode) that the copy protection key changes. Enter **10** in this field. **Example:** For example, typing a 10 in this field would cause the copy protection key to change once every 100 seconds for modules in single-stream mode, and 10 minutes for modules in multi-stream mode. This occurs because any CableCARD or M-Card module in single-stream mode interprets this value in decaseconds, while any M-Card module in multi-stream mode interprets this value in minutes. **Important:** Defining a rate less than 10 requires a large number of unnecessary calculations on the CableCARD. Defining a rate greater than 20 does not coincide with best security practices.
Maximum Host Change Count Allowed	The maximum number of times that a CableCARD module is allowed to autobind with a different host. When a module's Host Change Count equals this limit, it will no longer be allowed to autobind with a different host. This feature can help prevent a subscriber's unauthorized use of CableCARD modules. You can enter a value in the range from **0 to 99**. ■ Entering **0** in this field disables autobinding. ■ Entering **99** indicates that an unlimited number of autobindings can occur. This is the default setting.
RF Output	The channel over which the system delivers digital services. Select **Channel 3**.

Card Authorization Phone Number	The telephone number that subscribers call to verify that their CableCARD module was authorized. You can enter up to 20 alphanumeric characters, including spaces.
Maximum Bindings within Authorization Time-Out Period	The number of CableCARD modules and set-tops that can be bound during each staging period. The recommended value for this setting is **1500**. **Note:** This value cannot be changed from the Server Configuration window. To change this value, execute the modCCardStagingLimit script. For assistance using this script, refer to *Change the CableCARD Module Staging Limit* (part number 4020737). To obtain a copy of this publication, see ***Printed Resources*** (on page 8).

CableCARD Filter Options

The following table describes the Filter options for searching CableCARD modules.

By Field	By Value	Examples
CCard MAC Address	Enter any part of a CableCARD MAC address in the By Value field to have the filter display CableCARD modules with MAC addresses that match any portion of the text entered in this field. **Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons.	If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules with any of the following MAC addresses: ■ **AA:BB**:CC:EE:DD:FF ■ CC:**AA:BB**:CC:DD:EE ■ CC:FF:FF:DD:**AA:BB** **Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above.
Host MAC Address	Enter any part of a Host MAC address in the By Value field to have the filter display CableCARD modules paired with hosts whose MAC addresses match any portion of the text entered in this field. **Note:** This field accepts the numbers 0 to 9, the letters A to F (or a to f) and colons.	If you enter **aa:bb** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts that have any of the following MAC addresses: ■ **AA:BB**:CC:EE:DD:FF ■ CC:**AA:BB**:CC:DD:EE ■ CC:FF:FF:DD:**AA:BB** **Note:** It is not necessary to enter colons in this field. Entering **AABB** will also find the examples listed above.

Vendor ID **Note:** The Vendor ID consists of the first three digits of a Host ID. These first three digits are used to identify the manufacturer (or vendor) of the host device.	Enter the Vendor ID for a host device in the By Value field to have the filter display CableCARD modules whose hosts have the same vendor ID. **Note:** Enter only numbers in this field.	If you enter **0-38** in the By Value field, the Filter finds and displays CableCARD modules paired with hosts whose Host IDs begin with 0-38. Example: Any of the following Host IDs might be found: ■ **0-38**0-000-022-331 ■ **0-38**0-000-022-141

CCard Binding	■ **Active Binding** - Only those CableCARD module/host pairs that have been authorized to receive copy-protected content within the Authorization Timeout Period. Their authorization message is currently being broadcast by the ISDS. ■ **Active Unbinding** - Only those CableCARD module/host pairs that have been deauthorized for copy-protected content within the Deauthorization Timeout Period. Their deauthorization message is currently being broadcast by the ISDS. ■ **Bound** - All CableCARD module/host pairs that have been authorized to receive copy-protected content. ■ **Unbound** - All CableCARD module/host pairs that are not authorized for copy-protected content. ■ **Unprovisioned** - SSC DHCTs that have been batch installed, but have not yet been authorized to receive copy-protected content. **Note:** For more information on revoked hosts, see ***Certification Revocation List*** (see "***Maintain CRL***" on page 211).	

CCard ID	Enter any part of a CableCARD ID in the By Value field to have the filter display CableCARD modules with IDs that match any portion of the text entered in this field.	If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with CableCARD IDs that contain this number. Example: The Filter would find any of the following CableCARD IDs: ■ **0-010**-670-850-691 ■ 0-011-028-3**00-10**8 ■ 0-011-039-01**0-010**
Host ID	Enter any part of a Host ID in the By Value field to have the filter display CableCARD modules with Host IDs that contain the number you have entered. **Note:** Enter only numbers in this field.	If you enter **0-010** or **0010** in the By Value field, the Filter finds and displays CableCARD modules with Host IDs that contain this number. Example: The Filter would find any of the following Host IDs: ■ **0-010**-670-186-813 ■ 0-380-0**00-10**0-251 ■ 0-380-0**00-10**8-460

Manage CableCARD Modules and Hosts

Quick Path: <product-name_common> Administrative Console > <product-name_common> tab > Home Element Provisioning tab > CableCARD

From the CableCARD Summary window you can display and manage the CableCARD modules.

Add a CableCARD Module and Host Pair

Quick Path: <product-name_common> Administrative Console > <product-name_common> tab > Home Element Provisioning tab > CableCARD > Add CableCARD

Each CableCARD module must be paired with a host device in the <product-name_common> database before the host device can receive high-value, secure digital content.

Follow these instructions to add a CableCARD module and its associated host device to the <product-name_common>.

1. On the <product-name_common> Administrative Console, click the **<product-name_common>** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **Add CableCARD**. The Add CableCARD window opens.
5. Enter information as described in CableCARD Module and Host Pair Settings.
6. Click **Save**. The CableCARD Summary window opens and displays the message "CableCARD saved successfully" in the status are of the window.
7. Do you need to add another CableCARD module and host device?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Exit** to return to the <product-name_common> Administrative Console.

Modify a CableCARD Module and Host Pair

Quick Path: <product-name_common> Administrative Console > <product-name_common> tab > Home Element Provisioning tab > CableCARD > [Select CableCARD/ Host Pair] > Modify Selected CableCARD

After you save a CableCARD module and its associated host device in the <product-name_common> database, you can modify the following information about the module and host pair:

- Host device information
- Whether or not the host device is authorized to receive copy-protected content.

To modify the CableCARD module ID, delete the pair, and then re-add them with the updated information.

Follow these instructions to modify the host device information for a specific CableCARD module and host pair.

1. On the <product-name_common> Administrative Console, click the **<product-name_common>** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD.** The CableCARD Data Summary window opens.
4. Click the corresponding circle in the **Select** column to choose the CableCARD module and host device that you need to modify.
5. Click **Modify Selected CableCARD**. The Modify CableCARD window opens for that CableCARD module and host device.
6. Change the CableCARD module as described in Modify CableCARD Module and Host Pair Settings.
7. When you finish making changes, click **Save CableCARD**. The system saves the new information in the <product-name_common> database and closes the Modify CableCARD window. The CableCARD Data Summary window updates to include the new information.
8. Do you need to modify another host device for a particular CableCARD module?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **Exit All CableCARD screens** to return to the <product-name_common> Administrative Console.

Delete a CableCARD Module and Host Pair

Quick Path: <product-name_common> Administrative Console > <product-name_common> tab > Home Element Provisioning tab > CableCARD > [Select CableCARD/Host Pair] > Delete Selected CableCARD

Follow these instructions to separate (delete) a CableCARD module from its associated host device on the <product-name_common>.

1. On the <product-name_common> Administrative Console, click the **<product-name_common>** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click the corresponding circle in the **Select** column to choose the CableCARD module and host device that you want to delete.
5. Click **Delete Selected CableCARD**. A confirmation window opens asking if you are sure you want to delete the selected CableCARD module and host pair.
6. Click **OK** to confirm your decision. The question window closes and an alert window opens stating that the CableCARD module and host pair has been deleted.

7 Click **OK** to close the alert window. The CableCARD Data Summary window updates so that the deleted CableCARD module and host pair is no longer listed.

8 Do you need to delete another CableCARD module and host pair?

- If **yes**, repeat this procedure from step 4.
- If **no**, click **Exit all CableCARD screens** to return to the <product-name_common> Administrative Console.

Remove Conditional Access Services from CableCARD and M-CARD Modules

When CableCARD or M-CARD modules are taken out of service, you only need to remove the conditional access to deauthorize the services on the CableCARD or M-CARD modules. These services may be reactivated when the CableCARD or M-CARD module is returned to service. You can remove the conditional access using the billing system or the ISDS as described in the following procedure.

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

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

3 Click **DHCT**. The DHCT Provisioning window opens.

4 Select the **By MAC Address** option and type the MAC Address of the CableCARD or M-CARD module.

5 Click **Continue**. The Set Up DHCT window opens. A CableCARD or M-CARD entry appears in the DHCT Type box.

6 Click the **Secure Services** tab. The Secure Services tab moves to the forefront.

7 In the **Packages** area, select the first package in the Selected list. Scroll to the bottom of the list, hold down the Shift key, and select the last package in the list to highlight all of the packages in the list.

8 Click **Remove**. All of the packages move to the Available list.

9 In the **Options** area, select the options that are required by your internal procedures.

10 Click **Save**. Your changes are saved and all package authorizations are removed from the CableCARD or M-CARD module.

11 Click **Close**. The Set Up DHCT window closes.

Server Configuration Window

Quick Path: <product-name_common> Administrative Console > <product-name_common> tab > Home Element Provisioning tab > CableCARD > > Server Configuration

From the Server Configuration window, you can configure the CableCARD server process so that the <product-name_common> can send information to CableCARD modules.The CableCARD server provides a CableCARD module/host pair with information that allows the CableCARD module to be authorized and activated for use. The authorization process differs according to the type of system and host used.

CableCARD Server Authorization Process

The CableCARD server provides a CableCARD module/host pair with information that allows the CableCARD module to be authorized and activated for use. The authorization process differs according to the type of system and host used.

- In a **one-way system** or in a **two-way system with one-way hosts**, the CableCARD server provides the host with information that enables the host to display a message on its screen. The message prompts the subscriber to call the telephone number displayed to activate the CableCARD module.
- In a **two-way system with two-way hosts**, the CableCARD server monitors a dedicated port on the ISDS to manage incoming requests from CableCARD modules. The server handles requests in one of two ways depending upon how the MMI CP screen is configured. If the MMI CP screen is configured to display for two-way hosts (the default setting), the server provides the host with information that enables the host to display a message. The message prompts the subscriber to call the telephone number displayed to activate the CableCARD module.

On the other hand, if the MMI CP screen is not configured to display for two-way hosts, the server uses a process called autobinding to automatically authorize the CableCARD module without requiring the subscriber to telephone for authorization.

Note: To view the current settings for the MMI CP screen, see ***Displaying the Set CableCARD MMI Copy Protection Window*** (see "***View the Configure MMI Screen Data Window***" on page 221). To change these settings, see ***Configuring the CableCARD MMI CP Screen*** (see "***Configure the CableCARD MMI Screen***" on page 221).

You Need to Know

Before You Begin

Configure the CableCARD Server

1. On the <product-name_common> Administrative Console, click the **<product-name_common>** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Summary window opens.
4. Click **Server Configuration**. The Server Configuration window opens.
5. Complete the fields on the screen as described in CableCARD Server Settings.
6. Click **Save**. The system saves the new information in the DNCS database and closes the Configure Server window. The message "CableCARD Server Configuration Saved Successfully" appears in the status area of the screen.

Manually Add Devices to the ISDS

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > DHCT > Select Option > New

Devices (DHCTs and CableCARD modules) are normally added to the database through CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to add devices to the database.

Follow these instructions to manually add a device to the ISDS database.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Click **Add**. The Add DHCT window opens.
5. Enter information as described in Device Settings.
6. Click **Save**.
7. Do you need to add other devices?
   - If **yes**, repeat this procedure from step 4 for every device you need to add to the database.
   - If **no**, go to the next step.
8. Close the Set Up DHCT window and the DHCT Provisioning window.
9. Your next step is to link the devices to CVT files. Go to ***Link Devices to CVT Files*** (on page 131).

Device Settings

Use the following fields when you manage devices in the ISDS.

Field	Description
Communications tab	
Admin Status	Defines the administration status of the DHCT. Click the arrow to select one of the following options from the Admin Status list: ■ Out of Service ■ In Service One Way ■ In Service Two Way—select for CableCARD modules ■ Deployed

DHCT Type	Defines the device type you are adding. Select the device type from the drop-down list.
Boot Page	Boot page for this device (if used). Leave blank if you are using bootloader
Primary VASP Name	Primary VASP for this device. Click the arrow to select the Primary VASP Name from the drop-down list (leave blank if you are using bootloader).
S/W Table of Contents	The TOC file specific to this device type. Click **Select** to browse to the correct toc file for this device (leave blank if you are using bootloader). When you load the EMMs into the ISDS for a shipment of devices, a table of contents file (TOC file) is created and is available to your billing system. The TOC file contains the serial numbers, the MAC addresses, and the type (model and hardware revision) of all devices in the shipment.
Billing ID	Billing ID of the device.
IP Address	IP address of the DNCS server.
IPV6 Address	If you have the IPv6 feature enabled, this field displays the IPv6 address of the DHCT. It is a read-only field.
DHCT Serial Number	Serial number of the device.
Secure Services tab	
Key Certificate	Select the key certificate you are using (if any) with this device. To load the certificates from a batch file or CD, click **Load from batch CD...**.
Packages	Select the packages you want to add to the device from the **Available** list. Click **Add** to move the packages to the **Selected** list. **Notes:** ■ For a description of the available packages, click **Package Descriptions** at the bottom of the window. ■ 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 device must be authorized for that package as well. This should have been done when the device was staged.

IPPV Enable	Select this option to enable this device to receive IPPV events.
IPPV Credit Limit	Active only if you select the **IPPV Enable** option. Enter the number of IPPV credits available to the device.
Max. IPPV Events	Active only if you select the **IPPV Enable** option. Enter the maximum number of IPPV events the device is allowed to view.
DMS Enable	Select this option to allow the device to receive secure services.
DIS Enable	Select this option to help generate VOD purchases.
Analog Enable	Select this option if this device needs to display secure analog services.
Fast Refresh Enable	This option is used to send EMMs to devices during staging. For more information, refer to
Location X	Leave these fields blank or enter a **0** (zero) in each field. The X and Y coordinates are used for Blackout and Spotlight features.
Location Y	

Adding Devices

Follow these instructions to manually add a device to the ISDS database.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Click **Add**. The Add DHCT window opens.
5. Enter information as described in Device Settings.
6. Click **Save**.
7. Do you need to add other devices?
   - If **yes**, repeat this procedure from step 4 for every device you need to add to the database.
   - If **no**, go to the next step.
8. Close the Set Up DHCT window and the DHCT Provisioning window.
9. Your next step is to link the devices to CVT files. Go to ***Link Devices to CVT Files*** (on page 131).

Link Devices to CVT Files

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > Type > Add

Devices (DHCTs and CableCARD modules) are normally linked to their CVT files using the CDs that accompany the shipment of devices. However, if there are no CDs available, you should use the procedure in this section to link the devices to their CVT files.

CVT File Settings

Use the following fields when you link devices to CVT files in the ISDS.

Field	Description
DHCT Type Number	The DHCT Type number of the device that you are linking to the CVT file.
Revision	Software revision represented by the CVT files.
Org. Unit ID	The OUI portion of the device MAC address. Type **00:02:DE**.
Name	The name representing the type of device you are linking.
Vendor	Manufacturer of this device. Type **Cisco**.
S/W Table of Contents	Table of contents (TOC) file related to the CVT file. Click **Select** to browse to the correct TOC file (leave blank if you are using bootloader).
Boot Page Name	The name of the boot page associated with this device. Click the arrow to select the boot page from the drop-down list (leave blank if you are using bootloader).

Linking Devices to CVT Files

Follow these instructions to link devices to CVT files.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens.
4. Click **Add**. The Add DHCT Type window opens.

5 Enter information as described in CVT File Settings.

6 Click **Save**. The Add DHCT Type window closes.

7 Click **Exit** to close the DHCT Type List window.

8 Your next step is to configure the device image file. Go to ***Configure the Device Image File*** (on page 133).

Configure the Device Image File

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > Image > Downloadable Files tab > Add

After you link the devices (DHCTs and CableCARD modules) to their image files, you need to configure the image files.

Device Image File Settings

Use the following fields when you configure device image files in the ISDS.

Field	Description
Downloadable Files Tab	
Image ID	Specifies an image ID. Leave blank if you want the DNCS to automatically assign an image ID. **Note:** Typing a specific image ID allows you to use the same image ID for this image across multiple headends.
File	The name of the image file. Click **Browse** to select the appropriate set-top image file.
Description	Description of the image file.
DHCT Groups Tab	
Group ID	The group ID associated with this image file (if any).
Group Name	The name of the group associated with this image.
DHCT Downloads Tab	
DHCT Resource File	The resource file (settop.res) associated with this image. Click **Browse** to locate the /dvs/resapp/settop.res file.

Configuring the Device Image File

Follow these instructions to configure the device image file.

1. On the Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.

5 Click **Add**. The Add Downloadable File window opens.

6 Enter information as described in Device Image File Settings.

7 Click **Save**.

8 On the Image List window, click the **Device Groups** tab. The window updates to display device groups.

9 Click **Add**. The Add Device Group window opens.

10 Enter information as described in the Device Group section of Device Image File Settings.

11 Click **Save** and close the Set Up DHCT Group window.

12 On the Image List window, click the **Device Downloads** tab. The window updates to display device downloads configured with the appropriate type and group.

13 Click **Load DHCT Resource File**. The Load DHCT Resource File window opens.

14 Click **Browse** and select the **/dvs/resapp/settop.res** file.

15 Click **Save**.

16 Click **Add**.

17 Change the group to the Group Name assigned to this image, if necessary.

18 Click **Save**.

Create and Update CVT Groups

CVT groups allow you to separate certain devices in your service network from the general population. These devices can then receive software downloads apart from the general device population.

This section provides instructions to create CVT groups.

CVT Test Group Settings

Use the following fields when you manage CVT test groups in the ISDS.

Field	Description
Group ID	The group ID for this CVT test group. Type a unique group ID number (other than zero).
Group Name	The name of this CVT test group.
DHCT MAC Address	The MAC address of a device you want to add to the group. **Note:** Before you add a CableCARD module to the group, the module must be installed in a host and functioning correctly.

Create CVT Groups

Quick Path: ISDS tab > Home Element Provisioning tab > Image > File > New

CVT groups allow you to separate certain devices in your service network from the general population. These devices can then receive software downloads apart from the general device population.

Complete the following steps to create CVT groups for devices in the network. If you already created CVT test groups, do not complete this procedure; go to ***Update CVT Groups*** (on page 140).

Important: A device should be connected to the network within 2 hours of creating or adding it to a group. If the device is not connected within 2 hours, then the device does not receive a group assignment until the ISDS database cycles through all in-service devices. Depending on the number of devices in your system, this process could take a significant amount of time.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.

4 Click the **DHCT Groups** tab. The DHCT Groups tab opens.
5 Select **File > New**. The Set Up DHCT Group window opens.
6 Enter information as described in CVT Group Settings.
7 Click **Add**. The MAC Address of the device moves to the Associated DHCTs column.
8 Repeat steps 6 and 7 for each device you want to add to the group.
9 Click **Save**. The new group appears in the list of group descriptions on the DHCT Groups tab.

Update CVT Groups

Quick Path: ISDS tab > Home Element Provisioning > Image > DHCT Groups tab > [Group name] > File > Open

Complete the following steps to update test groups for devices in the network. If you need to add CVT groups to the ISDS, use the procedure in ***Create CVT Groups*** (on page 139).

Important: A device should be connected to the network within 2 hours of creating or adding it to a group. If the device is not connected within 2 hours, then the device does not receive a group assignment until the ISDS database cycles through all in-service devices. Depending on the number of devices in your system, this process could take a significant amount of time.

1 On the ISDS Administrative Console, select the **ISDS** tab.
2 Select the **Home Element Provisioning** tab.
3 Click **Image**. The Image List window opens.
4 Click the **DHCT Groups** tab. The DHCT Groups tab opens.
5 Select the group you want to update from the list.
6 Click **File > Open**. The Set Up DHCT Group window for the group you selected opens.
7 Evaluate the list in the Associated DHCTs list. Are the Associated devices listed correct?
   - If **yes**, click Cancel.
   - If **no**, add or remove MAC addresses of the devices (as needed), then click **Save**.

Load New Image Files onto the BFS

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > Image > Downloadable Files tab > Add

The next step is to load the image files onto the BFS. Load only the image files for the devices that you have in your system.

Important:

- If a file is used by more than one device type or device revision, you only need to add that file once.
- Unnecessary files will slow the software download. Be careful to load only those files currently required by your system. Refer to ***Delete Unused Device Types from the Database*** (on page 143) for more information.

Follow these instructions to load a new image file onto the BFS.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Click the **Downloadable Files** tab.
5. On the Image List window, click **Add**. The Add Downloadable File window opens.
6. Do you want to specify an image ID?
   - If **yes**, type a unique **Image ID**.
   - If **no**, leave the Image ID field blank, and the DNCS will automatically assign an Image ID.

   Note: Typing a specific image ID allows you to use the same name for the image ID across multiple headends.
7. In the **File** field, click **Select**. The File Chooser window opens.
8. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
9. Choose one of the following options for the Filter field:
   - **DHCTs:** Type **/dvs/resapp/xxx*rom**
   - **CableCARD modules:** Type **/dvs/cablecard/xxx*rom**

   Note: The "xxx" is part of the file name provided in the software release notes document.

   Example: For a DHCT, type **/dvs/resapp/141*rom**.
10. Click **Filter**. The directory entered becomes the working directory and a filters file list opens.

11 In the **Files** column, select the ROM file that you want to add to the list of downloadable files.

   Example: 1419pe4a7.rom

12 Click **OK**. The file path for the ROM file opens on the Add Downloadable File window.

13 In the **Downloadable File** window, copy or type the file name without the path in the **Description** field.

   Example: 1419pe4a7.rom

14 Click **Save**. The new file and file description appear in the Image List window.

   Note: If the save fails, the file may already exist in the list.

Manage Device Images

This section is an overview of configuring and downloading client software to test groups or to your device population. For a full discussion of the procedures, including all the prerequisites required before your software download, refer to *Downloading Client Application Software to ISDP Set-Tops Installation Instructions* (part number 4021172).

Note: You will need a secure GUI password to set up the image files. Obtain a secure GUI password from Cisco Services. This provides Cisco Services the opportunity to communicate known issues about the software as well as other information that may be needed before loading the software onto your network.

Delete Unused Device Types from the Database

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning > Type > [select type] > Delete

Follow these instructions to delete an unused device type from the ISDS database.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Type**. The DHCT Type List window opens, listing the device type, revision, OUI, and name.
4. Look at each entry in the list. Is the entry used in your system?
   - If **yes**, there is no need to delete this entry. Look at the next entry.
   - If **no**, or if you are not certain, continue with this procedure.
5. Select the device type you want to delete and click **Delete**. The following message appears:

   Are you sure you want to delete the current item?
6. Click **OK**.
7. Did an **Unspecified Error** message appear?
   - If **yes**, the selected device type is used in your system and you cannot delete it.
   - If **no**, the selected device type is not used in your system, and the ISDS deletes it from the database.
8. Repeat steps 4 through 7 for each device type in the DHCT Type List.
9. From the DHCT Type List window, click **Exit**. The DHCT Type List closes.

Load the settop.res File into the Database

For CVT downloads, you must install the set-top resource file (settop.vxx) that contains the device types installed in your network. The system refers to this data during the image file download assignment process to verify software compatibility with the selected device type.

1. On the ISDS Administrative Console, select the **ISDS** tab.
2. Select the **Home Element Provisioning** tab.
3. Click **Image**. The Image List opens.
4. Click **Load Device Resource File**. The Load DHCT Resource File window opens.

   Note: Though the screen only mentions DHCTs, you can load CableCARD module software using this screen.
5. Click **Select**. The File Chooser window opens.
6. Highlight the current entry in the **Filter** field and press **Backspace** to delete it.
7. Choose one of the following options:
   - If you are installing the resource file from an FTP server, type **/export/home/dncs/download/settop*** in the Filter field.
   - If you are installing the resource file from a CD, complete the following steps.

     a. Insert the CD containing the resource file into the CD drive of the ISDS. The system automatically mounts the CD to /cdrom/cdrom0 within 30 seconds.

     b. Type **/cdrom/cdrom0/settop*** in the Filter field.
8. Click **Filter**. The Selection field updates with the directory from which you selected the resource file.
9. Click **settop.vxx** in the Files column.

   Note: This file is named settop.v followed by a version number (for example, **settop.v62**). Be sure that you select the latest version of this file.
10. Click **OK**. The DHCT Resource File field in the Load DHCT Resource File window updates to display the resource file path.
11. Click **Save**. A 'Process Control file saved' message appears on the Image List window.
12. On the Image List window, click **Exit**.
13. Did you install the resource file from a CD?
    - If **yes**, type **eject cdrom** (in either the CD window or in an xterm window on the ISDS) and press **Enter**. The ISDS ejects the CD from the CD drive.
    - If **no**, you are finished with this procedure.

Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

Important: You will need a SW TOC Verification password (or secure GUI password) to complete the following steps. Contact Cisco Services to obtain a SW TOC Verification password.

1 Open an xterm window on the ISDS.

2 Type **cd /export/home/dncs/doctor** and press **Enter**.

3 Type **doctor -q** and press **Enter**. Initially, this command sends a ping command to the QAM to ensure the QAM is communicating with the DNCS. Then, a remote procedure call (RPC) request is sent to each QAM to validate that the higher-level functions in the QAM are working correctly.

4 Are all of the QAMs active in the network?

- If **yes**, go to step 5.
- If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

Example: The following is an example list of network elements that has a non-responding QAM.

```
OK:    QAM BCASTQAM1     172.16.4.201    is alive.
OK:    QAM BCASTQAM1     172.16.4.201    RPC working.
Error: QAM VODMBQAM1      172.16.4.210    is not pingable.
OK:    QAM BCASTQAM2     172.16.4.202    is alive.
OK:    QAM BCASTQAM2     172.16.4.202    RPC working.
OK:    QAM BCASTQAM3     172.16.4.203    is alive.
OK:    QAM BCASTQAM3     172.16.4.203    RPC working.
OK:    QAM VODMQAM2      172.16.4.212    is alive.
OK:    QAM VODMQAM2      172.16.4.212    RPC working.
OK:    BIG    CVLab      172.16.4.101    is alive.
OK:    TED   dncsted     192.168.1.2     is alive.
```

Important: Non-responding QAMs may have an old CVT table retained in memory. If the non-responding QAMs do not become active, then the device may attempt to download software because it is receiving conflicting information from the non-responding QAMs.

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

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

7 Click **Image**. The Image List window opens.

8 On the Image List window, click the **Device Downloads** tab. The Device Downloads window displays the different devices that have already been configured for a CVT download.

9 Click on the top of the **Group** column to sort the list of device types by group.

10 Does a configured download already exist for the device type, revision, and group that you are testing?

- If **yes**, click to highlight the download and select **Edit**.
- If **no**, go to the next step.

11 At the **File Description** field, click the down arrow and choose the new software. Go to step 12.

12 Select **Add**. The Add Device Download window opens.

13 Complete the following steps to configure the Add Device Download window for the test download.

   a Click the **Device Type** arrow and select a device that needs to receive the new software.

   b Click the **Group** arrow and select the test group.

   c Click the **File Description** arrow and select the file that corresponds to the new application platform release that you want to download.

   Note: Unless you have old or test versions still posted, there should be only one choice.

   d Click the **Download Scheduling** arrow and select **Emergency**.

   e If you are using multiple download carousels, select the appropriate **Carousel** for the image download.

14 Click **Save**.

   Note: An emergency download begins instantaneously and no barker opens to the subscriber.

   Result: The Association Verification window opens.

15 Verify that the **DHCT Type**, **Group**, and **Image File** versions shown on the Association Verification window are correct.

16 Configure the following fields on the Association Verification window:

   - **Are you SURE you want to do this?:** Type **yes**.
   - **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
   - **Password:** Type the password you received from Cisco Services.

17 Click **OK**.

   Results:

   - The Association Verification window closes.
   - The Image List window is updated with the newly defined test download schedule.
   - The software download to the device test groups begins.

18 Do you have more devices or groups to test?

   - If **yes**, repeat steps 8 through 17 for each group being tested.

     Note: Since a group can contain multiple device types, you might have multiple downloads to the same device group.

   - If **no**, in the Image List window, click **Exit** to return to the Admin Console window.

19 Open an xterm window on the DNCS.

20 Type **cd /export/home/dncs/doctor** and press **Enter**.

21 Type **doctor -q** and press **Enter**.

22 Are all of the QAMs still active in the network?

- If **yes**, go to step 21.
- If **no**, reboot any non-responding QAM. If a QAM continues to be unresponsive, then contact Cisco Services.

23 Your next step is to verify that the test device or devices downloaded software and operate as expected. Go to ***Verify that Test Devices Downloaded Software*** (on page 148) for more information.

Download Images to CVT Test Groups

This section provides instructions for downloading the software to the test groups you have created.

Important: You will need a SW TOC Verification password (or secure GUI password) to complete the following steps.

1 On the <product_name_common Administrative Console, select the **ISDS** tab and select the **Home Element Provisioning** tab.

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

3 On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.

4 Does the DHCT type, revision, and group that you are testing already exist?

- If **yes**, select the appropriate row and select **File > Open.** Go to step 6.
- If **no**, go to step 5.

5 At the **File Description** field, click the down arrow choose the new software and select Immediate in the Download Scheduling field. Then, go to step 8.

6 Select **File > New**. The Set Up DHCT Download window opens.

7 Complete the following steps to configure the Set Up DHCT Download window for the test download.

   a Click the **DHCT Type** field arrow and select a device that needs to receive the new software.

   b Click the **Group** field arrow and select the test group you created in Create and Update CVT Test Groups.

   c Click the **File Description** field arrow and select the file that corresponds to the new application platform release that you want to download.

   Note: Unless you have old or test versions still posted, there should be only one choice.

   d Click the **Download Scheduling** field arrow and select **Immediate**.

8 On the Set Up DHCT Download window, click **Save**.

Note: An emergency download begins instantaneously and no barker opens to the subscriber.

Result: The Association Verification window opens.

9 Verify that the DHCT Type, Group, and Image File versions shown on the Association Verification window are correct.

10 Configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?:** Type **yes**.
- **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password:** Type the password you received from Cisco Services.

11 Click **OK**.

Results:

- The Association Verification window closes.
- The Image List window is updated with the newly defined test download schedule.
- The software download to the ISDS test groups begins.

12 Do you have more devices or groups to test?

- If **yes**, repeat steps 3 through 11 for each group being tested.

  Note: Since a group can contain multiple DHCT types, you might have multiple downloads to the same DHCT group.
- If **no**, in the Image List window, select **File > Close** to return to the Admin Console window.

13 Your next step is to verify that the test device or devices downloaded software and operate as expected. Go to ***Verify that Test Devices Downloaded Software*** (on page 148).

Verify that Test Devices Downloaded Software

Verify that the test devices operate as expected by checking the following items.

Verify that Set-Tops Downloaded Software

- Check the diagnostic screens on the test set-top to verify that the software version is correct.
- Check the diagnostic screens to verify that all services are available.
- Verify that the IPG contains 7 days of data.
- Verify that all third-party applications are available and function as expected.
- Verify that you can successfully purchase and view a PPV event on the test set-

top.

Verify that CableCARD Modules Downloaded Software

- Verify that each host can display all authorized services.

Download Client Software to Devices

The instructions in this section provide the steps to prepare and download the application platform software release to devices using the CVT method.

Notes:

- This procedure is for downloading client software to your entire population of devices (set-tops and CableCARD modules). If you need the procedure to download only to a specific CVT group, follow the procedure in ***Download Images to CVT Test Groups*** (on page 144, on page 147).
- The file names and version numbers provided as examples in this section will probably not match the file names and version numbers you see on your system.

1. On the ISDS Administrative Console, select the **ISDS** tab and select the **Home Element Provisioning** tab.
2. Click **Image**. The Image List window opens.
3. On the Image List window, click the **DHCT Downloads** tab. The Image List window updates to display the different devices that have already been configured for a CVT download.
4. In the DHCT Type column, select the DHCT type that will receive the new software where the value in the Group column is labeled **Default**.
5. Click **File > Delete**.
6. Repeat steps 4 and 5 for each DHCT type that will receive new software.

   Note: Do *not* remove the download entries for your test groups. Leave the download entries for your test groups configured.
7. In an xterm window, type **listCVT** and press **Enter**. The listCVT report displays. Look for unused files in the report.

   Example:

```
Model Rev        OUI    IMG# Grp  Download Group  Image
Mode   DHCTs
----- ---   ----  ----  --- --------------  ------------
-----   ----

430   1.1   02DE    10       Default
VALINOR_02.02.29.00_ Emerg   -
                    9   .. (not being used)
VALINOR_02.01.25.00_
                    8   .. (not being used)
VALINOR_02.00.92.00_
```

```
-------------------------------------------------------------
--------------
Total image files being downloaded = 1
```

8 Select the **Downloadable Files** tab on the Image List window and compare the list of files displayed with the list of unused files listed in the listCVT report.

9 Select any unused file on the **Downloadable Files** tab.

Note: The new software should not be listed as unused because it is associated with a test group.

10 Click **File > Delete**.

Note: The ISDS will not allow you to delete a file that is already associated with a download.

11 Repeat steps 9 and 10 until you have deleted all unused files.

12 Select the **DHCT Downloads** tab.

13 Click **File > New**. The Set Up DHCT Download window opens.

14 Complete the following steps to configure the Set Up DHCT Download window.

a Click the **DHCT Type** field arrow and select a device that needs to receive the new software.

b Click the **Group** field arrow and select **Default**.

c Click the **File Description** field arrow and select the file that corresponds to the new application platform release that you want to download.

Note: Unless you have old or test versions still posted, there should be only one choice.

d Click the **Download Scheduling** field arrow and select either **Normal** or **Immediate**.

15 Click **Save**. The Association Verification window opens.

16 Verify that the DHCT Type, Group, and Image File versions shown on the Association Verification window are correct.

17 Configure the following fields on the Association Verification window:

- **Are you SURE you want to do this?:** Type **yes**.
- **Enter your name:** Type the name (in lowercase letters) you provided to Cisco Services when you requested the secure GUI password.
- **Password:** Type the password you received from Cisco Services.

18 Click **OK**. The system schedules the software download according to the schedule you configured earlier in this section.

19 Repeat steps 13 through 18 for each DHCT type that you want to receive the software using the CVT method.

Maintain CRL

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > CableCARD Summary window > Maintain CRL

The Maintain CRL window allows you to keep track of host devices that CableLabs has placed on its Certification Revocation List (CRL). Hosts listed on the CRL are devices that CableLabs considers to be compromised or untrustworthy. These host devices should be unbound from their CableCARD modules so that they are no longer able to decrypt copy-protected content.

Whenever CableLabs sends you a CRL, enter the hosts listed on the CableLabs CRL in the Maintain CRL window. By adding hosts to the Maintain CRL window, you keep a comprehensive list of all host devices CableLabs has identified should have their ability to decrypt copy-protected content copy-protected content revoked.

Important: In order to ensure that the CRL host devices cannot decrypt copy-protected content, you must unbind any CableCARD modules that are bound to these CRL hosts. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. In addition, all services should be removed from the module. To view list of CableCARD modules that are bound with CRL hosts, select **CableCARDs with CRL Hosts** in the upper left portion of the Maintain CRL window.

Add a Host Device to the Maintain CRL Window

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD Summary window > Maintain CRL > Add

This topic describes how to add to the Maintain CRL window the host devices that CableLabs has placed on its Certification Revocation List (CRL). CableLabs publishes the CRL periodically to notify you of devices with digital certificates that are no longer trustworthy. These host devices should have their ability to decrypt copy-protected content revoked.

Whenever CableLabs sends you a new CRL, you should add the host devices listed in the CRL to the Maintain CRL window. Adding the devices to this window ensures that you have a comprehensive list of all host devices that CableLabs has identified as having untrustworthy digital certificates. On the other hand, should CableLabs notify you that devices have been removed from the CRL, you should remove these devices from the Maintain CRL window.

Note: In order to ensure that the devices listed in the Maintain CRL window cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host. To determine if a CableCARD module is bound to a host, see ***View CableCARD Module/Host Pairs on the CRL*** (see "***View CableCARDs with CRL Hosts***" on page 213).

You Need to Know

Before You Begin

Follow these instructions to add a host device listed in the CableLabs CRL to the Maintain CRL window.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Summary window opens.
4. Click **Maintain CRL**. The Maintain CRL window opens.
5. Click **Add**. A field containing a dummy ID appears in the Host ID table
6. Click in the empty field and type the ID of the host device you want to add to the Maintain CRL window.
7. Click **Save**. The ID is added to the Host ID table and the message "CRL Item Saved Successfully" appears in the status area of the window.
8. Do you need to add another host device to the Maintain CRL window?
   - If **yes**, repeat step 5 through 7.
   - If **no**, make certain to unbind all hosts/module pairs so that the host devices you have added to the Maintain CRL window are no longer authorized to receive copy-protected content. To determine if a CableCARD module is bound to a host, go to ***View CableCARD Module/Host Pairs on the CRL*** (see "***View CableCARDs with CRL Hosts***" on page 213).

     Important: In order to ensure that the devices listed in the Maintain CRL window cannot decrypt copy-protected content, you must unbind the module and host. Until the module and host are unbound, the module will remain authorized to decrypt copy-protected content. A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.
9. Click **Exit** to return to the CableCARD Summary window.

Remove a Host Device From the Maintain CRL Window

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > CableCARD Summary window > Maintain CRL > [Select Revoked Host] > Delete

If you have inadvertently placed a host device on the CRL or if a host device is removed from the CableLabs CRL list, then you can remove the host from the Maintain CRL window. This topic describes how to remove a device from the Maintain CRL window.

Hosts listed in the Maintain CRL window should not be bound to any CableCARD modules.

You Need to Know

Before You Begin

Complete these steps to remove a host device from the Maintain CRL window.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Summary window opens.
4. Click **Maintain CRL**. The Maintain CRL window opens.
5. Select the boxes next to the host devices that you want to remove from the Maintain CRL window.
6. Click **Delete**. A confirmation window opens.
7. Click **OK**. The confirmation window closes and the list updates so that the host devices are no longer listed. The message "CRL Item Deleted Successfully" appears in the status area of the window.

   Note: Removing a host from the CRL does not cause a CableCARD module/host pair's binding status to change. Any hosts that are removed from the CRL and unbound from a CableCARD module can only be re-bound by changing the CableCARD module's Host Bound status to "Yes" in the Edit CableCARD window or by sending a billing transaction to bind the module and host. To determine if a CableCARD module is associated to a host, go to ***View CableCARD Module/Host Pairs on the CRL*** (see "***View CableCARDs with CRL Hosts***" on page 213).
8. To return to the CableCARD Summary window, click **CableCARD Summary**.

View CableCARDs with CRL Hosts

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > CableCARD Summary window > Maintain CRL > CableCARDs with CRL Hosts

Use this procedure to determine which CableCARD modules, if any, are associated (or paired) with the host devices that are listed in the Maintain CRL window.

If any hosts in the Maintain CRL window are bound to CableCARD modules, then these CableCARD module/host pairs should be unbound or deauthorized in order to prevent them from receiving copy-protected content. In addition, conditional access services should be removed from these CableCARD modules. For assistance removing services from modules, see Remove Conditional Access Services from CableCARD or M-Card Modules.

Note: A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.

Complete these steps to view a list of CableCARD modules that are bound with hosts in the Maintain CRL window.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Summary window opens.
4. Click **Maintain CRL**. The Maintain CRL window opens.
5. Click **CableCARDs with CRL Hosts**. The CableCARDs with CRL Hosts window opens and lists any CableCARD modules that are associated with CRL hosts.
6. Are any CableCARD modules listed in the CableCARDs with CRL Hosts window?
   - If **yes**, this indicates that a CRL host is bound to the modules listed in the window. As a result, the host is able to decrypt copy-protected content. Unbind the host and modules so that the host is unable to decrypt copy-protected content. In addition, these CableCARD modules should be removed from any services. For assistance removing services from modules, see ***Remove Conditional Access Services from CableCARD or M-Card Modules*** (see "***Remove Conditional Access Services from CableCARD and M-CARD Modules***" on page 214, "***Remove Conditional Access Services from CableCARD and M-CARD Modules***" on page 189).

     Note: A CableCARD module and host can be unbound by changing the CableCARD module's Host Bound status to "No" in the Edit CableCARD window or by sending a billing transaction to unbind the module and host.
   - If **no**, this indicates that no CableCARD modules are associated (or paired) with a CRL host. As a result, the host device is unable to decrypt copy-protected content.
7. To return to the CableCARD Summary window, click **CableCARD Summary**.

Remove Conditional Access Services from CableCARD and M-CARD Modules

ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > DHCT > [MAC address of CableCARD module] > Show > Edit

When CableCARD or M-CARD modules are taken out of service, you only need to remove the conditional access to deauthorize the services on the CableCARD or M-CARD modules. These services may be reactivated when the CableCARD or M-CARD module is returned to service. You can remove the conditional access using the billing system or the ISDS as described in the following procedure.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **DHCT**. The DHCT Provisioning window opens.
4. Select the **By MAC Address** option and type the MAC Address of the CableCARD or M-CARD module.
5. Click **Show**. The DHCT Provisioning window changes to include the device you searched.
6. Select the device and click **Edit**. The Edit Device window opens. A CableCARD or M-CARD entry appears in the Device Type box.
7. Click the **Secure Services** tab. The Secure Services tab moves to the forefront.
8. In the **Packages** area, select the first package in the Selected list. Scroll to the bottom of the list, hold down the Shift key, and select the last package in the list to highlight all of the packages in the list.
9. Click **Remove**. All of the packages move to the Available list.
10. In the **Options** area, select the options that are required by your internal procedures.
11. Click **Save**. Your changes are saved and all package authorizations are removed from the CableCARD or M-CARD module.
12. Click **Exit**. The Edit Device window closes.

CableCARD MMI Copy Protection Screen

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > CableCARD Summary window > MMI Screen Format

This Configure MMI Screen Data window allows you to make the following changes to the MMI Copy Protection (CP) screen that CableCARD hosts display to subscribers:

- Customize the default message that the CableCARD host displays to prompt subscribers to telephone for CableCARD authorization
- Configure the MMI CP screen to display information that is useful in verifying correct CableCARD installation
- Define the conditions under which the CableCARD host displays the MMI CP screen

CableCARD MMI Screen Data Settings

Use the following fields when you manage the MMI screen in the ISDS.

Field	Description
	MMI Options
Display MMI for bi-directional device	Determines whether or not two-way CableCARD hosts display the MMI CP screen: ■ **Disabled (no checkmark displayed - DEFAULT)** - Two-way CableCARD hosts never display the MMI CP screen. (To turn **autobinding on**, make sure that **no checkmark** is displayed.) ■ **Enabled (checkmark displayed)** - Two-way CableCARD hosts display the MMI CP screen according to the Bidirectional timeout value. (To turn **autobinding off**, make sure that the **checkmark is** displayed.)
Network failure operation -- Display CP MMI	Defines the criterion that two-way CableCARD hosts use to determine when to display the MMI CP screen: ■ **Disabled (DEFAULT)** - The host always uses the Bidirectional timeout to determine when to display the MMI CP screen ■ **Enabled** - The host displays the MMI CP screen if no network boot occurs.

Bidirectional timeout (decimal seconds)	Defines how long two-way CableCARD hosts wait to display the CP MMI screen. ■ To turn **autobinding on**, set this to **180** seconds (3 minutes). ■ To turn **autobinding off**, set this to **0**. Enter a value that defines how long two-way CableCARD hosts wait to display the CP MMI screen after the host determines that it cannot connect to the DNCS or receive a response from the ISDS. The **default setting (0)** indicates that the host should display the MMI CP immediately after it determines that it cannot connect to the ISDS or did not receive a response from the ISDS. Valid characters for this field are numerical characters in the range of 0 to 65535.
Choose Fields	
Line	Defines the line number on the MMI CP screen where this field appears. Enter a line number based on the following criteria: ■ The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen. ■ Options for this field are the numbers 0 to 16. ■ Selecting 0 indicates that the field is not to be displayed in the MMI CP screen.
Field	Lists the fields that can be displayed in the MMI CP screen. The values for these fields are obtained from the data in the CableCARD Data Summary window.
Display Label **Important:** The maximum number of characters that can be entered for any of these fields must take into account the number of characters required for both the display label and the field value. Taking the characters for the	Defines the label that displays in the MMI CP screen for the following fields. (Because each line is limited to 32 characters, the display label must take into account the number of characters required for both the display label and the field value. In cases where the field value requires many characters, you may need to shorten the display label. For example, you might configure the MMI CP screen to use the display label "Host MAC:" for the Host MAC Address field.) **Host MAC Address** - Displays the MAC address of the host Enter the MAC address of the host, based on the following criteria: ■ A maximum of 15 characters can be entered for this display label ■ The address itself requires 17 characters ■ The default label is **Host MAC:**

field's value into account is necessary because a single line on the MMI CP screen can contain a maximum of 32 characters, including the field label field value, and any blank spaces. For example, if you assign the label "Host ID:" to the Host Copy Protection ID field, and the field has a value of "0-100-331-784-015," the total number of characters used is 25.	**Host Copy Protection ID** - Displays the copy protection ID of the host	Enter the copy protection ID of the host, based on the following criteria: ■ A maximum of 15 characters can be entered for this display label ■ The ID itself requires 17 characters ■ The default label is **Host ID:**
	Cable Modem MAC Address - Displays the MAC address of the cable modem	Enter the MAC address of the cable modem, based on the following criteria: ■ A maximum of 15 characters can be entered for this display label ■ The address itself requires 17 characters ■ The default label is **CM MAC:**
	CableCARD Copy Protection ID - Displays the copy protection ID of the CableCARD module	Enter the copy protection ID of the CableCARD module, based on the following criteria: ■ A maximum of 15 characters can be entered for this display label ■ The ID itself requires 17 characters ■ The default label is **CableCARD ID:**
	Host Direction - Displays the direction of the host	Enter the host direction, based on the following criteria: ■ A maximum of 32 characters can be entered for both the Display Label and the corresponding Text. ■ The default label is **Type:**
	Host Attributes - Displays attributes of the host	Enter the host attributes, based on the following criteria: ■ A maximum of 32 characters can be entered for both the Display Label and the corresponding Text. ■ The default label is **Host Code:**.
Available Options	Defines the types of hosts (one-way or two-way) that display the following fields in the MMI CP screen.	
	Host MAC Address	Select one of the following options, based on the directionality of the host: ■ **One-Way Host** ■ **Two-Way Host**

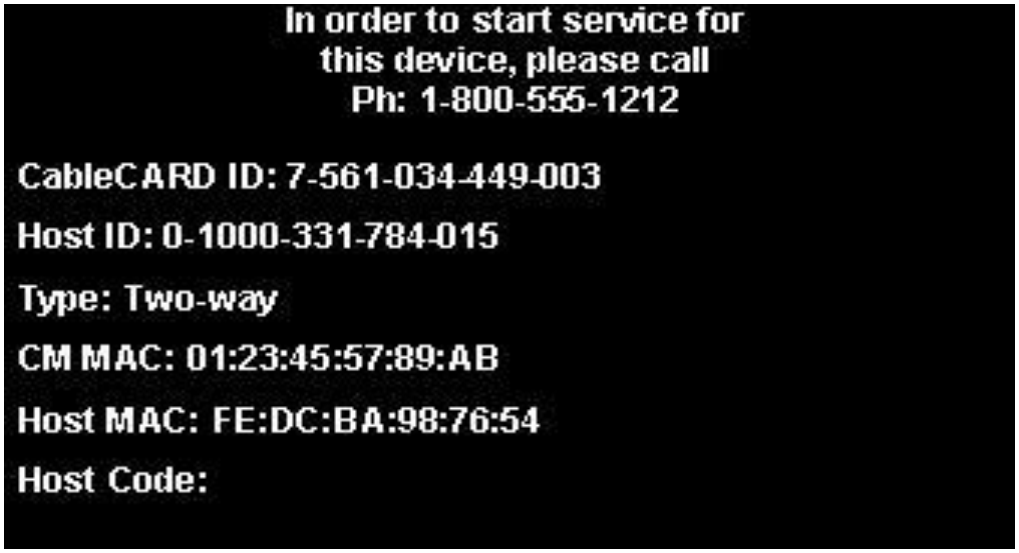
	Cable Modem MAC Address	Select one of the following options, based on the directionality of the cable modem: ■ **One-Way Cable Modem** ■ **Two-way Cable Modem**
	One-way - Defines the values that appear in the Host Direction field for one-way hosts.	You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **One-Way**.
	Two-way - Defines the values that appear in the Host Direction field for two-way hosts.	You can enter a maximum of 32 characters for both the Text field and the corresponding Display Label. The default value is **Two-Way**.
Additional Text	Settings in the following fields allow you to define custom text to be displayed in the MMI CP screen.	
	Line - Determines where on the MMI CP screen the custom text appears	Enter the line number on the MMI CP screen where custom text appears, based on the following criteria: ■ Options for this field are the numbers 0 to 16. ■ Selecting 0 indicates that no custom text is to be displayed in the MMI CP screen. ■ To display a blank line, assign a line number to a text field, but leave the text field empty. **Note:** The MMI CP screen contains 16 lines. The lines are numbered in order from the top of the screen to the bottom of the screen.
	Text - Determines the custom text	Enter the custom text to be displayed in the MMI CP screen for the selected line number. **Note:** Each line can contain a maximum of 32 characters, including marks of punctuation and blank spaces. For example, to display "In order to start service for this device, please call 1-800-555-1212." in the MMI CP screen, you would need to break the text up into a minimum of three lines because there are 70 characters in this sentence.

Default Values	The default values for lines 1 to 3: ■ Line 1 - The default value is **In order to start service for**. ■ Line 2 - The default value is **this device please call**. ■ Line 3 - The default value is taken from the **Card Authorization Phone Number** value on the Configure CableCARD Server window.

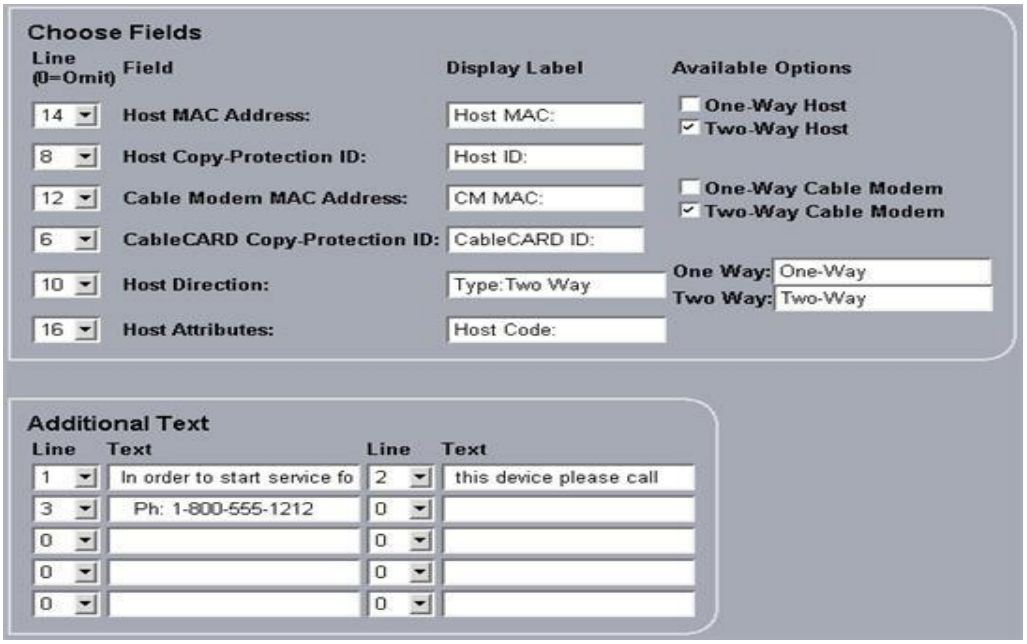
MMI Copy Protection Sample

The following example shows how MMI CP information might appear on the screen of a host device, such as a TV. The actual text that is displayed depends upon how you have configured the settings in the Set CableCARD MMI Copy Protection window.

Important: When configuring settings for the MMI CP screen, keep in mind that MMI CP information is limited to 16 lines, including any blank lines. The lines are numbered in order from 1 to 16, starting at the top of the screen. Each line can contain a maximum of 32 characters, including marks of punctuation and blank spaces. All 16 lines are used in this example.



To configure the MMI CP screen to display as shown in the above example, the following options were set as indicated:



View the Configure MMI Screen Data Window

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > System Provisioning tab > CableCARD > MMI Screen Format

This topic describes how to display the Configure MMI Screen Data window so that you can view the settings and determine if they meet the needs of your system.

Complete the following steps to display the Configure MMI Screen Data window.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Summary window opens.
4. Click **MMI Screen Format**. The Configure MMI Screen Data window opens.
5. Do the settings in this window meet the needs of your system? (For a description of the settings in this window, go to CableCARD MMI Screen Data Settings.
   - If **yes**, click **Exit** to close the window.
   - If **no**, change the settings that you desire. For assistance, go to ***Configure the CableCARD MMI CP Screen*** (see "***Configure the CableCARD MMI Screen***" on page 221).

Configure the CableCARD MMI Screen

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > MMI Screen Format

Complete these steps to replaces the default values on the CableCARD MMI CP screen with values appropriate to your site.

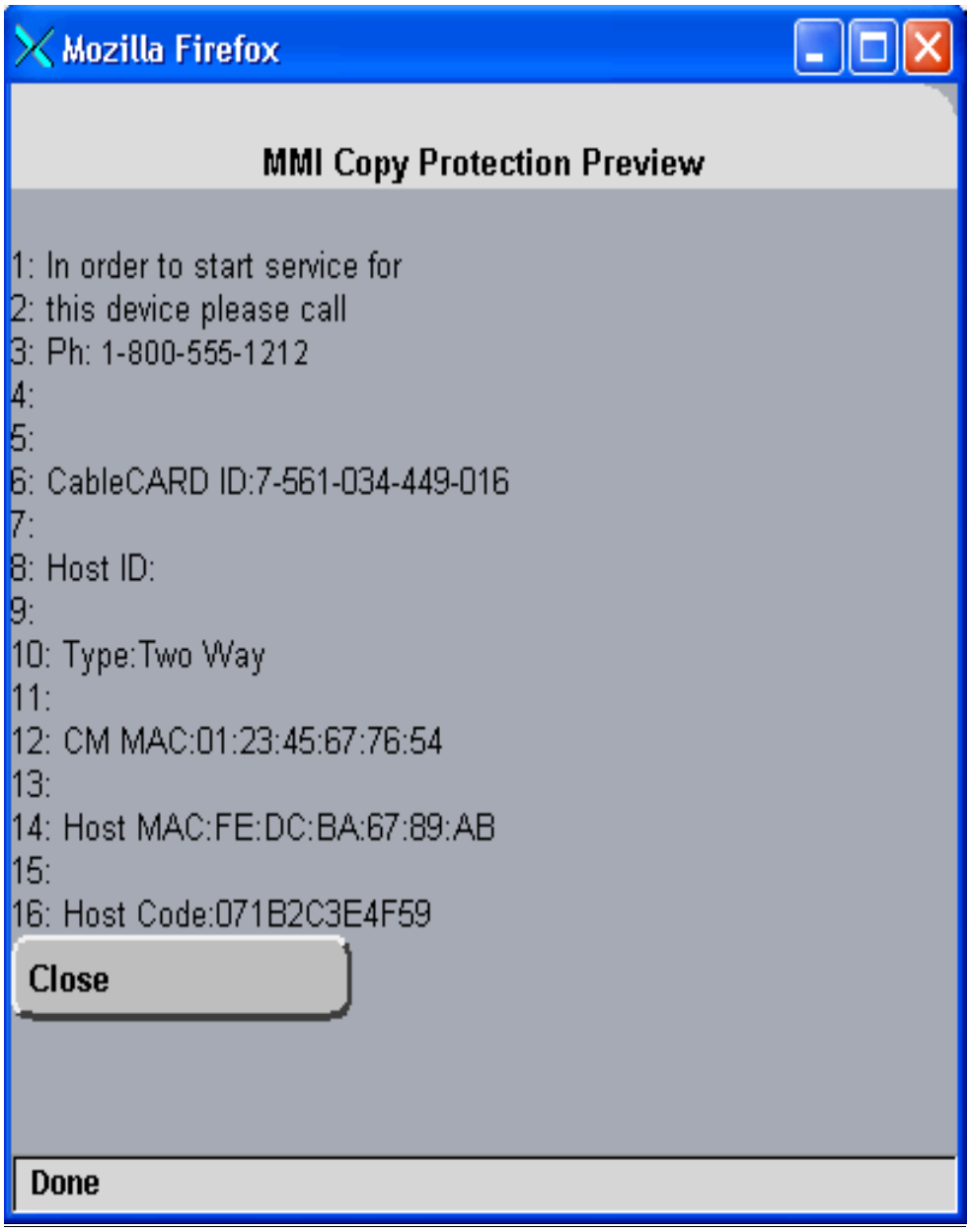
1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Home Element Provisioning** tab.
3. Click **CableCARD**. The CableCARD Data Summary window opens.
4. Click **MMI Screen Format**. The Configure MMI Screen Data window opens.
5. Complete the fields on the screen as described in CableCARD MMI Screen Data Settings.
6. To see how the MMI CP screen would display using your configuration, click **Preview**. The Sample MMI Copy Protection Data window opens and shows an example of the text that appears for each of the 16 lines in the MMI CP screen. To close this window, click **Close**.
7. Are you are satisfied with appearance of the MMI CP screen?
   - If **yes**, click **Save** to save your configuration. When a message box appears to let you know that the save was successful, click **OK** to close the message box. Once you save the changes you have made, the data is saved in the file /dvs/dvsFiles/CCardServer/CPDefinition.tbl and is put on the BFS Client under podServer/POD_Data/0/CPDefinition.tblo.
   - If **no**, repeat steps 5 through 7 to change the settings and preview your changes.
8. To close the Configure MMI Screen Data window, click **Exit**.

Previewing the MMI CP Screen

Quick Path: ISDS Administrative Console > ISDS tab > Home Element Provisioning tab > CableCARD > MMI Screen Format > Preview

From the Set CableCARD MMI Copy Protection window, you can preview how the MMI CP screen appears on the screens of CableCARD hosts. Previewing the MMI CP screen is helpful when you are configuring the MMI CP screen and want to get an idea of how the screen appears to subscribers before you save the configuration. If you don't like what you see, you can make changes to the configuration and preview the screen again. When you are satisfied with the screen's appearance, save your configuration.

To preview the MMI CP screen, click **Preview** from the Configure MMI Screen Data window. The following shows an example of the preview screen.



Authorize a Device for a Service

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

You Need to Know

Before You Begin

Time To Complete

Performance Impact

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

1. Make sure the test DHCT is connected to a television and to an RF feed into your network.
2. Make sure both the DHCT and television are plugged into a power source.
3. On the ISDS Administrative Console, click the **ISDS** 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 or CableCARD module you are testing.

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

   Tip: When entering IP addresses, type a period to move from octet to octet. Do *not* press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
7. Select the device you want to authorize and click **Edit**. The Edit DHCT window opens with the Communications tab in the forefront.
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 or CableCARD module 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 or CableCARD module must be authorized for that package as well. This should have been done when the DHCT or CableCARD module 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 or CableCARD module 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 to allow the DHCT or CableCARD module to receive secure services.
- **DIS Enable** - Enable this option. It must be enabled to help generate VOD purchases.
- **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 *Analog Descrambling Support for the Digital Broadband Delivery System Application Guide* (part number 716370) for details. To obtain a copy of this publication, see .
- **Fast Refresh Enable** - This option is used to send EMMs to DHCTs or CableCARD modules during staging. For more information, refer to *Explorer Digital Home Communications Terminal Staging Guide* (part number 734375).
- **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 or CableCARD module.

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

15 Click **Exit** to close the Edit DHCT window and return to the DHCT Provisioning window.

16 Click **Exit** 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.

Identify Error-Handling Conditions

CableCARD module errors are set by the HOST-POD Interface Standard (ANSI-SCTE 28 2001), as written and approved by the Society of Cable Communications Engineers (SCTE). Please refer to the standards document located on the Internet for the most current error-handling conditions (http://www.scte.org/documents/pdf/ANSISCTE282004.pdf).

13

IPG Collector

Introduction

The IPG collector loads IPG data from the IPG data provider's FTP site. This section describes how to set up the IPG collector and how to associate channels with the IPG collector.

In This Chapter

IPG Collector Settings

Use the following fields when you manage IPG collectors in the ISDS.

Field	Description
ID	Unique number to identify this IPG collector.
Service Provider	The provider of this IPG.
Description	A description of this IPG.
Host Name	The host of the FTP server from which the ISDS will download the IPG.
User Name	The user name associated with the FTP server.
Password	The password associated with the FTP server.
Directory	The directory on the FTP server where the IPG file is located.
File Template	The file name of the IPG file to download.
Max Long Description Length	The maximum length of the description from the IPG file.
Daily Collection Time	The time of day the ISDS will download the IPG file in the HH:MM format. Click the arrow and select either AM or PM for the time.

Set Up the IPG Collector

Quick Path: ISDS Administrative Console > Server Applications tab > IPG > File > New

The IPG collector loads IPG data from the IPG data provider's FTP site. You need to tell the Application Server where the files are located and when to download the IPG files.

1. From the ISDS Administrative Console, click the **Server Applications** tab.
2. Click **IPG**. The IPG Server List window opens.
3. Highlight **IPG_eng**.
4. Click **File > New Collector**. The Set Up IPG Collector window opens.
5. Enter information as described in IPG Collector Settings.
6. Click **Save**. A message appears that asks you to enter the FTP password.
7. Type the password and click **Continue**.
8. Click **File > Close** to close the IPG Server List window.
9. You now need to ***Associate Channels with the IPG Collector*** (on page 230).

Associate Channels with the IPG Collector

Quick Path: ISDS Administrative Console > Server Applications tab > IPG > File > Services > File > New > [IPG Provider Service name]

After you set up the IPG collector, you can designate specific channels to update using that IPG collector.

1. From the ISDS Administrative Console, click the **Server Applications** tab.
2. Click **IPG**. The IPG Servers list opens.
3. Click **File > Services**. The IPG Service List opens.
4. Click **File > New**. The Set Up IPG Service window opens.
5. Type the **IPG Provider Service** Name.

   Note: This is typically the same as the Short Description of the service.
6. Type the appropriate **SAM Service ID**.
7. Click **Save**.
8. Repeat this procedure from step 2 for any other channels you want to add to the IPG Collector.
9. Click **File > Close**. A message appears that asks if you want to update the server.
10. Choose one of the following options:
    - Click **yes** if you want the IPG Collector to run immediately (actually in about 20 minutes).
    - Click **no** if you want to wait for a maintenance window or have the update process run at the normal time the IPG Collector runs.

14

PowerKEY Conditional Access

tiIntroduction

This section describes the PowerKEY Conditional Access (CA) system, the benefits it offers to system operators, and how it works to protect secure services.

Important: Only sites that provide secure (encrypted) services to subscribers need to setup Conditional Access. If your site provides only clear (unencrypted) services, you do need to set up Conditional Access.

This section does not provide step-by-step instructions for setting up the PowerKEY CA system. Refer to the *Transaction Encryption Device FX Server Installation and Operation Guide* (part number 736138) for that information.

In This Chapter

What Is Conditional Access?

Conditional Access (CA) refers to the system, software, and components necessary to provide or deny subscribers selective access to specific services.

Because these services are available only to those subscribers who are authorized to receive them, you must encrypt these services to keep them secure from theft by unauthorized users. Consequently, these services are often called **secure** services. Our ISDS uses the PowerKEY CA system to provide secure services.

Benefits of PowerKEY CA

The PowerKEY CA system offers the following benefits to system operators:

- Enhanced encryption and decryption techniques to secure the transmission of sensitive applications, such as IPPV, Internet service, and VOD
- Increased number of secured services that can be offered to and purchased by subscribers
- Increased revenue due to the increased number of secured services offered for purchase

How Conditional Access Works

The PowerKEY CA system uses either the Transaction Encryption Device (TED) server or the TED FX server. Both servers ensure that secure applications remain secure as they are transported throughout the network. However, the TED FX server is able to encrypt more Entitlement Management Messages (EMMs) per second than the TED server.

The TED/TED FX server is connected directly to the ISDS using a short Ethernet connection. As shown in the following diagram, when the ISDS receives a request to authorize a service to a specific set-top, the ISDS generates EMMs. EMMs contain information for a specific set-top that enables that set-top to access specific secure services.

After the ISDS generates the EMMs, it sends them 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 ISDS. The ISDS then sends the encrypted EMMs through the network to the set-top.

These encrypted EMMs enable set-tops to decrypt premium broadcasts that have been encrypted to keep subscribers who have not purchased the broadcasts from accessing them. In other words, EMMs deliver the "keys" by which an authorized DHCT can access secure services.

For more information about the TED FX server and procedures for setting up the PowerKEY CA system, see the *Transaction Encryption Device FX Server Installation and Operation Guide* (part number 736138).

Set Up PowerKEY Conditional Access

For specific instructions on installing the TED, installing the TED files, initializing the PowerKEY CA system, and supporting the TED server, refer to *Transaction Encryption Device 3.0 Installation and Operation Guide* (part number 4031371).

15

Daylight Saving Time (DST)

Introduction

Setting up the right DST rules enables the set-tops in your system to automatically adjust to changes in DST observance. After creating a rule for a particular zone, apply the rule to one or more hubs. set-tops will then use the rule of the hub to which they belong.

In This Chapter

Overview

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > DST

From the Set Daylight Saving Time Rules window, you can create, change, and delete daylight saving time (DST) rules that can be used by set-tops in different DST zones. The Set Daylight Saving Time Rules window allows you to define how DST is observed in a specific DST Zone ID and indicate when the ISDS broadcasts this information to set-tops in the DST zone.

Important:

- To enable the set-tops in your system to adjust for DST, you must first create a DST rule for a particular zone and then you must apply the correct rule to each hub;otherwise, unexpected results can occur.
- We strongly recommend that you configure the DST Rules more than 30 days before the time change. The ISDS will broadcast the DST rules to the set-tops within 30 days of the DST start and end times that you specify in the DST Rules window. However, you can add DST rules as necessary at any time. If you add DST rules within the 30-day window, the ISDS will broadcast the rules to the set-tops immediately.
- Once you set up a DST rule, that rule remains in effect for each subsequent year; you should not need to adjust the rule unless you upgrade your system release (SR) software.

Note: If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However, you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to ***Modify a Hub*** (on page 23).

Default DST Rules

When you open the Set Daylight Savings Time Rules window for the first time, it will be blank. If no data appears in the fields, a DST rule has not been created and set-tops use their default DST rules (the time moves forward 1 hour on the first Sunday in April, and back 1 hour on the last Sunday in October).

DST Settings

Use the following fields when you manage DST rules in the ISDS.

Field	Description
Daylight Saving Time Zone ID	ID of the DST zones that the ISDS uses. The following values are available: ■ US - United States of America ■ UK - United Kingdom of Great Britain and Northern Ireland ■ Europe - All countries of Europe except the United Kingdom of Great Britain and Northern Ireland ■ Australia - All states and territories in the Commonwealth of Australia. ■ Local DST Zone - Used for all other countries and territories, except as noted below **What if my country or territory isn't listed?** If an area you serve follows the same DST observance as a country or territory in the DST Zone ID list (US, Europe, Australia, and UK), select that territory from the DST Zone ID list. **Example:** If you serve a Canadian province that follows the same DST observance as the United States of America, select US to define a DST Zone ID rule for that province. If an area you serve does not follow the DST observance of a territory in the DST Zone ID list, select **Local DST Zone** for the Zone ID.
Daylight Saving Time Offset (minutes)	The time shift (in minutes) relative to standard time. **Example:** If daylight saving time is one hour ahead, you would enter **60** in this field. If you enter a 0 (zero) in this field, it indicates that the associated DST rule will be ignored and not applied to the associated DST Zone ID. **Note:** This field accepts any positive number from 0 to 1439.
Effective Year	The year the DST rule becomes effective.
Daylight Saving Time Start and End Settings in this area define how DST is applied in that DST Zone ID. **Important:** All DST rules (except those created for the Australia Zone ID and Local Zone ID) must be applied to the same year.	
Start: Month	The month the DST rule begins.
Start: Day	The day the DST rule begins.
Start: Day Rank in Month	The day of the month the DST rule begins. **Example:** The first, second, third, fourth, or last Sunday of the month.

Start: Hour	The hour the DST rule begins. **Note:** The hours are displayed in 24-hour time format. **Example:** 10:00 PM is listed as **22**.
Start: Minute	The number of minutes after the Start Hour the DST rule begins.
End: Month	The month the DST rule ends.
End: Day	The day the DST rule ends.
End: Day Rank in Month	The day of the month the DST rule ends. **Example:** The first, second, third, fourth, or last Sunday of the month.
End: Hour	The hour the DST rule ends. **Note:** The hours are displayed in 24-hour time format. **Example:** 6:00 PM is listed as **18**.
End: Minute	The number of minutes after the Start Hour the DST rule ends.

Broadcast Start

Settings in this area define when the ISDS broadcasts this rule to set-tops that reside in the DST Zone ID.

Important: Broadcast Start Time can begin no more than 30 days before the start of the DST rule.

Year	The year the ISDS begins broadcasting this rule to set-tops.
Month	The month the ISDS begins broadcasting this rule to set-tops.
Day	The day the ISDS begins broadcasting this rule to set-tops.
Day Rank in Month	The day of the month the ISDS begins broadcasting this rule to set-tops. **Example:** The first, second, third, fourth, or last Sunday of the month.
Hour	The hour the ISDS begins broadcasting this rule to set-tops. **Note:** The hours are displayed in 24-hour time format. **Example:** 8:00 PM is listed as **20**.
Minute	The number of minutes after the Start Hour the ISDS begins broadcasting this rule to set-tops.

View a DST Rule

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > DST > [Select DST Zone ID]

By displaying a DST rule in the Set DST Rules window, you can quickly verify that the settings are correct.

Note: If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However, you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to ***Modify a Hub*** (on page 23).

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Set Daylight Saving Time Rules window opens.
4. Click the **DST Zone ID** arrow and select the ID of the zone whose settings you want to view. The window updates and displays the settings of the DST Zone ID that you selected.

   Note: If no data appears in the fields, a rule has not been created for this DST Zone ID, and set-tops in this zone use their default DST rules. To create a rule for this DST Zone ID, go to ***Create a DST Rule*** (on page 243).
5. To view the settings of another DST rule, repeat step 4.
6. For an explanation of the DST fields, see ***DST Settings*** (on page 240).
7. To close the Set Daylight Saving and Time Rules, click **Exit**.

Create a DST Rule

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > DST > [Configure Settings] > Save

DST rules are typically created during a system upgrade or installation. However, as your system changes you may need to create new rules. The instructions on this page describe how create a DST rule and ensure that it is used by the appropriate hubs.

Notes:

- If the sites you serve do not observe daylight saving time, there is no need to use DST rules. However, you should verify that the hubs in your system use a DST Zone ID setting of "No Zone. Observe Standard Time." For assistance verifying this setting and changing it if needed, go to ***Modify a Hub*** (on page 23).
- Once you set up a DST rule, that rule remains in effect for each subsequent year; you should not need to adjust the rule unless you upgrade your system release (SR) software.

Important: Make certain that Timezone and DST Zone ID settings are set correctly in the Hub Summary window. These settings must be correct because the ISDS uses them to broadcast DST data to set-tops in hubs.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Set Daylight Saving Time Rules window opens.
4. Click the **DST Zone ID** arrow and select the Zone ID for the rule that you want to create.

   Note: You must select one of the predefined Zone IDs (US, Europe, Australia, UK, or Local DST Zone) to create a DST Rule.
5. Enter information as described in DST Settings.

   Important: The Broadcast Start Time can begin no more than 30 days before the start of the DST rule.
6. Click **Save**. A message window opens and informs you that the ISDS database will be updated with the DST data you have selected.
7. Click **OK**. The message window closes and the ISDS database is updated with your changes. Set-tops receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a set-top causes it to update immediately with DST data.
8. Display the Hub Summary window and confirm that the correct settings are selected for Timezone and DST Zone ID fields. If necessary, change these settings. For assistance, go to ***Modify a Hub*** (on page 23).
9. To change settings for another DST rule, repeat this procedure from step 4.

10 To close the Set DST Rules window, click **Exit**.

Modify a DST Rule

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > DST > [Select DST Zone ID] > [Change Desired Fields] > Save

As your system changes, you may need to change a DST rule. Complete these steps to change a DST rule and ensure that it is used by the appropriate hubs.

Important: Make certain that Timezone and DST Zone ID settings are set correctly in the Hub Summary window. These settings must be correct because the ISDS uses them to broadcast DST data to set-tops in hubs.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Set Daylight Saving Time Rules window opens.
4. Is the rule that you want to change shown in the Set DST Rules window?
   - If **yes**, change the settings that you want. For information about the settings in this window, go to DST Settings.

     Important: The Broadcast Start Time can begin no more than 30 days before the start of the DST rule.
   - If **no**, display the rule whose settings you want to change. For help displaying a rule, go ***View a DST Rule*** (on page 242).
5. Click **Save**. A message window opens and informs you that the ISDS database will be updated with the DST data you have selected.
6. Click **OK**. The message window closes and the ISDS database is updated with your changes. Set-tops receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a set-top causes it to update immediately with DST data.
7. Display the Hub Summary window and confirm that the correct settings are selected for Timezone and DST Zone ID fields. If necessary, change these settings. For assistance, go to ***Modify a Hub*** (on page 23).
8. To change settings for another DST rule, repeat this procedure from step 4.
9. To close the Set DST Rules window, click **Exit**.

Delete a DST Rule

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > DST > [Select DST Zone ID] > Delete

As your system changes, you may need to delete a DST rule. Follow these instructions to delete a DST rule.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **DST**. The Set Daylight Saving Time Rules window opens.
4. Is the rule that you want to delete shown in the Set DST Rules window?
   - If **yes**, click Delete.
   - If **no**, display the DST rule that you want to delete and click **Delete**. Go to ***View a DST Rule*** (on page 242) for assistance displaying a rule.

   Result: A message window opens and asks you to confirm that you want to delete the rule.
5. Click **OK**. The ISDS removes the rule from the database and removes all settings from the fields in the window. Set-tops receive DST data within 10 to 60 minutes, depending on the size of your system. Rebooting a set-top causes it to update immediately with DST data.
6. Display the Hub Summary window and confirm that the correct settings are selected for Timezone and DST Zone ID fields. If necessary, change these settings. For assistance, go to ***Modify a Hub*** (on page 23).
7. To delete another DST rule, repeat this procedure from step 4.
8. To close the Set DST Rules window, click **Exit**.

16

Regional Control System (RCS)

Introduction

The Regional Control System (RCS) allows operators to control remote headend sites from a central ISDS.

If you are using our Regional Control System (RCS), you have the ability to provision and manage remote sites from a central ISDS and Application Server. Because all system provisioning and management is done from a central ISDS, there is no need for system managers to be physically located at remote sites.

This section describes the setup and configuration of a typical RCS network.

In This Chapter

RCS Topology

To communicate with remote sites, the ISDS and Application Server use a 1.5 Mbps data link to route information to remote sites.

From each remote router, information is passed on to a Remote Network Control Server (or RNCS), which stores data received from the ISDS in persistent storage and cache. Each RNCS then connects to the elements of the remote digital broadband delivery system in much the same way that the elements of a standard IP network connect to an ISDS. In fact, it may help to think of an RNCS as a remote ISDS with no user interface.

Note: You might also hear an RNCS referred to as a LIONN, or Lights Out Network Node because an RNCS has no operator lights and is a node on the RCS network.

RCS Settings

This section contains information on the settings required to manage an RCS.

RCS Remote Site Settings

Use the following fields when you manage a remote site in an RCS.

Field	Description
Site Name	The name for the site. You can use up to 15 alphanumeric characters. **Example:** If your site is located in Denver, Colorado, you might enter **Denver**. **Note:** Be sure to use a name that is consistent with the naming scheme used on your network map.
Site ID	A unique number to identify this site. Use any number 2 or greater. **Important:** Make sure that each site ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to change this field later.
Site IP Address	The IP address of the RNCS/LIONN at the remote site. Be careful to properly place the dots (.) between numbers. **Tip:** When entering IP addresses, type a period to move from octet to octet. Do *not* press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.
Site Multicast Flow IP Address	The site-wide multicast IP address. Be careful to properly place the dots (.) between numbers. For more information on the flows in the ISDS, see ***Flows*** (on page 569).
Site MAC Address	The MAC address of this RNCS/LIONN.
BFS MAC Address	A number that represents the BFS MAC address of the site you are adding, based on the following criteria: ■ Each address must be unique. ■ The central ISDS site always uses an address of 00:00:00:00:00:00. ■ If you are adding a remote site, use a similar, but unique address that incorporates the ID site ID. **Example:** If you are adding the first remote site, you might use the number 00:00:00:00:00:02 to represent the BFS MAC address of the first remote site.

Online	Determines whether this site is active or inactive.

Billing Reference Settings

Use the following fields when you manage billing references in an RCS.

Important: Be careful entering information in these fields. After a billing reference is created, you cannot modify these fields. You can only delete the billing reference and add it again using new information.

Field	Description
Select	Allows you to select the billing reference.
Billing ID	A unique number to identify this billing reference. Type any number 2 or greater that you will use to identify the billing system for each site. **Important:** Make sure that each billing ID is unique. In addition, be sure to use a number that is consistent with the numbering scheme used on your network map. **Example:** You might have the billing ID match the Site ID.
Site Name	The site associated with this billing reference.

RCS Headend Settings

Use the following fields when you manage an RCS headend.

Field	Description
Headend ID	The number you will use to identify this headend. You can use any number between 1 and 2147483647. **Important:** ■ Be sure to use a number that is consistent with the numbering scheme used on your network map. ■ You will not be able to modify this field later.
Headend Name	The name you will use to identify this headend (for example, **HE1**). You can use up to 15 alphanumeric characters. **Example:** If this headend is the first headend in Denver, you might use **Dnvr_HE1**.
Site Name	The site this headend is associated with.

RCS Hub Settings

Use the following fields when you manage a hub in an RCS headend.

Field	Description
Hub Name	The name you will use to identify this hub. You can use up to 15 alphanumeric characters. **Example:** If this hub is in Headend 1, which is in the Denver site, you might use **Dnvr_HE1_Hub1**.
Hub ID	The number you will use to identify this hub. You can use up to eight digits. **Important:** Be sure to use a number that is consistent with the numbering scheme used on your network map. You will not be able to modify this field later.
Headend	The headend where this hub is located.
Hub Multicast IP Flow	The unique multicast IP address associated with the flow through this hub. For more information on the flows in the ISDS, see ***Flows*** (on page 569).
Source IP	The IP address of the ISDS (dncsatm) that controls this hub.
Time Zone	The time zone used where this hub resides.
DST Zone ID	If this hub resides in an area that uses daylight saving time, select the appropriate DST Zone ID. **Notes:** ■ For more information on DST Zone ID, see the DST Zone ID field in Fields in the DST Rules window. ■ For more information on DST rules, see Set Daylight Saving Time Rules Window. ■ To manage time correctly on your network, you must install the Digital System Time Kit, if not installed previously. Refer to *DBDS System Time Installation and Maintenance Guide* (part number 4011510) for more information. To obtain a copy of this publication, see ***Printed Resources*** (on page 8).

RCS VASP Entry Settings

Use the following fields when you manage a VASP entry in an RCS.

Field	Description
VASP Type	Only displays when adding or editing a VASP entry. The type of VASP entry you need to add. Select **General** for a VOD server or if you do not see the specific VASP type you need. **Note:** This field is not editable. You can only access this field when creating a VASP entry.
ID	A unique number that you will use to identify this VASP entry. You can use up to 10 numeric characters. Use 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 VOD 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 a VOD service. **Note:** This field is not editable. You can only access this field when creating a VASP entry.
Name	The name of this VASP entry. You can use up to 80 alphanumeric characters. Use 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. **Example:** A name of **VODhub1Q43** would represent a VOD server on Hub 1 that uses the QAM modulator whose IP address ends in 43.
IP Address	The IP address for the server associated with this VASP entry based on your network map. **Tip:** When entering IP addresses, type a period to move from octet to octet. Do *not* press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window. **Note:** This field is not editable. You can only access this field when creating a VASP entry.
Status	Determines whether this VASP is activated. Select **In Service** to activate this VASP.
Site ID	Only displays if you are using an RCS. Determines which RCS site has access to this VASP entry.

Set Up RCS Elements

When setting up RCS elements, you will set up many of the network elements that you are already familiar with. In addition to setting up those elements, you will also set up elements that are unique to an RCS configuration.

Note: For an overview of elements in a typical network, see Network Overview.

Add a Remote Site to an RCS

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS > Site Summary > Add Site

Important: Follow this procedure only if you use an RCS.

If you are using a Regional Control System (RCS), the first step in setting up the elements in an RCS is to set up each site remote site that the RCS will manage.

You can add up to 24 sites to your RCS. You need to set up one remote site for each RNCS in your network. You do not need to set up a central site for your ISDS because the system automatically creates one for you.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Add Site**. A new row appears in the Site Summary window.
5. Complete each field of the new row based on the information in RCS Remote Site Settings.

   Tip: If you are adding several sites at once, you may find it easier to copy information from one field, paste it to another, and modify the information you have pasted.
6. Click **Save**. The system displays the message "Site data update completed."

   Tip: If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already in use), , follow these instructions:

   a. Click **OK** to close the message.
   b. Click **Go > Back**. The system displays the information you entered earlier in step 5.
   c. Modify this information and click **Save** again.
7. Click **OK**. The system saves information about this site.
8. Do you need to add another site?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, go to step 9.

9 Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add a billing reference to each of your sites. Go to *Add a Billing Reference to an RCS* (on page 254).
- If **no**, continue making any other changes that you need to make to your network. When finished, update your network map with the changes.

Add a Billing Reference to an RCS

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS > Site Summary > Billing References > Add Billing

Important: Follow this procedure only if you use an RCS.

After you add remote sites to the RCS, you then need to add billing references for each site (central and remote). A billing reference indicates the billing system to which each site is connected.

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

2 Click the **System Provisioning** tab.

3 Click **RNCS Sites**. The Site Summary window opens.

4 Click **Billing References**. The Billing Reference Summary opens and lists any billing IDs have been assigned to a site.

5 Click **Add Billing**. A new row appears in the Billing Reference Summary window.

6 Complete each field of the new row based on the information in Billing Reference Settings.

Important: Be careful entering information in these fields. After a billing reference is created, you cannot modify these fields. You can only delete the billing reference and add it again using new information.

7 Click **Save**. The system displays the message "Billing update completed."

Tip: If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already used), follow these instructions:

a Click **OK** to close the message.

b Click **Go > Back**. The system displays the information you entered earlier in step 6.

c Modify this information and click **Save** again.

8 Do you need to add a billing reference to another site?

- If **yes**, repeat this procedure from step 5.
- If **no**, go to step 9.

9 Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add headends to your sites. Click **Exit** to close the Billing Reference Summary list, then go to ***Add a Headend to an RCS Site*** (on page 255).
- If **no**, continue making any other changes that you need to make to your network.

Add a Headend to an RCS Site

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS Sites > Site Summary > Headends > Add Headend

Important: This procedure can be used only for an RCS. If you do not use an RCS, follow the procedure in ***Add a Headend*** (on page 19) to add a headend to your system.

After setting up billing references for the sites to your RCS, add headends in each of the sites by following the steps given below.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens and lists all sites in the RCS network.
4. Click the **Select** button for the site where the headend is located.
5. Click **Headends**. The Headend Summary window for the site you selected in step 4 opens.
6. Click **Add Headend**. A new row containing empty fields appears in the Headend Summary window.
7. Complete each field of the new row by based on the information in RCS Headend Settings.

   Tip: If you are adding several headends at once, you may find it easier to copy information from one field, paste it to another, and modify the information you have pasted.
8. Click **Save**. The system displays the message "Headend update completed."

   Tip: If the system does not accept the save and displays a message in an Alert box (for example, if you have inadvertently entered a number that is already used), follow these instructions:

   a. Click **OK** to close the message.

   b. Click **Go > Back**. The system displays the information you entered earlier in step 7.

   c. Modify this information and click **Save** again.
9. Click **OK**. The system saves information about this headend.
10. Do you need to add another headend?

- If **yes**, repeat this procedure from step 6.
- If **no**, go to step 11.

11 Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add hubs to your RCS network. Click **Exit** to close the Headend Summary list, then go to ***Add a Hub to an RCS Site*** (on page 256).
- If **no**, continue making any other changes that you need to make to your RCS network.

Add a Hub to an RCS Site

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS Sites > Site Summary > Hubs > Add Hub

Important: Follow this procedure only if you use an RCS. If you do not use an RCS, follow the procedure in ***Adding a Hub*** (see "***Add a Hub***" on page 22) to add a hub to your system.

After you have added headends to your RCS, next add hubs. A hub is a logical element identified by a multicast IP address which set-tops join to acquire system information (SI). In the network topology, a hub belongs to a headend. A cluster belongs to a hub.

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

2 Click the **System Provisioning** tab.

3 Click **RNCS Sites**. The Site Summary window opens and lists all sites in the RCS network.

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

5 Click **Add Hub**. A new row containing empty fields appears in the Hub Summary window.

6 Complete each field of the new row based on the information in RCS Hub Settings.

Tip: If you are adding several hubs at once, you may find it easier to copy information from one field, paste it to another, and modify the information you have pasted.

7 Click **Save**. The system displays the message "Hub save completed."

8 Click **OK**. The message closes and to show the Hub Summary window.

9 Do you need to add another hub?

- If **yes**, repeat this procedure from step 5.
- If **no**, go to step 10.

10 Are you setting up RCS elements for the first time?

- If **yes**, you are ready to add the clusters for your RCS network. Click **Exit** to close the Hub Summary window, then go to ***Clusters*** (on page 26).

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

VASP Entries in an RCS

This section contains information on managing VASP entries in an RCS.

Verify the VASP Configuration in an RCS

Complete these steps to verify the VASP configuration in your RCS is correct.

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

VASP Entry Name	IP Address	Status	Site ID
Broadcast File System	10.253.0.1	In Service	1
CFSessionUI	10.253.0.1	In Service	1
GEARServer	10.253.0.1	In Service	1
HCTM Server	10.253.0.1	In Service	1
Message Server	10.253.0.1	In Service	1
MMM Server	10.253.0.1	In Service	1
OSM Server	10.253.0.1	In Service	1
mmmRemote	172.20.0.201	In Service	2

Notes:

- The VASP entries shown in this table 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.
- The Site ID of 1 in this table represents the Site ID of the central site.
- The Site ID of 2 in this table represents the Site ID of a remote site.

5. Do all of the VASP entries shown in step 4 appear in the VASP List window, does an mmmRemote entry show for each remote site in your RCS, and do all entries 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, such as for a VOD server?
   - If **yes**, go to ***Add a VASP Entry*** (on page 259).

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

7 Take your next step based on the information in your VASP List window:

- If entries are missing from your VASP List, add the missing entries. Go to ***Add a VASP Entry*** (on page 259).
- If any entries do not show a status of In Service, activate these VASP entries. Go to ***Activate a VASP Entry*** (on page 259).

8 Are you setting up the elements of your system for the first time?

- If **yes**, click **File > Close** to close the VASP List window and return to the ISDS Administrative Console.
- If **no**, click **File > Close** to close the VASP List window and return to the ISDS Administrative Console. Add the new VASP entry information to your network map.

VASP Entries Required for the Central Site

The following VASP entries are required for any central site in an RCS. 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

Important: Depending on the services your network offers, there may be more VASP entries listed in the DNCS. However, the entries listed above **must** be present **and** in service for the DBDS to function properly. In addition, if you are offering VOD, you must add one VASP entry for each VOD server installed in your central site. Without a VASP entry, the DNCS is unable to process signals to and from the VOD server.

VASP Entry Required for Remote Sites

One **mmmRemote** VASP entry is required for each RNCS/LIONN in an RCS. This entry is used for EAS activity at a remote site and is created manually when an RNCS/LIONN site is first set up.

Occasionally, this entry 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 an RNCS/LIONN. However, the mmmRemote entry **must** be present **and** in service for the DBDS to function properly. In addition, if a remote site offers VOD, you must add one VASP entry for each VOD server installed in the remote site. Without a VASP entry, an RNCS/LIONN is unable to process signals to and from the VOD server.

Add a VASP Entry

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

Complete these steps if you need to add a VASP entry to your RCS. For more descriptive information about VASP entries, refer to ***Verify the VASP Configuration in an RCS*** (on page 257).

Note: Systems that do not use an RCS use a different method to add a VASP entry to a non-RCS system.

Important: If you are offering VOD services, you must add one VASP entry for each VOD server installed in your network. Without a VASP entry, an ISDS or RNCS/LIONN is unable to process signals to and from the server.

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

1. On the VASP List window, click **File >New**. The Set Up VASP window opens.
2. Complete each field of the new row based on the information in RCS VASP Entry Settings.
3. Click **Save**. The system saves the VASP entry information in the ISDS database and closes the Set Up VASP window. The VASP List window updates to include the new VASP entry.
4. Do you need to add another VASP entry?
   - If **yes**, repeat this procedure.
   - If **no**, click **File >Close** to close the VASP List window and return to the ISDS Administrative Console.
5. Add the new VASP entry information to your network map.

Activate a VASP Entry

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Open > In Service option

Occasionally, a VASP entry is taken out of service, such as during maintenance or when you change server brands.

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 >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 this procedure.
- If no, click **File > Close** to close the VASP List window and return to the ISDS Administrative Console.

Modify a VASP Entry

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Open

After a VASP entry has been saved in the ISDS, 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 ISDS, using the new information.

1 On the ISDS Administrative Console, click the **ISDS** 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 > 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 and the hub where the server resides.

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 Click **Save**. The system saves the new VASP information in the ISDS 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 this procedure from step 4.
- If **no**, click **File > Close** to close the VASP List window and return to the ISDS Administrative Console.

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

Delete a VASP Entry

Quick Path: ISDS Administrative Console > ISDS tab > Network Element Provisioning tab > VASP > [VASP Name] > File > Delete

Follow these instructions to delete a VASP entry from the ISDS.

1. On the ISDS Administrative Console, click the **ISDS** 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 >Delete**. A confirmation window opens.
6. Click **Yes**. The confirmation window closes. The system removes the VASP entry from the ISDS database and from the VASP List window.
7. Delete the VASP entry from your network map.
8. Do you need to delete another VASP entry?
   - If **yes**, repeat this procedure from step 4.
   - If **no**, click **File >Close** to close the VASP List window and return to the ISDS Administrative Console.
9. Continue making any other changes that you need to make to your network.

Manage an RCS

To provide continuous, quality service to subscribers, make sure that you regularly perform maintenance for your network. See ***Maintaining Your ISDP*** (on page 377) for more information.

View the Headends in Your RCS

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS Sites > SitesSummary

Important: This procedure can be used only for an RCS.

You may want to view all of the headends in your RCS network so that you can quickly view or modify them.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Headends**. The Headend Summary window opens.
5. Click **Exit** to close the Headend Summary or Hub Summary window.

View the Hubs in Your RCS

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS Sites > SitesSummary

Important: This procedure can be used only for an RCS.

You may want to view all of the hubs in your RCS network so that you can quickly view or modify them.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **RNCS Sites**. The Site Summary window opens.
4. Click **Hubs**. The Hub Summary window opens.
5. Click **Exit** to close the Headend Summary or Hub Summary window.

View the Headends of an RCS Site

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS Sites > Sites Summary

Important: This procedure can be used only for an RCS.

You may want to view the headends of a specific site so that you can quickly view or make changes to a group of headends.

Follow these steps to view the headends of a specific site.

1 On the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **System Provisioning** tab.
3 Click **RNCS Sites**. The Site Summary window opens.
4 Click **Select** for the site whose headends you want to view.
5 Click **Headends**. The Site Summary window for the site you selected in step 4 opens.
6 From this window, you can complete any of the following tasks (see ***Regional Control System (RCS)*** (on page 247) for more information):
   - Delete a headend from this site.
   - Modify a headend that is in this site.
   - Add a headend to this site.
7 Close the Site Summary window by clicking **Exit**.

View the Hubs of an RCS Site

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > RNCS Sites > Sites Summary

Important: This procedure can be used only for an RCS.

You may want to view the hubs of a specific site so that you can quickly view or make changes to a group of hubs.

Follow these steps to view the hubs of a specific site.

1 On the ISDS Administrative Console, click the **ISDS** tab.
2 Click the **System Provisioning** tab.
3 Click **RNCS Sites**. The Site Summary window opens.
4 Click the **Select** button for the site whose hubs you want to view.
5 Click **Hubs**. The Hub Summary window for the site you selected in step 4 opens. From this window, you can complete any of the following tasks (see ***Regional Control System (RCS)*** (on page 247) for more information):
   - Delete a hub from this site.
   - Modify a hub that is in this site.
   - Add a hub to this site.
6 Close the Site Summary window by clicking **Exit**.

Verify That RCS Applications Have Registered with BFS

Quick Path: ISDS Administrative Console > Application Interface Modules tab > BFS Client > File > Select

Important: This procedure can be used only for systems using our RCS Solution.

Registering applications with the BFS is critical because the BFS provides set-tops with data they need to provide services to subscribers. The BFS is used because it provides storage for many of the files that a set-top needs but cannot store locally because of memory limitations. In a sense, you might think of the BFS as an extended hard drive for a set-top.

Applications that are standard to an RCS network and some non-standard, third-party applications automatically register with the BFS at system startup or when the BFS process is restarted. You can determine whether a third-party application has registered with the BFS client by viewing the BFS List window. Applications that appear in the BFS List window have registered with the BFS client. Because an RCS distributes BFS data to all the sites within the RCS, view the BFS List window of each site in your RCS that will use the application.

Follow these steps to verify that the applications of a specific site have registered with the BFS.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click the **BFS Client**. The Site selection window opens and lists each site in your RCS network.
3. Click the site that you want to check. The site is highlighted.
4. Select **File > Select**. The BFS List window appears for the site you selected in step 3 and displays all applications that have registered with the BFS.
5. Examine the applications listed in the BFS Client List window to verify that all RCS applications have registered with the BFS. The following applications are standard and should appear in the BFS Client List window of any site.
   - **IPG_eng** - Provides data in English for the interactive program guide (IPG).
   - **MMMAud** - Provides audio files, such as those that may accompany an Emergency Alert Message (EAM).
   - **MMMCfg** - Provides configurations of multimedia messages, such as those in Emergency Alert Messages (EAMs).
   - **bootloader** - Provides set-tops with appropriate operating system and/or applications software.
   - **camPsm** - Sends conditional access information used by the pay-per-view application.
   - **osm** - The operating system manager uses this application to load image files onto the BFS for distribution to set-tops.
   - **ppv** - Used for pay-per-view service.
   - **sam** - The Service Application Manager uses this application to define the services a site provides.
   - **sgm** - Used for service group mapping.

   Note: In addition to these servers required standard applications, a site may have other servers listed to support additional applications.

6 If any applications have not registered with the BFS, verify that the applications are authorized. Go to ***Verify That RCS Applications are Authorized*** (on page 265).

Verify That RCS Applications are Authorized

Quick Path: ISDS Administrative Console > Application Interface Modules tab > BFS Admin > File > Select

Important: This procedure can be used only for an RCS.

For an application to register with the BFS client on the DNCS, the application first must be authorized on the BFS Administration window. If you are installing a third-party application on your RCS, authorize the application from the BFS Administration window so that the application can register with the BFS client. Because an RCS distributes BFS data to all sites within the network, view the BFS Administration window for each site whose applications you want to verify.

Note: If you determine that a third-party application has not automatically registered with the BFS client, manually register the application with the BFS client by registering the application's server.

Follow these steps to verify that the applications of a specific site are authorized on the BFS Administration window.

1 On the ISDS Administrative Console, click the **Application Interface Modules** tab.

2 Click **BFS Admin**. The Site selection window opens and lists each site in your RCS network.

3 Click the site that you want to check. The site is highlighted.

4 Select **File > Select**. The BFS Administration window appears for the site you selected in step 3.

5 Click the **Servers** tab. The servers of this site that have been authorized to register with the BFS appear in the list.

6 If any servers are missing, the application has not automatically registered with the BFS client. To correct this, manually register the application with the BFS client.

17

Video on Demand (VOD)

Introduction

Video-on-demand (VOD) services make up one type of interactive services that you can offer to your subscribers through our network. Interactive services allow each subscriber to actively control how a service is used.

In This Chapter

Overview

Quick Path: ISDS Administrative Console > ISDS tab > System Provisioning tab > IP VOD

With VOD, subscribers can use their remote controls to select, purchase, and view VOD events.

After subscribers have purchased the event, the reverse path allows them to forward, reverse, pause, and play the event just as they would with a VCR.

VOD Settings

Use the following fields when you set up VOD in the ISDS.

Field	Description
VOD Type	Select the type of VOD server you are using from the drop-down list.
Manufacturer	Select the manufacturer of the VOD server you are using from the drop-down list.
Server URL	Type the IP address of the VOD server.

Setting Up VOD in the ISDS

Most of the equipment in your VOD network is third-party equipment. You will need to set that equipment up according to the directions of the manufacturer of that equipment.

However, there ISDS must know some basic information about the VOD server. Follow these instructions to set up the VOD server in the ISDS.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **IP VOD**. The VOD Applications window opens and lists all the VOD servers in your network.
4. Click **New**. A new line appears at the top of the list.
5. Complete each field of the new row based on the information in VOD Settings.
6. Click **Save**.
7. Click **Exit** to close the VOD Applications window.

18

Bandwidth Management

Introduction

When high-speed data, video, and VoIP all share the same internet connection in a home network, issues with bandwidth problems might occur.

The best solution to these kinds of problems is to use methods such as QoS (Quality of Service) to manage bandwidth. Bandwidth management controls your traffic (also known as traffic shaping) by prioritizing certain types of data and making sure that everyone gets a fair share of bandwidth.

In This Chapter

Why Bandwidth Management?

In the era of triple- and quad-play with services competing for bandwidth, bandwidth management has become an imperative. The primary objectives that a robust bandwidth management scheme should achieve are as follows:

- Optimize video bandwidth by prioritizing downstream home traffic
- Prevent oversubscription of the link
- Prevent lower priority applications from starving higher priority ones
- Reallocate bandwidth intelligently among services (high speed data, VoIP, over-the-top, and video) according to the user's needs
- Enable subscribers to use bandwidth efficiently across services (high speed data, VoIP, and video)
- Provide subscribers with useful feedback when bandwidth limits are reached

This section provides guidelines that allow you to ensure that your bandwidth management best meets your business objectives.

Bandwidth Restrictions and Sharing

To manage bandwidth effectively, you must first understand the bandwidth restrictions placed on set-tops and understand the way set-tops share bandwidth with other set-tops and services. The rules differ for homes with a single set-top and homes with multiple set-tops.

Homes with a Single Set-Top

A single set-top in a home will never join a service that requires more bandwidth than the set-top is authorized for. A single set-top follows this process for obtaining bandwidth.

1. The subscriber tunes to a channel.
2. The set-top checks the SI table for the bandwidth needed to display the program on this channel.
3. The set-top compares the bandwidth required by that channel to the amount of bandwidth allocated to the set-top by the bandwidth profile as follows:
   - If the channel requires less bandwidth than is assigned to the set-top, the set-top displays the channel.
   - If the channel requires more bandwidth than is assigned to the set-top, then the set-top displays a message that the channel cannot be displayed.

Homes with Multiple Set-Tops

In homes with multiple set-tops, active set-tops will never use more bandwidth than has been allocated to the home by the bandwidth business rule. Only one bandwidth busines rule is assigned to all set-tops in a home. A set-top in a multiple set-top environment follows this process for obtaining bandwidth.

1. The set-tops periodically register with each other using 233.126.125.17 for the multicast address and 4900 for the multicast port. The multicast address and port shown here are the default values. If you need to use a different address and port, use the ALBMP Multicast GDA and ALBMP Multicast Port fields on the System-Wide parameters window for bandwidth management. See the field descriptions for ALBMP Multicast GDA and ALBMP Multicast Port in ***Configuring the Set-Top Control Class Bandwidth*** (see "***Configure the Set-Top Control Class Bandwidth***" on page 278).
2. The subscriber tunes to a channel.
3. The set-top checks the bandwidth currently being used by the other set-tops in the home and checks the SI table for the bandwidth needed to display this program and calculates the total.
4. The set-top compares the bandwidth required by that channel to the total amount of bandwidth allocated to the set-tops by the business rule that is assigned as follows:

- If the channel requires less bandwidth than is currently available to the set-tops, the set-top displays the channel.
- If the channel requires more bandwidth than is currently available to the set-tops, then the set-top displays a message that the channel cannot be displayed.

Determining Bandwidth Requirements

Now that you understand the bandwidth restrictions for set-tops and the way set-tops share bandwidth, you must determine how you will manage the bandwidth. This is a multi-step process.

1. ***Review Your Bandwidth Requirements*** (on page 275).
2. ***Configure Bandwidth for Set-Top Control Class Data and Video*** (on page 275).
3. ***Determine the Bandwidth Business Rules Required*** (on page 276).
4. ***Create Bandwidth Packages*** (on page 277).
5. ***Create Bandwidth Management Business Rules*** (on page 277).
6. ***Authorize Set-Tops for Bandwidth*** (on page 277).

Review Your Bandwidth Requirements

Your first step in managing bandwidth is to identify how much bandwidth is available to a typical home.

From this analysis you should see patterns emerge where a few distinct groups have the same available bandwidth. You can use this information to create bandwidth business rules that accommodate the typical bandwidth usage in your network.

If each home has the same amount of bandwidth available, you need only one bandwidth business rule. In the more likely event that the total available bandwidth differs across your network, you must determine how many bandwidth business rules you need.

For example, you could configure your system with 10 Mb, 15 Mb, 20 Mb, and 25 Mb business rules.

Configure Bandwidth for Set-Top Control Class Data and Video

The second step is to look at the services and sources of traffic that compete for bandwidth and determine how to allocate the bandwidth. The typical competitors for bandwidth are high-speed data, VoIP, set-top control class data, and video services. Set-top control class data and video services both represent bandwidth used by the set-tops.

Set-Top Control Class Data Bandwidth

The set-top control class data is used for communication between the ISDS and the set-top.

You must allocate a certain amount of bandwidth for set-top control class data to ensure that the ISDS can always communicate with the set-tops. The bandwidth reserved for set-top control class data is shared by all set-tops in the home. For information on configuring set-top control class data, see ***Configure the Set-Top Control Class Bandwidth*** (on page 278).

Video Bandwidth

The video bandwidth used by set-tops can vary and is directly related to the number of set-tops and the services being accessed.

The amount of video bandwidth required increases based on the number of services being accessed simultaneously.

Examples:

- For our first example, assume you have two set-tops in the home both accessing HBO. In this scenario, only 3 Mb of bandwidth is used for video.
- In another scenario, assume you have two set-tops in the home where one is accessing HBO while the other is accessing Showtime at the same time. In this scenario 6 Mb of bandwidth (3 mb for each service) is required.
- For another example, if you have a DVR that is recording HBO while also accessing Showtime, then 6 Mb of bandwidth is required.

Thus, the amount of bandwidth you need for video is based on the number of services being accessed simultaneously.

Determine the Bandwidth Business Rules Required

The next step is to determine the bandwidth business rules you need by following these steps.

1. Determine how much total bandwidth is available to the home.
2. Subtract the amount of bandwidth used by the other services (high-speed data, VoIP, and set-top control class data) from the total amount available.
3. The amount of bandwidth left over can be used for video.

For each unique amount of bandwidth left for video, you need a business rule. In the following table, we show four home environments ranging from 10 Mb to 25 Mb of bandwidth available.

In the following table, notice that the 25 Mb home allocates 8 Mb of bandwidth to high-speed data, and the 20 Mb home allocates only 3 Mb of bandwidth to high-speed data, while leaving both homes with 15.5 Mb for video. In this example, you need three business rules for 5.5 Mb, 10.5 Mb, and 15.5 Mb of available bandwidth for video.

Total Bandwidth for Home	10 Mb	15 Mb	20 Mb	25 Mb

High-Speed Data	3 Mb	3 Mb	**3** Mb	**8** Mb
VoIP	.5 Mb	.5 Mb	.5 Mb	.5 Mb
Set-Top Control Class Data	1 Mb	1 Mb	1 Mb	1 Mb
Bandwidth Left Over for Video	5.5 Mb	10.5 Mb	15.5 Mb	15.5 Mb

Create Bandwidth Packages

The fourth step in bandwidth management is to create a package that your billing system and system operators can use to assign a business rule to the set-top(s).

The package name that you use on the ISDS *must* match the package name in the billing system. We recommend that you use package names that clearly identify the bandwidth business rules. For example, you could use 5.5 Mb, 10.5 Mb, and 15.5 Mb for package names.

For more information, see ***Creating Bandwidth Packages*** (on page 280).

Create Bandwidth Management Business Rules

The fifth step is to create bandwidth management business rules and assign the allotment of bandwidth for a business rule. You can then assign a business rule to a set-top using a package.

For more information, see ***Creating, Modifying, or Deleting Bandwidth Management Business Rules*** (on page 280).

Authorize Set-Tops for Bandwidth

The last step in bandwidth management is authorizing set-tops for bandwidth by assigning packages.

We recommend that you have the billing system assign the bandwidth management package to set-tops.

If you want to test your bandwidth management configuration, you can manually assign a bandwidth management package to a set-top(s) and test the configuration. See ***Test the Bandwidth Management Configuration*** (on page 281).

Provisioning the ISDS for Bandwidth Management

This section describes how to provision the ISDS for bandwidth management.

Configure the Set-Top Control Class Bandwidth

To configure the set-top control class bandwidth for your system, you must define some system-wide parameters, the minimum overhead bandwidth, the maximum control class traffic, and the multicast address and port that the set-tops will use to communicate with each other.

Set-Top Control Class Bandwidth Settings

Use the following settings when you manage the set-top control class bandwidth.

Field	Description
Video Class DSCP	The Video Class Differentiated Services Code Point (DSCP) is a 5-digit value that the originator of the traffic encodes in the 8-bit TOS field of an IP header to classify the traffic. All video class traffic to set-tops is DSCP-marked and routers are configured to handle congestion based on DSCP markings of traffic. Routers use this DSCP value to discriminate the type of traffic and assign a priority to the traffic. For example, VoIP traffic is given a higher priority than video class traffic. When a router sees an IP header with a DSCP value for VoIP that data is given a higher priority than an IP header with a DSCP value for video class traffic. **Default Value:** 0x20
Control Class DSCP	The Control Class DSCP is a 5-digit value that the originator of the traffic encodes in the 8-bit TOS field of an IP header to classify the traffic. All control traffic to set-tops is DSCP-marked and routers are configured to handle congestion based on DSCP markings of traffic. Routers use this DSCP value to discriminate the type of traffic and assign a priority to the traffic. For example, video traffic with a DSCP value of 0x20 is given a higher priority than control class traffic with a DSCP value of 0x18. **Default Value:** 0x18
Minimum Bandwidth Overhead for ISDS (bps)	The minimum video bandwidth that is reserved for BFS, cluster flow data, such as EAS messages, and other important data that you want to ensure gets delivered.

Maximum Control Class Traffic per STB (Kbps)	The maximum control class traffic bandwidth that you allot for the various types of control class data: ■ ISDS - Control class traffic from the ISDS to the set-top (for all set-tops). ■ CDS - VOD sessions control class traffic (for set-tops that use VOD) ■ MIDAS - VOD Navigation Catalog (for set-tops that use VOD) ■ Widevine - Conditional Access (for set-tops that use Widevine conditional access) ■ SRM - VOD back office The sum of the values that you enter for Maximum Control Class Traffic per STB (Kbps) populates the Control Class BW (Mbps) field on the Bandwidth Management Business Rules screen.
ALBMP Multicast GDA	Application Layer Bandwidth Management Protocol (ALBMP) Multicast Group Destination Address (GDA). The multicast destination address used for set-tops to communicate within the home LAN. **Default Value:** 233.126.125.17 **Note**: We recommend you use the default value.
ALBMP Multicast Port	ALBMP Multicast Port. The port number used by ALBMP multicast traffic for set-tops to communicate within the home LAN. **Default Value:** 4900 **Note**: We recommend you use the default value.

Configuring the Set-Top Control Class Bandwidth

To configure the set-top control class bandwidth for your system, complete the following steps.

1. From the ISDS Administrative Console, select **Sys Config** to display the ISDS System Configuration window.
2. Click the **Bandwidth Mgmt** tab to display the System-Wide parameters window for bandwidth management.
3. Complete the following fields as described in Set-Top Control Class Bandwidth Settings.
4. Click **Save**.
5. Your next step is to create packages for the bandwidth business rules. Go to ***Creating Bandwidth Packages*** (on page 280).

Creating Bandwidth Packages

Now that you have determined the bandwidth business rules you need and you have configured the set-top control class bandwidth, the next step is to create bandwidth packages that will be used to assign the appropriate business rule to the set-tops in your network.

If you need only one bandwidth package, you can use any package that is assigned to all set-tops, for example the Basic Service package. You can skip this step, and go to Assigning Video Bandwidth to Bandwidth Packages. But, in the more likely event that you will need several bandwidth packages, use this procedure to create bandwidth packages.

To create a bandwidth package, complete the following steps.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **System Provisioning** tab.
3. Click **Package**. The Package List window opens.
4. Click **File > 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.

   Note: The package name must match the packages in the billing system that will be used to assign bandwidth business rules. Cisco recommends that you use names that clearly identify the bandwidth business rules. For example, 10 Mb, 15 Mb, and 20 Mb bandwidth packages. Refer to your billing system documentation for instructions and specific information.
6. Select the **Default Staging Package** check box if this is the bandwidth package you will use as the default. All set-tops will be provisioned with this bandwidth package by default. You can specify only one bandwidth package as a staging default. For any additional bandwidth packages that you create, be sure to leave this field unchecked.
7. Select **Unlimited** for the Duration field.
8. Click **Save**.

   Results:

   - The ISDS saves the package information in the ISDS database and closes the Set Up Package window.
   - The Package List updates to include the new package.
   - If you selected this package as a default staging package, an asterisk (*) appears next to this package name in the list.

Creating, Modifying, or Deleting Bandwidth Management Business Rules

Now that you have created the bandwidth packages you need, the next step is to create bandwidth management business rules and assign the allotment of bandwidth for that business rule.

To create, modify, or delete business rules for bandwidth management, complete the following steps.

1. From the ISDS Administrative Console, click **Bandwidth Mgmt**. The Bandwidth Management Business Rules window opens.
2. Choose one of the following options:
   - To add a business rule, click **New** to add a new row. Go to step 4.
   - To modify a business rule, select the row that has the business rule you want to modify. Go to step 3.
   - To delete a business rule, select the row that has the business rule you want to delete, and click **Delete**.
3. Select the bandwidth package to which you want to assign bandwidth. The row highlights to show that it is selected.
4. In the **BW Package Name** column, use the drop-down list to select the package that will be used to identify this business rule. The row highlights to show that it is selected and a bandwidth group ID is assigned.
5. In the **Video Prog BW (Mpbs)** field, enter the maximum bandwidth associated for this business rule.
6. Click **Save**.
7. Repeat steps 2 through 6 for each business rule you want to use in your network.

Test the Bandwidth Management Configuration

Now that you have created the bandwidth packages and assigned business rules, you may may want to test your bandwidth management configuration. You can do this by setting up an environment that is similar to a home with set-tops configured so that they are competing for bandwidth.

Before You Begin

Configure Your Set-Tops

Complete the following instructions to test your bandwidth management configuration.

1. Set up a group of set-tops and configure them as if they are in a home environment competing for bandwidth.
2. On the ISDS Administrative Console, click the **ISDS** tab.
3. Click the **Home Element Provisioning** tab.
4. Click **DHCT**. The DHCT Provisioning window opens.
5. Click **Open** and select one of the following options:
   - **By MAC Address**: Enter the MAC address for the set-top.
   - **By IP Address**: Enter the IP address for the set-top.

- **By Serial Number**: Enter the serial number for the set-top.

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

7 Click the **Secure Services** tab.

8 Scroll through the **Available** list in the Packages area of the window and click to select the bandwidth package that you want the set-top to use.

9 Click **Add**. The package name you selected moves into the Selected list.

10 Click **Save**.

11 Repeat steps 3 through 10 for all set-tops that you want to test.

Test the Configuration

To ensure that your bandwidth management configuration is functioning as you intend, we recommend that you test different scenarios.

- In the first scenario, you want to verify that your set-tops can access the services using the bandwidth for which their bandwidth business rules allow. In this case, must make sure that your test does not exceed the bandwidth for which the set-tops in your test environment are authorized. For more information, see ***Subscriber Observed Behaviors*** (on page 282).
- In a second scenario, you want to exceed the bandwidth allocation for your test environment to verify that the correct conflict messages are displayed.

To test your bandwidth management configuration, complete the following steps.

1 Start accessing services. Make sure that the set-tops can access as many services as their business rules allow. If no conflict messages appear, you have configured your bandwidth correctly.

2 Access as many services as required to exceed the bandwidth allocation for the home. When the bandwidth allocation for your test environment is exceeded, you want to make sure that the correct bandwidth management conflict message appears.

Subscriber Observed Behaviors

When set-tops compete for bandwidth, conflicts will arise. Subscribers will see a barker when not enough bandwidth is available to watch all the programs they are attempting to watch.

19

Manage a Digital Emergency Alert System

Introduction

This section provides a brief overview of a digital EAS and how our ISDS helps operators comply with the FCC EAS mandate.

In This Chapter

Digital Emergency Alert System in a Typical System

For information on configuring, maintaining, or testing the EAS in a DBDS, refer to *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455). To obtain a copy of this publication, see ***Printed Resources*** (on page 8).

Because many digital systems are very large, an Emergency Alert Message could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the ISDS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, ***contact the representative who handles your account*** (see "***Contact Us***" on page 7).

Digital EAS in a System Using RCS

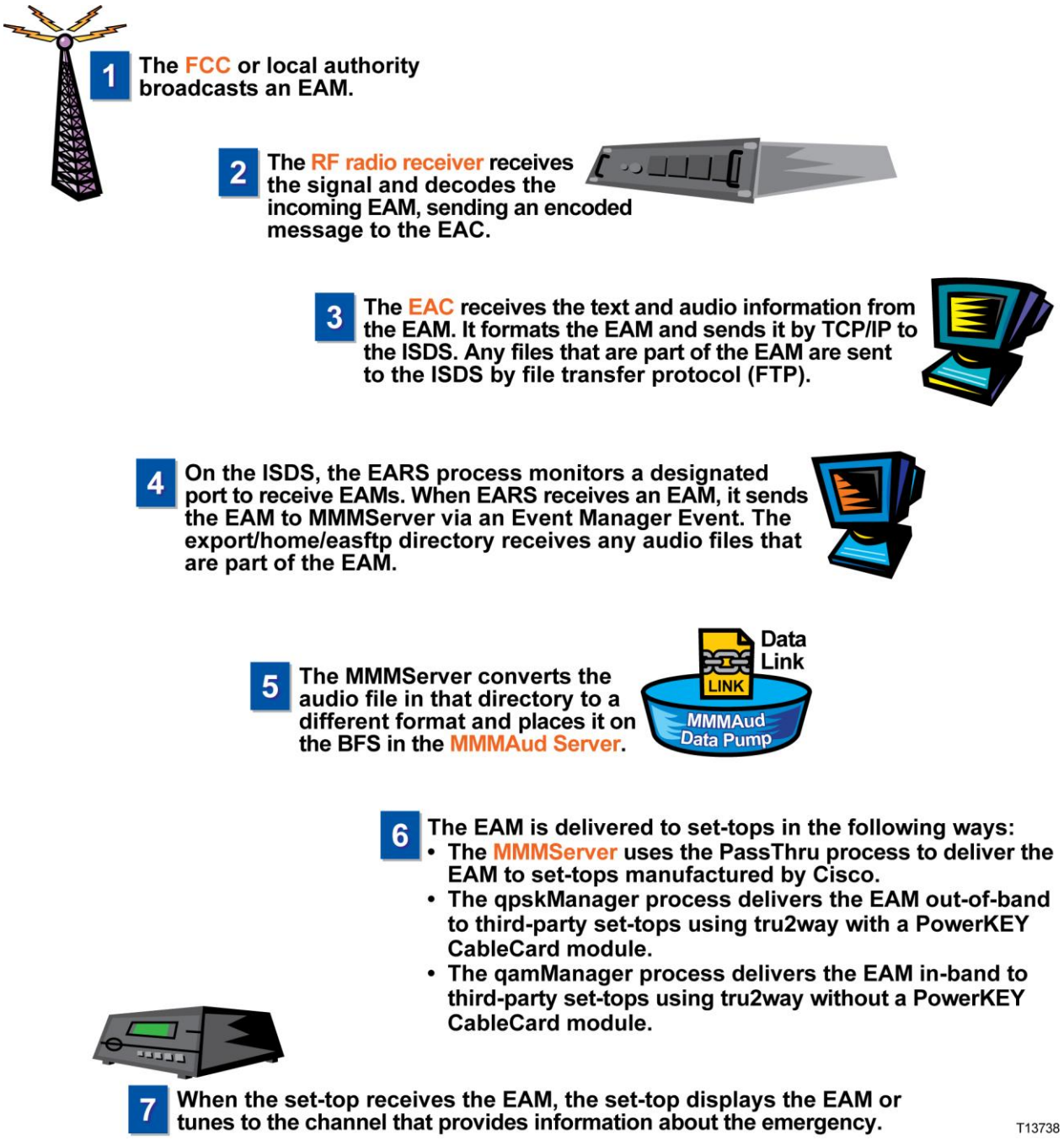
This section describes the digital EAS in a system using the LIONN/RCS.

Digital Emergency Alert System in the Central RCS Site

Important: This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic ***Digital Emergency Alert System in a Typical System*** (on page 284) describes how the digital EAS functions in a system without an RCS.

In an RCS, processes that manage EAMs reside both on the ISDS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in the **central** site, the EARS process on the ISDS sends the MMMServer process an Event EAM.

For more information on how an EAM is processed at the central site, see the following illustration. When reviewing this illustration, keep in mind that the equipment that receives the EAM—the RF receiver and the Emergency Alert Controller (EAC)—is provided by a vendor other than us.



Notes:

- To compare this with how an EAM is processed at the central RCS site, see ***EAS in a Remote RCS Site*** (see "***Digital Emergency Alert System in a Remote RCS Site***" on page 287).

- For information on configuring, maintaining, or testing an EAS in an RCS, refer to the *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).
- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the ISDS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, ***contact the representative who handles your account*** (see "***Contact Us***" on page 7).

Digital Emergency Alert System in a Remote RCS Site

Important: This process describes how the digital EAS works in a system that uses a Regional Control System (RCS). The topic ***Digital Emergency Alert System in a Typical System*** (on page 284) describes how the digital EAS functions in a system without an RCS.

In an RCS, processes that manage Emergency Alert Messages (EAMs) reside both on the ISDS and on each remote RNCS/LIONN. **Where the EAM originates** determines how the EAM is processed. When the EAM originates from an Emergency Alert Controller (EAC) in a **remote** site, it forwards the EAM on to a process on the RNCS/LIONN, which forwards the EAM on to the ISDS. Together, the ISDS and the RNCS/LIONN deliver the EAM to affected set-tops in the RCS:

- EAMs processed by the ISDS are distributed to third-party set-tops using OpenCable compliance without a PowerKEY CableCARD module.
- EAMs processed by an RNCS/LIONN are distributed to third-party set-tops that use OpenCable compliance with a PowerKEY CableCARD module and to our set-tops.

The following illustration explains in more detail the processes that are required to process an EAM. When reviewing this illustration, keep in mind that the equipment that receives the EAM—the RF receiver and the Emergency Alert Controller (EAC)—is provided by a vendor other than us.

Notes:

- To compare this with how an EAM is processed at the central RCS site, see ***EAS in the Central RCS Site*** (see "***Digital Emergency Alert System in the Central RCS Site***" on page 285).

- For information on configuring, maintaining, or testing an EAS in an RCS, refer to *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342).
- Because many digital systems are very large, an EAM could be very disruptive to a community that is not affected by a particular alert. Therefore, we offer a software product that you can purchase separately to enable the ISDS to filter and send EAMs to only targeted states, counties, or subdivisions. For more information about this software product, ***contact the representative who handles your account.*** (see "***Contact Us***" on page 7)

20

DSG Timers and Filters

Introduction

The Client Filters windows allow you to change the following settings in the global default DCD (Downstream Channel Descriptor) file, which supports basic DSG:

- **Timer Settings** - These settings define the overall amount of time a set-top's embedded cable modem waits to receive DSG packets. Timer settings can be applied to **any** system running basic DSG, including systems that use the PowerKEY® conditional access (CA) method and systems using a third-party CA method.
- **Client Filter Settings** - These settings control the provisioning of certain DSG client filter settings for set-tops that use a third-party CA system and operate in Basic DSG mode. (Unlike the timer settings, the filter settings can be applied only to systems that use a third-party CA system. They cannot be applied to systems that use the PowerKEY CA system.)

The DCD file is loaded on the BFS in the following location: BFS:///brf/default_global.dcd.

In This Chapter

Change DSG Timer Settings

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Client Filters > Configuration

Important: The DSG Timer user interface is intended for use by operators with DOCSIS network experience. If you need more detailed information on Basic DSG, please review the **DOCSIS Set-top Gateway (DSG) Interface Specification**, which you can access from the CableLabs® website (***http://www.cablelabs.com/*** (***http://www.cablelabs.com/***)).

The Client Filters user interface allows you to change any of the pre-configured timer settings in the global default DCD (Downstream Channel Descriptor) file. These settings define the overall amount of time a set-top's embedded cable modem waits to receive DSG packets. Timer settings are pre-configured with recommended default values and are applicable to **any** system running basic DSG, including systems that use the PowerKEY® CA method and systems using a third-party CA method.

Follow these instructions to change timer settings for basic DSG.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Client Filters**. The Rules for Client Filters window opens.
3. Click **Configuration**. The Configuration for Client Filters window opens.
4. Update the timer settings as necessary. The following list provides a brief description of each setting.
   - **DSG Initialization Timeout (TDSG1)** - The time the DHCT's embedded cable modem (also known as the eCM) stays on a DOCSIS channel during initialization, waiting for DSG packets to arrive from the CMTS. If DSG packets are not received within this time period, the DOCSIS channel is declared invalid, and the set-top does not lock on a particular DOCSIS channel. The default value is 2 seconds. You cannot set this timer to 0.
   - **DSG Operational Timeout (TDSG2)** - The time allowed for DSG packets to reach the set-top's embedded cable modem during normal operation. If DSG packets do not arrive within this time period, the DSG One-Way retry Timer (TDSG4) is activated. The default value for TDSG2 is 600 seconds. You cannot set this timer to 0.
   - **DSG Two-Way retry Timer (TDSG3)** - The time the set-top's embedded cable modem waits before trying to re-establish two-way connectivity with the CMTS while the embedded cable modem is in a one-way operational state. The default value is 300 seconds. You cannot set this timer to 0.

     Note: "One-way" and "Two-way" in these descriptions refer to the state of the embedded cable modem, not the operational state of the set-top.

- **DSG One-Way retry Timer (TDSG4)** - Determines how long the set-top's embedded cable modem waits to rescan for a DOCSIS downstream channel that contains DSG packets after an operational timeout occurs. If this time period expires, the DOCSIS channel is declared invalid and the DHCT's embedded cable modem will scan for another DOCSIS channel. The default value is 1800 seconds. You cannot set this timer to 0.

5 When you have finished updating the settings, click **Save**. The DCD file is updated with the values and reloaded on the BFS.

Define Third-Party Client Filters

Quick Path: ISDS Administrative Console > Application Interface Modules tab > Client Filters

Important: The Client Filters user interface is intended for use by operators with DOCSIS network experience. If you need more detailed information on Basic DSG, please review the **DOCSIS Set-top Gateway (DSG) Interface Specification**, which you can access from the CableLabs website (***http://www.cablelabs.com/*** (***http://www.cablelabs.com/***)).

The Client Filters user interface allows you to control the provisioning of certain DSG client filter settings for set-tops that use a third-party conditional access (CA) system and operate in Basic DSG mode. A client filter identifies packet characteristics (such as destination MAC address, destination IP address, and so on) with the ID of the client needing those packets. In this context, the clients are software running on set-tops operating in Basic DSG mode.

Important: Do **not** define basic DSG client filters to provision standard network flows on a PowerKEY-only system. Basic DSG filters for PowerKEY systems are already implicit in the Bridge Resolution File (BRF). The **Rules for Client Filters** window is provided for cable operators provisioning additional DSG flows, such as third-party CA systems.

Client Filter Basics

To properly configure client filters through the Client Filters user interface, it is necessary to understand the way Basic DSG DHCTs are provisioned with DSG information. The system architecture for provisioning DSG information to Basic Mode DHCTs has the following key features:

- Each hub has one or more DAVIC QPSK Modulators carrying all OOB information for the hub.
- The ISDS publishes a BRF on OOB BFS that provides the mapping of hub ID to DSG Tunnel MAC address. The BRF provides the information needed by the DHCT to locate the correct DSG OOB Bridge. This file and its contents are automatically generated by the ISDS when operators set up a CMTS bridge for multicasting. No user configuration of the contents of this file is available or necessary.
- The ISDS publishes a global default DCD file on OOB BFS. The global default DCD file communicates rules, classifiers, and DSG Configuration information to DHCTs operating in Basic DSG mode. The rules and classifiers map DSG Client IDs to packet filter settings used to acquire traffic for those clients. These filter settings are in addition to the information provided in the BRF and do not affect the DHCT DOCSIS scan behaviors. The Client Filters user interface provides a way for the operator to configure the rules and classifiers portion of the global default DCD file.

- Upon boot, DHCTs operating in Basic DSG mode first find a DAVIC QPSK Modulator to obtain the correct hub ID and read the BRF before attempting to locate a DSG OOB Bridge.
- Once a DHCT has acquired the correct DSG OOB Bridge per the BRF, it uses the client filter information in the global default DCD file to acquire traffic for applicable Client IDs supported by the DHCT. The DHCT monitors the DCD file for changes and uses the latest version available.

Third-Party Client Filter Settings

Use the following fields when you manage third-party client filters with the ISDS.

Field	Description
Client ID Type	**Broadcast ID** - Determines whether the traffic being sent to set-tops conforms to specific industry standards, such as SCTE 65, SCTE 18, OCAP Object Carousel, and OpenCable Common Download Carousel.
	Well Known MAC - Determines whether the client is identified with a six-byte MAC address.
	CA System ID - Determines whether the client is identified with a third-party CA system ID.
	Application ID - Refer to the *DOCSIS Set-top Gateway (DSG) Interface Specification* if you need information on this option.
Client ID	The corresponding ID or address: ■ If the Client ID Type is **Broadcast ID**, type the corresponding ID ■ If the Client ID Type is **Well Known MAC**, type the MAC address in the form AA:BB:CC:DD:EE:FF ■ If the Client ID Type is **CA System ID**, type the ID assigned to the set-tops (for example, 09:00 for DHCTs that receive NDS) Refer to the *DOCSIS Set-top Gateway (DSG) Interface Specification* if you need information on this option.
DSG Tunnel Address	The destination MAC address of the DSG Tunnel. If RFC 1112 compliant mapping is being used for this tunnel, check that the DHCT Tunnel Address and Destination IP Address match per RFC 1112.
Source IP Address	The IP address of the ISDS or server that originates the traffic associated with the Client ID. If this information is not required, you can type **0** or leave this field blank. **Tip:** When entering IP addresses, type a period to move from octet to octet. Do *not* press the Tab key to move from octet to octet; pressing the Tab key moves the cursor to the next field on the window.

Source IP Mask	The subnet mask of the originator of the associated IP address of the ISDS or server that originates the DSG data. If this information is not required, you can type **0** or leave this field blank.
Destination IP Address	The multicast destination IP address of the traffic associated with the Client ID.
Destination Port Start	The ports associated with the multicast destination. Complete these fields using the following guidelines. ■ To specify a single port, enter the same value in both of these fields. ■ To specify a continuous range of a few ports, enter the lower and upper values of this range. ■ If no ports are being specified, leave both fields blank.
Destination Port End	

Building the Global Default DCD File

Follow these steps to configure the filters for the global default DCD file for your system.

Important: Do not define basic DSG client filters to provision standard network flows on a PowerKEY-only system.

1. On the ISDS Administrative Console, click the **Application Interface Modules** tab.
2. Click **Client Filters**. The Rules for Client Filters window opens.
3. Click **Add Rule**. The new data fields appear.
4. Complete the fields on the screen as described in Third-Party Client Filter Settings.
5. Repeat this procedure from step 3 as needed. You can add up to 21 filters.

   Example: If you are implementing multiple industry standard flows or if you have non-contiguous port numbers, you need to add a filter for each standard or for each range of port numbers.
6. When you have finished adding all filters for the DCD file, click **Save**. The system builds the DCD file and loads this file on the BFS in the following location: BFS:///brf/default_global.dcd.

21

Other ISDS Features

Introduction

This section contains information on other ISDS features that you can implement.

In This Chapter

SD-Only Mode

This section provides instructions to configure sources to support standard-definition (SD)-Only mode.

SD-Only Mode Settings

Use the following fields when you manage the SD-only mode in the ISDS.

Field	Description
Service Name	Name of the service. **Example:** SDO Configuration.
Short Description	Required field. Enter **_SDO**
Long Description	Description of the service. **Example:** Field-Selectable SD-only Mode.
Application URL	Append the following to the directory path: **;HDMIN=<kbps>;SOC1=HD;SOC0=HD** **Notes:** ■ Replace <kbps> with the minimum HD Stream bandwidth supported by your system. ■ The SOC0=HD setting configures all single-SOC set-tops to be set to HD by default. ■ The SOC1=HD setting configures the first SOC for IPN603 set-tops to be set to HD by default. **Example:** bfs://resapp/watchtv;HDMIN=10000;SOC0=HD;SOC1=HD;SOC2=SD;SOC3=SD **Note:** This tells the set-tops that any service defined with a data rate less than 10 Megabits per second is SD.
Logo	Leave blank.
Parameter	Select the **Number** option.
Number	Enter a unique number.

Enable Support for Field-Selectable SD-Only Mode

1. From the ISDS Administrative Console, click the **Application Interface Module** tab.
2. Click the **SAM Service** button. The SAM Service List window appears.

3 Click **File > New**. The Set Up SAM Service window appears.
4 Complete the fields as described in SD-Only Mode Settings.
5 Click **Save**. The SAM service is added to the SAM Service List.
6 Click **File > Close** to close the Same Service List window.

Disable Support for Field-Selectable SD-Only Mode

1 From the ISDS Administrative Console, click the **Application Interface Module** tab.
2 Click the **SAM Service** button. The SAM Service List window appears.
3 Locate the **_SDO** service in the Short Description column and highlight it.
4 Click **File > Delete**. A prompt appears to confirm the deletion.
5 Click **Yes**. The service is deleted.

Configure the Stream Capability on a Set-Top

1 Press and hold the **OK** key on the remote control until the HD LED light is flashing on the front panel.
2 Press the down arrow key. The boot up diagnostic screen appears.
3 Press the left or right arrow key to scroll to the **Options** window.
4 Select **Stream Capability**, which will be set to either **HD Capable** or **SD_only**.
5 Complete the following steps to change the setting:
   a Hold the **VOD** key on the remote control until the HD LED light is flashing on the front panel.
   b Press the down arrow key to toggle the Stream Capability setting to the alternate option. Allow a few moments for the change to be reflected on the screen.
6 Exit from the diagnostic screen.
7 Press the **Guide** key on the remote control to confirm that HD channels are available or suppressed, depending on the setting you selected in step 5b.

Walled Garden

The signaling from the ISDS to provision walled garden services is accomplished by defining walled garden SAM service definitions via the ISDS, one for each walled garden service to be provisioned.

A base walled garden service and nine other walled garden services can be defined. Additionally, two special walled garden services for "My Account" and "App Store" can be defined.

Walled Garden SAM Service Settings

Use the following fields when you manage walled gardens in the ISDS.

Field	Description
Service Name	Required field. The name of the service if only available and shown to users of the ISDS who have access to the SAM Services List. Make this descriptive enough to understand what walled garden service is being offered. Subscribers will not see this field. **Example:** SDO Configuration.

Short Description	Required field. The short description is from a set of well-known values defined in the list below. The set-top uses these short description values to determine whether those services should be provisioned. If you are configuring the walled garden service to appear in the EPG, this field is used as the channel indicator. **Example: WG00** The following short description names are reserved for provisioning walled garden services. Each of these Short Descriptions must only be used once per system and must be used exactly as shown. ■ **_WG00** - Main service for walled garden ■ **_WG01** - Service for walled garden subsection 1 ■ **_WG02** - Service for walled garden subsection 2 ■ **_WG03** - Service for walled garden subsection 3 ■ **_WG04** - Service for walled garden subsection 4 ■ **_WG05** - Service for walled garden subsection 5 ■ **_WG06** - Service for walled garden subsection 6 ■ **_WG07** - Service for walled garden subsection 7 ■ **_WG08** - Service for walled garden subsection 8 ■ **_WG09** - Service for walled garden subsection 9 ■ **_WGMA** - Service for walled garden "My Account" ■ **_WGAP** - Service for walled garden "App Store"
Long Description	The long description is for meaningful display to the subscriber. This field appears in the Menu and/or in the grid cell of the EPG, as indicated by the options in the **Application URL** field.

Application URL

The application URL provides additional information for how the walled garden service can be accessed. It contains the application name and addition attributes, separated by semi-colons.

- **inEPG**
  - **0 (zero)** - Service is not displayed in the EPG
  - **1 (or name)** - Service is displayed in the EPG (default)

  The inEPG flag is independent whether the service is channel-mapped or not:

Channel Mapped?	inEPG Flag	Result
No	X	Not listed in EPG
Yes	0	Not listed in EPG; Direct tune brings up the service
Yes	1	Listed in EPG; Direct tune brings up the service

- **inMenu**
  - **0 (or name not present)** - Service is not displayed in the Portal Menu (default)
  - **1 (or name is present)** - Service is displayed in the Portal Menu
- **url -** The URL to access the service. This **must** be the last attribute of the Application URL so that is not required to be escaped.

  Format:

  wgarden://wgarden;inEPG=0;inMenu=1;eid=[xx];url=http://[server]/[location].html

  Notes:
  - Replace [xx] with the EID value associated with the walled garden package
  - Replace [server] with the name or IP address of the server
  - Replace [location] with the location of the web page or application
  - The syntax requires the EID to be placed before the URL

Logo	The channel or application logo number associated with this walled garden application. ■ If the walled garden appears in the Portal Menu, the linked 30x30 logo appears with it ■ If no linked 30x30 logo is provided, a default logo is displayed. ■ The logo functions in the EPG in the same way as current channel logos.
Parameter	Select the **Number** option.
Number	Enter **0** (zero).

Adding a Walled Garden SAM Service

1. From the ISDS Administrative Console, select the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens.
3. Click **File > New**. The Set Up SAM Service window opens.
4. Complete the fields on the screen as described in Walled Garden SAM Service Settings.
5. Click **Save**.

Modifying the SAM Services List

Complete the steps below to modify an already existing Walled Garden service.

1. From the ISDS Administrative Console, select the **Application Interface Modules** tab.
2. Click **SAM Service**. The SAM Service List window opens
3. Locate and highlight the service you want to modify.
4. Click **File > Open**. The configuration window for the service selected opens.
5. Edit the fields as described in Walled Garden SAM Service Settings.
6. Click **Save**.
7. If prompted, confirm the changes.

Downloadable Channel Logos

Beginning with ISDP Client 2.4, the ISDS now supports downloadable channel logos, making it possible for the service provider to customize logos displayed to the subscriber for any channel or service available.

Prepare Source Files

1. From the workstation where the logos are created or maintained, create a folder named logos for high resolution logos and a folder named logos30x30 for low resolution logos.
2. Name the contents of the folders as [ID].png.

   Notes:

   - The ID for the high resolution logo must match the ID for the low resolution logo. This ID will be the logo ID you use when you set up the SAM Service from the ISDS GUI.
   - Replace ID with the logo identification number.

   Example folder/file name convention:

   - High resolution logo: logos/1.png
   - Corresponding low resolution logo: logos30x30/1.png
3. Create a zip file named channel_logos.zip that contains the logos and the logos30x30 folders.
4. Copy the channel_logos.zip file from the source workstation and save the file onto the ISDS in the export/home/dncs/SiteFiles directory.

Set Up the isdpclient Server

1. From the ISDS Admin Console, select the **Servers Apps** tab.
2. Click the **BFS Administration** button, then select the **Servers** tab.
3. Does a server named isdpclient exist?

   - If **yes**, skip to the section ***Implement Channel Logos*** (on page 304).
   - If **no**, continue with step 4.
4. Click **File > New Server**.
5. In the **Server Name** field, type **isdpclient**.
6. Click the **Save** button, then continue with the section ***Implement Channel Logos*** (on page 304).

Implement Channel Logos

1. If necessary, from the ISDS Admin Console, select the **Servers Apps** tab.

2 Click the **BFS Client** button.

3 Does the isdpclient server have a directory named *galio*?

- If **yes**, skip to step 4.
- If **no**, add the directory as follows:

a Click **File > New Directory**.

b Name the new directory **galio**, then click **Save**.

c Continue with step 4.

4 Highlight the galio directory, then click **File/New File**. The system prompts you to provide source information. The destination information is prepopulated.

5 Enter **/export/home/dncs/SiteFiles/channel_logo.zip** in the Source field, then click **Save**.

Notes:

- If a logo exists in the channel_logos.zip file located on BFS, this logo will override the default logos built into Galio.
- An operator can add new logos to the channel_logos.zip file.

Example:

- Example of the channel_logos.zip file contents:
  - The logos file contains:
    - 1.png
    - 10005.png
  - The logos30x30 contains:
    - 1.png
    - 10005.png
- If an operator adds the channel_logos.zip file example above to the BFS, Galio (the web browser on the platform) will select the logos from these files to override the logos stored as defaults for a SAM service with the logo ID 1 and 10005 (which corresponds to ABC in the IPTV logos list).
- If the provider wants to associate a newly created walled garden service with Logo ID 1 in the SAM Services Dialog, and a logo "1.png" exists in the logos30x30 and logos directory of the channel_logos.zip file, this logo will be used as the service logo (in the EPG, Info Banner, and Menu, if desired) for that walled garden service.

Standard IPTV Logos in Order by Logo Number

This section lists the number and name of common service logos in numerical order by logo number. When using these logos, the logo file name must match the service number identified in this section.

10000	@Max
10003	5StarMax
10004	A&E Network
10005	ABC
10006	ABC Family Channel
10007	ABS-CBN (The Filipino Channel)
10008	ActionMax
10009	African Independent Television (AIT)
10010	Africast Television Network
10012	AMC
10015	Home Shopping Network
10018	American Life TV Network
10020	Animal Planet
10021	Anime Network
10022	Anime Network On Demand
10024	ART (Arab Radio & Television)
10027	AYM Sports
10028	B Mania
10030	Bandamax
10032	BBC America
10035	BET (Black Entertainment Television)
10036	BET Gospel
10037	BET Hip-Hop
10038	BET Jazz: The Jazz Channel
10041	Biography Channel, The
10045	Black Family Channel
10048	Bloomberg Television
10056	Bravo
10058	Broadway.com Television
10059	Buzztime Entertainment, Inc
10060	Canal 24 Horas
10063	Cartoon Network
10065	CBS
10066	CCTV-4
10067	CCTV International
10068	Channel One Russia Worldwide Network
10070	Church Channel, The
10071	Cine Latino
10072	Cinemax
10073	Cinemax HD
10074	Classic Arts Showcase
10076	CMT: Country Music Television
10077	CNBC
10078	CNBC World
10079	CNC Columbia
10080	CNN (Cable News Network)
10081	CNN en Espanol
10082	CNN Headline News
10083	CNNI (CNN International)
10086	Comedy Central
10087	truTV (formerly Court TV)
10088	Crime Channel, The
10089	CRN; Networks
10090	C-SPAN (Cable Satellite Public Affairs Network)
10091	C-SPAN 3
10092	C-SPAN 2
10093	CSTV
10094	CTI Zhong Tian Channel
10095	CW Television Network, The
10097	Daystar Television Network
10098	DePelicula
10102	Discovery Channel
10103	Discovery en Espanol
10104	Discovery HD Theater'"
10105	Discovery Health Channel
10106	Planet Green (formerly Discovery Home Channel)
10107	Discovery Kids Channel
10108	Investigation Discovery (formerly Discovery Times Channel)
10110	Disney Channel
10111	DIY -Do-It-Yourself Network
10112	DMX MUSIC
10114	EI Entertainment Television
10115	ECOLOGY Communications
10118	Encore
10119	Encore Action
10120	Encore Drama
10121	Encore HDTV
10122	Encore Love
10124	Encore Mystery
10125	EncoreWAM
10126	Encore Westerns
10129	ESPN
10130	ESPN Classic
10131	ESPN Deportes
10132	ESPN HD
10133	ESPN2

Standard IPTV Logos in Order by Logo Number, continued

10134	ESPN2 HD
10135	ESPNEWS
10136	ESPN PPV
10137	ESPNU
10139	Events iNDEMAND
10185	Fuel
10186	Fuse
10187	FX (Fox Basic Cable)
10188	FX On Demand
10189	G4 (formerly G4TechTV)

10140	EWTN
10144	Familyland Television Network
10145	FamilyNet
10147	FCS Atlantic
10148	FCS Central
10149	FCS Pacific
10152	FitTV
10153	FLiX
10154	Food Network
10155	FOX Cable Networks
10156	Fox College Sports
10158	FOX Movie Channel
10159	FOX News Channel
10160	Fox Business Channel
10161	Fox Reality Channel
10162	Fox Soccer Channel
10163	Fox Sports en Espanol
10164	Fox Sports Latin America
10166	FSN
10167	FSN Arizona
10168	FSN Bay Area
10169	FSN Chicago
10170	FSN Detroit
10171	FSN Florida
10172	FSN HD
10173	FSN Midwest
10174	FSN New England
10175	FSN New York
10176	FSN North
10177	FSN Northwest
10178	FSN Ohio
10179	FSN Pittsburgh
10180	FSN Rocky Mountain
10181	FSN South
10182	FSN Southwest
10183	FSN West
10184	FSN West 2
10190	Galavision
10192	German TV
10195	Gol TV
10196	Golden Eagle Broadcasting
10197	Golf Channel, The
10201	Grandes Documentales
10202	Great American Country (GAC)
10203	GSN
10205	Hallmark Channel
10206	Hallmark Movie Channel
10207	HBO (Home Box Office)
10208	HBO 2
10209	HBO Comedy
10210	HBO Family
10211	HBO HD
10212	HBO Latino
10213	HBO Signature
10214	HBO ZONE
10215	HDNet
10216	HDNet Movies
10217	here!TV
10218	History Channel en Espanol, The
10219	History Channel, The
10220	History Channel On Demand, The
10221	History International
10222	HITN-TV Hispanic Information & Telecommunications Network
10223	Hollywood.com Television
10224	Home and Garden Television (HGTV)
10228	HorseRacing TV
10229	Hot Body Channel, The
10231	Hot Zone
10233	HSN, The Home Shopping Network
10234	HTV
10235	Hustler TV
10239	iN DEMAND Networks
10240	iNDEMAND Pay-Per-View
10241	Independent Film Channel (IFC), The

Standard IPTV Logos in Order by Logo Number, continued

10243	lnfinito
10244	MOJO (formerly INHD)
10245	INHD2 (iNDEMAND HD2)
10247	Inspiration Network, The (INSP)
10248	Inspirational Life Television (i-Lifetv)
10249	International Channel
10251	JCTV
10252	Jewelry Television by ACN
10254	Kids Unlimited
10256	La Familia Network
10258	Learning Channel, The (TLC)
10259	Liberty Channel
10304	National Iranian Television (NITV)
10306	NBA TV
10307	NBC
10308	NBC Universal Cable
10309	New England Cable News
10310	New England Sports Network (NESN)
10312	Newsworld Inlemational
10313	NFL Network
10314	NHL Network
10315	Nick at Nite
10316	Nick2
10317	Nickelodeon

10260	Lifetime Movie Network
10261	Lifetime Real Women
10262	Lifetime Television
10264	LOGO
10267	Mas Musica TV
10268	MavTV--Mav'rick Entertainment Network
10269	MBC America (MunHwa Broadcasting Corp.)
10270	Meadows Racing Network, The
10272	Military Channel, The (Discovery)
10273	Military History Channel
10274	Moody Broadcasting Network
10276	MoreMax
10277	Movie Channel-HD, The
10278	Movie Channel, The (TMC)
10279	Movie Channel en Espanol, The
10280	Movie Channel On Demand, The
10281	Movie Channel Xtra, The
10282	Movie Channel Xtra en Espanol, The
10284	MOVIEplex
10285	Movies On Demand
10287	MSNBC
10289	MTV Espanol
10290	MTV Hits
10291	MTV Jams
10292	MTV: Music Television
10293	MTV2
10295	mun2
10297	Music Choice
10299	Music Unlimited
10303	National Geographic Channel
10319	Nicktoons
10320	Noah's World International Television
10321	nickjr (formerly Noggin)
10322	NorthWest Cable News
10324	NTV America
10328	Outdoor Channel, The
10329	Versus (formerly Outdoor Life Network)
10330	OuterMax
10331	OVATION -The Arts Network
10332	Oxygen Media, Inc
10333	ion (formerly PAX TV)
10336	Playboy TV Networks
10337	Playgirl TV
10338	Pleasure
10340	Product Information Network (PIN)
10341	Puma TV
10344	QVC
10346	RAI International
10347	Rang-A-Rang
10352	Regional News Network (RNN)
10354	Ritmoson Latino
10356	Russian Television Network of America (RTN)
10359	Saigon Broadcasting Television Network (SBTN)
10360	SyFy (formerly SCI FI Channel)
10361	Science Channel, The
10362	SCOLA
10366	Shop At Home Network
10367	ShopNBC
10368	Short TV
10369	Showtime

Standard IPTV Logos in Order by Logo Number, continued

10370	Showtime en Espanol
10371	Showtime Beyond
10372	Showtime Beyond en Espanol
10373	Showtime Extreme
10374	Showtime Extreme en Espanol
10375	Showtime Family Zone
10376	Showtime Family Zone en Espanol
10377	Showtime HD
10378	Showtime Next
10379	Showtime On Demand
10380	Showtime Showcase
10381	Showtime Showcase en Espanol
10382	Showtime Too
10383	Showtime Too en Espanol
10384	Showtime Women
10385	ShowtimeWomen en Espanol
10386	Si-TV
10387	SOAPnet
10415	Sur
10416	TBN -Trinity Broadcasting Network
10417	TBN Enlace USA
10418	TBS
10419	Telefe Internacional
10420	Telefutura
10421	Telehit
10422	Telemundo
10423	Telemundo Internacional
10424	Penthouse TV (formerly TEN)
10425	TEN On Demand
10426	Vavoom (formerly TENBlox)
10427	SexxSee (formerly TENBlue)
10428	TENClips
10429	TENMax
10430	Tennis Channel, The
10431	TENXtsy
10434	ThrilierMax

10388	Sorpresa!
10389	Soundtrack Channel (STC)
10390	Southern Entertainment Television
10391	Southern Entertainment Television 2: Bluegrass Music Channel
10392	Southern Entertainment Television 3: Classic Black Gospel
10393	Speed Channel
10394	Spice 1
10395	Spice 2
10397	Spike TV
10398	Sports iNDEMAND
10399	Sportsman Channel, The
10400	STARZ
10401	STARZ Cinema
10402	STARZ Comedy
10403	STARZ Edge
10405	STARZ HDTV
10406	STARZ in Black
10407	STARZ Kids & Family
10408	STARZ On Demand
10410	Style Network, The
10411	Studio 4 Kids
10412	Sun Sports
10413	Sundance Channel
10414	Sundance Documentary Channel
10436	TNT (Turner Network Television)
10437	TNT HD
10438	Disney XD (formerly Toon Disney)
10439	TR!0
10440	Travel Channel
10442	Tumer Classic Movies (TCM)
10443	Turner South
10444	TV 5
10445	TV Asia
10446	TV Games Network
10447	TV Guide Channel
10448	TV Guide Interactive
10449	TV JAPAN
10450	TV Land
10451	TVOne
10452	TV Polonia
10453	TVE Internacional
10454	TVG Network
10455	tvK24
10458	Universal HD
10459	Univision
10460	Urban Xtra
10462	USA Network
10463	Utilisima Satelital

Standard IPTV Logos in Order by Logo Number, continued

10464	Vegas Channel, The
10465	MTVU (formerly VH Uno)
10466	VH1 (Music First)
10467	VH1 Classic
10468	VH1 Country
10469	VH1 Mega Hits
10470	VH1 Soul
10471	Video Rola
10472	VOY Network
10473	We: Women's Entertainment
10474	Wealth TV
10475	Weather Channel, The
10476	Weatherscan
10480	Wisdom Television
10481	Wmax
10482	Word Network, The
10483	Worship Network, The
10485	Zee TV USA, Inc
10486	Zhong Tian Channel
10487	ABC Family HD
10488	Animal Planet HD
10489	Big Ten HD
10490	Cartoon Network HD
10507	Teennick
10508	TLC HD
10509	USA HD
10510	Versus HD
10511	PBS Kids Sprout
10512	ABC News Now
10513	RFD TV
10514	CMT Pure Country
10515	MTV TR3S
10516	Chiller
10517	Sleuth
10518	Crime & Investigation Network
10519	Discovery Familia
10520	Urge
10521	IndiePlex
10522	RetroPlex
10523	A&E HD
10524	E! HD
10525	Food Network HD
10526	HGTV HD
10527	National Geographic HD
10528	NFL Network HD
10529	Palladia

10491	Club Jenna
10492	CNN Headline News HD
10493	Discovery HD
10494	Disney HD
10495	Disney XD HD
10496	ESPN News HD
10497	ESPNU HD
10498	Fresh
10499	Golf Channel HD
10500	Investigation Discovery
10501	Lifetime HD
10502	Planet Green HD
10503	Science HD
10504	SkinTV (fomerly Shorteez)
10505	SyFy HD
10506	TBS HD
10530	STARZ Kids & Family HD
10531	STARZ Edge HD
10532	STARZ Comedy HD
10533	HBO 2 HD
10534	HBO Family HD
10535	HBO Comedy HD
10536	HBO Signature HD
10537	HBO Zone HD
10538	HBO Latino HD
10539	MoreMax HD
10540	ActionMax HD
10541	ThrillerMax HD
10542	Wmax HD
10543	@Max HD
10544	5StarMax HD
10545	OuterMax HD

Standard IPTV Logos in Order by Channel Title

This section lists the name and number of common service logos in alphabetical order by channel title. When using these logos, the logo file name must match the service number identified in this section.

10000	@Max
10543	@Max HD
10003	5StarMax
10544	5StarMax HD
10523	A&E HD
10004	A&E Network
10005	ABC
10006	ABC Family Channel
10487	ABC Family HD
10512	ABC News Now
10007	ABS-CBN (The Filipino Channel)
10008	ActionMax
10540	ActionMax HD
10009	African Independent Television (AIT)
10010	Africast Television Network
10012	AMC
10018	American Life TV Network
10020	Animal Planet
10488	Animal Planet HD
10021	Anime Network
10022	Anime Network On Demand
10024	ART (Arab Radio & Television)
10027	AYM Sports
10028	B Mania
10030	Bandamax
10032	BBC America
10035	BET (Black Entertainment Television)
10036	BET Gospel
10065	CBS
10067	CCTV International
10066	CCTV-4
10068	Channel One Russia Worldwide Network
10516	Chiller
10070	Church Channel, The
10071	Cine Latino
10072	Cinemax
10073	Cinemax HD
10074	Classic Arts Showcase
10491	Club Jenna
10514	CMT Pure Country
10076	CMT: Country Music Television
10077	CNBC
10078	CNBC World
10079	CNC Columbia
10080	CNN (Cable News Network)
10081	CNN en Espanol
10082	CNN Headline News
10492	CNN Headline News HD
10083	CNNI (CNN International)
10086	Comedy Central
10518	Crime & Investigation Network
10088	Crime Channel, The
10089	CRN; Networks
10093	CSTV
10094	CTI Zhong Tian Channel
10095	CW Television Network, The

10037	BET Hip-Hop
10038	BET Jazz: The Jazz Channel
10489	Big Ten HD
10041	Biography Channel, The
10045	Black Family Channel
10048	Bloomberg Television
10056	Bravo
10058	Broadway.com Television
10059	Buzztime Entertainment, Inc
10090	C-SPAN (Cable Satellite Public Affairs Network)
10092	C-SPAN 2
10091	C-SPAN 3
10060	Canal 24 Horas
10063	Cartoon Network
10097	Daystar Television Network
10098	DePelicula
10102	Discovery Channel
10103	Discovery en Espanol
10519	Discovery Familia
10493	Discovery HD
10104	Discovery HD Theater'''
10105	Discovery Health Channel
10107	Discovery Kids Channel
10110	Disney Channel
10494	Disney HD
10438	Disney XD (formerly Toon Disney)
10495	Disney XD HD
10111	DIY -Do-It-Yourself Network

Standard IPTV Logos in Order by Channel Title, continued

10112	DMX MUSIC
10524	E! HD
10115	ECOLOGY Communications
10114	EI Entertainment Television
10118	Encore
10119	Encore Action
10120	Encore Drama
10121	Encore HDTV
10122	Encore Love
10124	Encore Mystery
10126	Encore Westerns
10125	EncoreWAM
10129	ESPN
10130	ESPN Classic
10131	ESPN Deportes
10132	ESPN HD
10496	ESPN News HD
10136	ESPN PPV
10133	ESPN2
10134	ESPN2 HD
10135	ESPNEWS
10137	ESPNU
10497	ESPNU HD
10139	Events iNDEMAND
10140	EWTN
10144	Familyland Television Network
10145	FamilyNet
10147	FCS Atlantic
10148	FCS Central
10149	FCS Pacific
10152	FitTV
10153	FLiX
10154	Food Network
10525	Food Network HD
10160	Fox Business Channel
10164	Fox Sports Latin America
10498	Fresh
10166	FSN
10167	FSN Arizona
10168	FSN Bay Area
10169	FSN Chicago
10170	FSN Detroit
10171	FSN Florida
10172	FSN HD
10173	FSN Midwest
10174	FSN New England
10175	FSN New York
10176	FSN North
10177	FSN Northwest
10178	FSN Ohio
10179	FSN Pittsburgh
10180	FSN Rocky Mountain
10181	FSN South
10182	FSN Southwest
10183	FSN West
10184	FSN West 2
10185	Fuel
10186	Fuse
10187	FX (Fox Basic Cable)
10188	FX On Demand
10189	G4 (formerly G4TechTV)
10190	Galavision
10192	German TV
10195	Gol TV
10196	Golden Eagle Broadcasting
10499	Golf Channel HD
10197	Golf Channel, The
10201	Grandes Documentales
10202	Great American Country (GAC)
10203	GSN

10155	FOX Cable Networks
10156	Fox College Sports
10158	FOX Movie Channel
10159	FOX News Channel
10161	Fox Reality Channel
10162	Fox Soccer Channel
10163	Fox Sports en Espanol
10205	Hallmark Channel
10206	Hallmark Movie Channel
10207	HBO (Home Box Office)
10208	HBO 2
10533	HBO 2 HD
10209	HBO Comedy
10535	HBO Comedy HD

Standard IPTV Logos in Order by Channel Title, continued

10210	HBO Family
10534	HBO Family HD
10211	HBO HD
10212	HBO Latino
10538	HBO Latino HD
10213	HBO Signature
10536	HBO Signature HD
10214	HBO ZONE
10537	HBO Zone HD
10215	HDNet
10216	HDNet Movies
10217	here!TV
10526	HGTV HD
10218	History Channel en Espanol, The
10220	History Channel On Demand, The
10219	History Channel, The
10221	History International
10222	HITN-TV Hispanic Information & Telecommunications Network
10223	Hollywood.com Television
10224	Home and Garden Television (HGTV)
10015	Home Shopping Network
10228	HorseRacing TV
10229	Hot Body Channel, The
10231	Hot Zone
10233	HSN, The Home Shopping Network
10234	HTV
10235	Hustler TV
10239	iN DEMAND Networks
10240	iNDEMAND Pay-Per-View
10241	Independent Film Channel (IFC), The
10521	IndiePlex
10245	INHD2 (iNDEMAND HD2)
10247	Inspiration Network, The (INSP)
10248	Inspirational Life Television (i-Lifetv)
10249	International Channel
10500	Investigation Discovery
10108	Investigation Discovery (formerly Discovery Times Channel)
10333	ion (formerly PAX TV)
10251	JCTV
10258	Learning Channel, The (TLC)
10259	Liberty Channel
10501	Lifetime HD
10260	Lifetime Movie Network
10261	Lifetime Real Women
10262	Lifetime Television
10243	lnfinito
10264	LOGO
10267	Mas Musica TV
10268	MavTV--Mav'rick Entertainment Network
10269	MBC America (MunHwa Broadcasting Corp.)
10270	Meadows Racing Network, The
10272	Military Channel, The (Discovery)
10273	Military History Channel
10244	MOJO (formerly INHD)
10274	Moody Broadcasting Network
10276	MoreMax
10539	MoreMax HD
10279	Movie Channel en Espanol, The
10280	Movie Channel On Demand, The
10282	Movie Channel Xtra en Espanol, The
10281	Movie Channel Xtra, The
10277	Movie Channel-HD, The
10278	Movie Channel, The (TMC)
10284	MOVIEplex
10285	Movies On Demand
10287	MSNBC
10289	MTV Espanol
10290	MTV Hits
10291	MTV Jams
10515	MTV TR3S
10292	MTV: Music Television
10293	MTV2
10465	MTVU (formerly VH Uno)
10295	mun2
10297	Music Choice
10299	Music Unlimited
10303	National Geographic Channel
10527	National Geographic HD

10252	Jewelry Television by ACN
10254	Kids Unlimited
10256	La Familia Network
10304	National Iranian Television (NITV)
10306	NBA TV
10307	NBC

Standard IPTV Logos in Order by Channel Title, continued

10308	NBC Universal Cable
10309	New England Cable News
10310	New England Sports Network (NESN)
10312	Newsworld Inlemational
10313	NFL Network
10528	NFL Network HD
10314	NHL Network
10315	Nick at Nite
10316	Nick2
10317	Nickelodeon
10321	nickjr (formerly Noggin)
10319	Nicktoons
10320	Noah's World International Television
10322	NorthWest Cable News
10324	NTV America
10328	Outdoor Channel, The
10330	OuterMax
10545	OuterMax HD
10331	OVATION -The Arts Network
10332	Oxygen Media, Inc
10529	Palladia
10511	PBS Kids Sprout
10424	Penthouse TV (formerly TEN)
10106	Planet Green (formerly Discovery Home Channel)
10502	Planet Green HD
10336	Playboy TV Networks
10337	Playgirl TV
10338	Pleasure
10340	Product Information Network (PIN)
10341	Puma TV
10344	QVC
10346	RAI International
10347	Rang-A-Rang
10352	Regional News Network (RNN)
10522	RetroPlex
10513	RFD TV
10354	Ritmoson Latino
10356	Russian Television Network of America (RTN)
10359	Saigon Broadcasting Television Network (SBTN)
10361	Science Channel, The
10503	Science HD
10362	SCOLA
10427	SexxSee (formerly TENBlue)
10366	Shop At Home Network
10367	ShopNBC
10368	Short TV
10369	Showtime
10371	Showtime Beyond
10372	Showtime Beyond en Espanol
10370	Showtime en Espanol
10373	Showtime Extreme
10374	Showtime Extreme en Espanol
10375	Showtime Family Zone
10376	Showtime Family Zone en Espanol
10377	Showtime HD
10378	Showtime Next
10379	Showtime On Demand
10380	Showtime Showcase
10381	Showtime Showcase en Espanol
10382	Showtime Too
10383	Showtime Too en Espanol
10384	Showtime Women
10385	ShowtimeWomen en Espanol
10386	Si-TV
10504	SkinTV (fomerly Shorteez)
10517	Sleuth
10387	SOAPnet
10388	Sorpresa!
10389	Soundtrack Channel (STC)
10390	Southern Entertainment Television
10391	Southern Entertainment Television 2: Bluegrass Music Channel
10392	Southern Entertainment Television 3: Classic Black Gospel
10393	Speed Channel
10394	Spice 1
10395	Spice 2
10397	Spike TV
10398	Sports iNDEMAND
10399	Sportsman Channel, The
10400	STARZ
10401	STARZ Cinema
10402	STARZ Comedy
10532	STARZ Comedy HD
10403	STARZ Edge
10531	STARZ Edge HD

Standard IPTV Logos in Order by Channel Title, continued

10405	STARZ HDTV
10406	STARZ in Black
10407	STARZ Kids & Family
10530	STARZ Kids & Family HD
10408	STARZ On Demand
10411	Studio 4 Kids
10410	Style Network, The
10412	Sun Sports
10413	Sundance Channel
10414	Sundance Documentary Channel
10415	Sur
10360	SyFy (formerly SCI FI Channel)
10505	SyFy HD
10416	TBN -Trinity Broadcasting Network
10417	TBN Enlace USA
10418	TBS
10506	TBS HD
10507	teennick
10419	Telefe Internacional
10420	Telefutura
10421	Telehit
10422	Telemundo
10423	Telemundo Internacional
10425	TEN On Demand
10428	TENClips
10429	TENMax
10430	Tennis Channel, The
10431	TENXtsy
10434	ThrilierMax
10541	ThrillerMax HD
10508	TLC HD
10436	TNT (Turner Network Television)
10437	TNT HD
10439	TR!0
10440	Travel Channel
10087	truTV (formerly Court TV)
10442	Tumer Classic Movies (TCM)
10443	Turner South
10444	TV 5
10445	TV Asia
10446	TV Games Network
10447	TV Guide Channel
10448	TV Guide Interactive
10449	TV JAPAN
10450	TV Land
10452	TV Polonia
10453	TVE Internacional
10454	TVG Network
10455	tvK24
10451	TVOne
10458	Universal HD
10459	Univision
10460	Urban Xtra
10520	Urge
10509	USA HD
10462	USA Network
10463	Utilisima Satelital
10426	Vavoom (formerly TENBlox)
10464	Vegas Channel, The
10329	Versus (formerly Outdoor Life Network)
10510	Versus HD
10466	VH1 (Music First)
10467	VH1 Classic
10468	VH1 Country
10469	VH1 Mega Hits
10470	VH1 Soul
10471	Video Rola
10472	VOY Network
10473	We: Women's Entertainment
10474	Wealth TV
10475	Weather Channel, The
10476	Weatherscan
10480	Wisdom Television
10481	Wmax
10542	Wmax HD
10482	Word Network, The
10483	Worship Network, The
10485	Zee TV USA, Inc
10486	Zhong Tian Channel

Downloadable Configuation Files

Beginning with ISDP Client 2.4, the ISDS now supports downloadable configuration files to enable the service provider to customize Galio (the Web Browser on the platform) and RTN (Reference TV Navigator UI) configuration variables.

Set Up a Downloadable Configuration File

Complete the steps below to implement the downloadable configuration file feature.

Important: We recommend that modifications to configuration variables be performed only by operators with full understanding of the impacts to the system.

1. Create a customized configuration file using the known configuration variables listed in the section Configuration Variables.
   Example:

```
# Set the Media Object Model (MOM) to insecure mode
# (allow non-wafer applications, e.g. Walled Gardens, access to
"sensitive" APIs)
mom.insecure: 1


# Set the default theme, over-riding the user's selection every time
com_antplc_tvlib.tvlib_config_global_theme: darkblue
```

2. Name the customized file **dl-config.txt**.
3. Save the file onto the ISDS in the export/home/dncs/SiteFiles directory.

Set Up the isdpclient Server

1. From the ISDS Admin Console, select the **Servers Apps** tab.
2. Click the **BFS Administration** button, then select the **Servers** tab.
3. Does a server named isdpclient exist?
   - If **yes**, skip to the section ***Implement the Downloadable Configuration File*** (on page 315).
   - If **no**, continue with step 4.
4. Click **File > New Server**.
5. In the **Server Name** field, type **isdpclient**.
6. Click the **Save** button, then continue with the section ***Implement the Downloadable Configuration File*** (on page 315).

Implement the Downloadable Configuration File

1. If necessary, from the ISDS Admin Console, select the **Servers Apps** tab.

2 Click the **BFS Client** button.

3 Does the isdpclient server have a directory named *galio*?

- If **yes**, skip to step 4.
- If **no**, add the directory as follows:

a Click **File > New Directory**.

b Name the new directory **galio**, then click **Save**.

c Click **View > Refresh**.

d Continue with step 4.

4 Highlight the galio directory, click **File > New Directory**.

5 Name the new directory **conf.d**, then click **Save**.

6 Click **View > Refresh**.

7 Highlight the conf.d directory, click **File**, then click **New Link**.

8 Name the new link **dl-config.txt**, then click **Save**. The system prompts you to provide source information. The destination information is pre-populated.

9 Enter **export/home/dncs/SiteFiles/dl-config.txt** in the Source field, then click **Save**.

Note: On startup, Galio checks ths directory /bfs/isdpclient/galio/conf.d/ and overrides the client default file and user settings with the customized file.

Configuration Variables

- **com_antplc_tvlib.tvlib_config_global_theme: darkblue**
  This variable is the currently selected skin/theme. If set, each user's set-top will use this theme by default, overriding their selection. Appropriate values of as version 2.5 of the ISDP Client code are "darkblue," "coolbreeze," and/or "kubrickblack."

- **mom.insecure: 1**
  This variable allows access to sensitive "MOM" (Media Object Model) APIs. This should only be used on sites wishing to support Walled Garden applications.

- **mom.pc.pin.tries: 3**
  This variable tells the UI how many attempts at entering a correct PIN (Parental Control or Purchase) that the user is allowed. After this number of unsuccessful PIN entries, the dialog is dismissed and the user is not able to access the PIN-blocked feature.

- **com_antplc_tvlib.tvlib_config_main_menu_has_live_tv_entry:**
  This variable tells the UI whether or not to display the "Live TV" element in the Menu Portal. A value of "false" will hide the "Live TV" entry in the menu. A value of "true" will show the "Live TV" entry in the menu.

- **com_antplc_tvlib.tvlib_config_global_power_on_at_boot:**

This variable tells the UI whether or not to boot on set-top power on. A value of 1 indicates that the set-top should boot to UI and video when powered-on or rebooted. A value of 0 indicates that the set-top should wait for the user to press the "Power" button to leave the "standby" state and boot to UI and video.

- **com_antplc_tvlib.tvlib_config_media_variable_volume_control:**

  This variable tells the UI whether the set-top volume control is fixed or variable. A value of "false" sets the volume control to fixed. A value of "true" sets the volume control to variable.

- **com_antplc_tvlib.tvlib_config_media_fixed_volume:**

  This variable tells the UI which volume to use when in fixed (not variable) volume mode. Any value between 0 and 100 can be used with 0 indicating 0% volume and 100 indicating 100% volume.

- **mom.output.digital.audio.mode: ac3**

  This variable tells the UI which digital audio output mode to be used by default. Current options are: "ac3" for Dolby™ Digital technology, or "uncompressed" for Other (PCM).

- **mom.output.hd.video.format: 480i**

  This variable tells the UI which HD video format to be used by default. Current options are: 1080i, 720p, 480p, and 480i

- **mom.output.tv.aspect.ratio: 4:3**

  This variable tells the UI which TV aspect ratio to be used by default. Current options are: "4:3" for Standard 4:3, "4:3letterbox" for Standard 4:3 Letterbox, and "16:9" for 16:9.

- **com_antplc_tvlib.tvlib_config_global_header: http://myserver.com/location/file.png**

  This variable points to a maximum 400px by 60px image displayed in the header when "Menu" and "Guide" are displayed. This variable can be an HTTP location, such as http://myserver.com/location/file.png or a BFS location, such as file:///bfs/isdpclient/company_logo.png. This area should be reserved for a company logo to complement the Cisco logo or an advertisement spot.

- **com_antplc_tvlib.tvlib_config_zapper_skip_forward_secs: 30**

  This variable should be set to the number of seconds for forward skipping when the user presses the skip forward button on their remote control while watching a DVR program or the time-shift buffer. The default setting is 30 seconds.

- **com_antplc_tvlib.tvlib_config_zapper_skip_backward_secs: 10**

  This variable should be set to the number of seconds for backward skipping when the user presses the skip backward button on their remote control while watching a DVR program or the time-shift buffer. The default setting is 10 seconds.

- **com_antplc_tvlib.tvlib_config_global_operator_contact_number: (800) 555-555 5**

  This variable defines the operator's contact number. This will be used throughout the UI in up-sell opportunities, such as DVR and PPV.

VBI Line Trim

This section provides instructions to implement the VBI Line Trim feature, which strips VBI lines that may appear on televisions using letterbox configurations.

VBI Line Trim Settings

Use the following fields when you manage the VBI line trim feature in the ISDS.

Field	Description
Service Name	Name of the service. **Example:** VBI Line Trim Config.
Short Description	Required field. Enter **vbitrim**
Long Description	Description of the service. **Example:** VBI Line Trim Configuration for [service].
Application URL	Append **;vbitrim=[numeric value]** to the directory path. **Notes:** ■ Appending this parameter is optional. If you create the SAM Service for VBI Line Trim and do not specify a value, the set-top will default the value to 100. ■ If you choose to specify the value, replace [numeric value] with a value ranging from 0 through 4096. See ***Choosing the VBI Line Trim Value*** (on page 320) for additional details. **Example:** `bfs://resapp/watchtv;vbitrim=2048`
Logo	Leave blank.
Parameter	Select the **Number** option.
Number	Enter a unique number.

Set Up the VBI Line Trim Feature

1. From the ISDS Administrative Console, click the **Application Interface Module** tab.
2. Click **SAM Service**. The SAM Service List window appears.
3. Click **File > New**. The Set Up SAM Service window appears.
4. Complete the fields as described in VBI Line Trim Settings.
5. Click **Save**. The SAM service is added to the SAM Service List.

6 Click **File > Close** to close the Same Service List window.

Choosing the VBI Line Trim Value

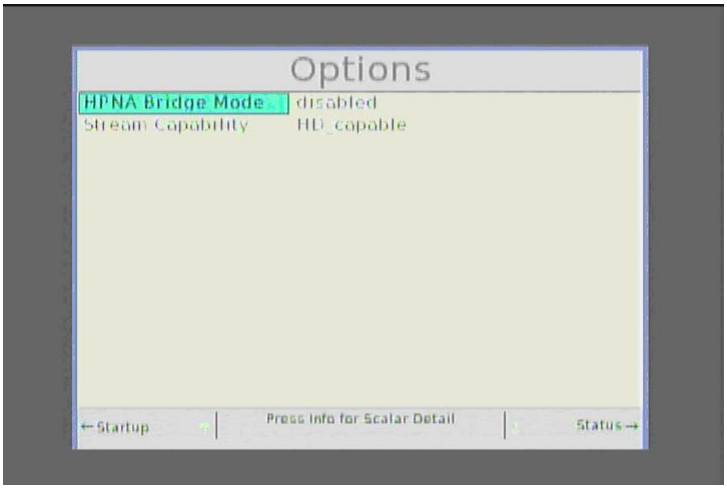
Follow the guidelines below to determine the numeric value you wish to use with the vbitrim SAM Service:

- 0 - Video is not trimmed
- 4096 - Entire image is trimmed
- 100 - default value the set-top will use if an alternate value is not defined
- Use the equation **(x*y)/4096 = z** to calculate a the number of lines to trim
  Notes:
  - x = the image size in pixels
  - y = vbitrim value setting
  - z = approximate number of lines that will be trimmed
    Example: `(720 * 100)/4096 = 17.56`
    - x represents a 720p image
    - y indicates that the vbitrim value is set to 100
    - z equals 17.56. Approximately 17 lines will be trimmed from the image.

HPNA Bridge Mode

Cisco ISDP set-tops support HPNA bridging. However, the HPNA Bridged mode option is disabled by default. To enable the set-top for HPNA Bridged mode, follow this procedure.

1. On the remote control, press and hold the **OK** key until the HD LED blinks on the front of the set-top.
2. Press the **Down** arrow key. The Startup page appears.
3. Press **Right** arrow key to move through the diagnostic pages until the Options diagnostic page appears, similar to the following example.



4. Press and hold the **Phone** key on the remote control until the HD LED blinks on the front of the set-top.
5. With **HD** LED flashing, press the **Down** Arrow key on the remote control to enable the HPNA Bridge mode, and then wait for five seconds for the Options diagnostic page to display this change.
6. When the Options page lists the HPNA Bridge Mode as "enabled," press the **Exit** key to exit the diagnostic pages.

Provision Authorization for Services

This section provides instructions to provision authorization for services (downloadable applications, DVR, EPS Search, or Walled Garden) on ISDP-compatible set-tops. Once the procedures in this section are complete, the authorization package can be added to the applicable set-tops via the ISDS or the Billing System.

Create a Package

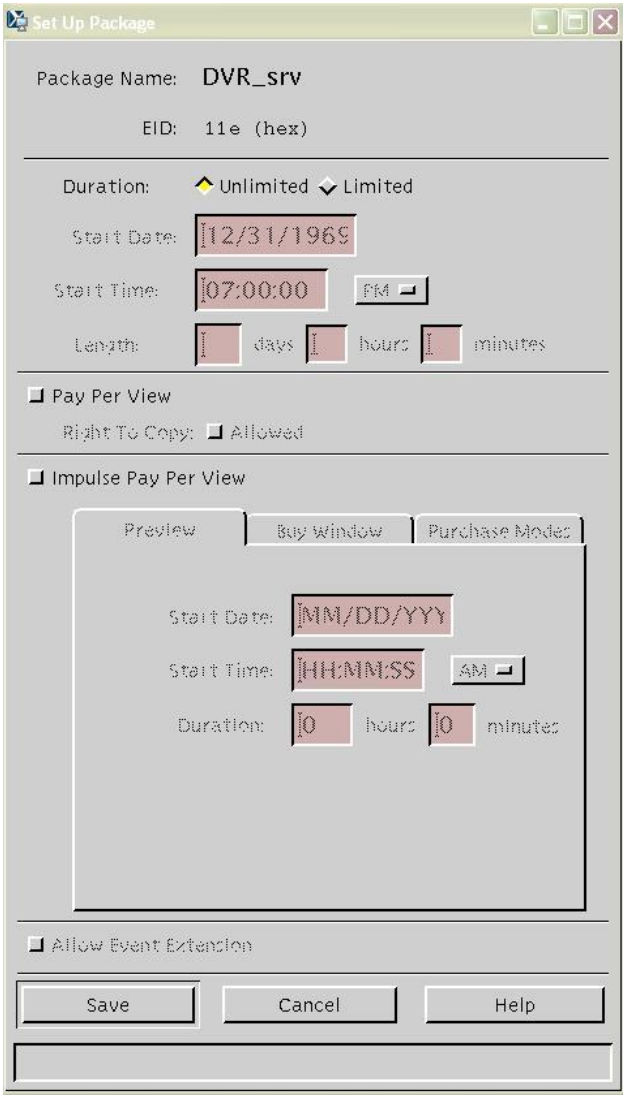
Complete the following steps to create a new package for the services or applications that you want to provision. If you have already created the package you want to use for the service, skip to the section ***Determine the EID Value*** (on page 322).

1. On the ISDS Administrative Console, click **Package** from the System Provisioning tab. The Package List window opens.
2. Select **File > New** to open the Set Up Package window.
3. Enter a unique name for the package.
4. Click **Save**. The package is created.

Determine the EID Value

Complete the steps below to determine the EID value of the service you want to authorize.

1 Open the package you will use to authorize the service and record the EID value: _____.



2 Click **Cancel** to close the Set Up Package window.

3 In the Package List window, select **File > Close** to close the window.

4 Continue with ***Create a SAM Service*** (on page 323).

Create a SAM Service

Complete the following steps to create a SAM service for the package you created.

1 From the ISDS Administrative Console, select the **Application Interface Modules** tab.

2 Click the **SAM Service** button. The SAM Service List window opens.

3 Click **File > New.** The Set Up SAM Service window opens.

4 Enter the SAM Service information per the guidelines below.

Guidelines:

The following variables are available to define a SAM Service:

- **Service Name** (required) - this name is only available and shown to users of the ISDS who have access to the SAM Services List. Make this descriptive enough to understand which service is being offered. End users will not see this field.
- **Short Description** (required) - the short description must match one of the values defined in this document; the set-top UI will use these short description values to determine if those services are being provisioned.

  The following short description names are reserved for provisioning services. Each of these Short Descriptions must only be used once per system and must be used **exactly** as shown.

SAM Short Description	Service
_SADV	DVR
_MRDV	MR-DVR
_VOD	VOD
_EPGS	EPG Search
_WG00	Walled Garden 0
_WG01	Walled Garden 1
_WG02	Walled Garden 2
_WG03	Walled Garden 3
_WG04	Walled Garden 4
_WG05	Walled Garden 5
_WG06	Walled Garden 6
_WG07	Walled Garden 7
_WG08	Walled Garden 8
_WG09	Walled Garden 9
_WGMA	Walled Garden for "My Account"
_WGAP	Walled Garden for "App Store"

- **Long Description** - The long description will be used for meaningful display to the user. The Long Description will appear in the Menu and/or in the grid cell of the electronic programming guide (EPG), as indicated by the options in the "Application URL", described below.
- **Application URL** - The application URL provides additional information for how the service can be accessed.
  Are you creating a service for a Walled Garden?

– If **yes**, enter the following:
wgarden://wgarden;inEPG=0;inMenu=1;eid=[xx];url=http://[server]/[location].html

Notes:

- Replace "xx" with the EID value associated with the Walled Garden package and "server" with the name or IP address of the server.
- Replace [server] with the name or IP address of the server
- Replace [location] with the location of the web page or application

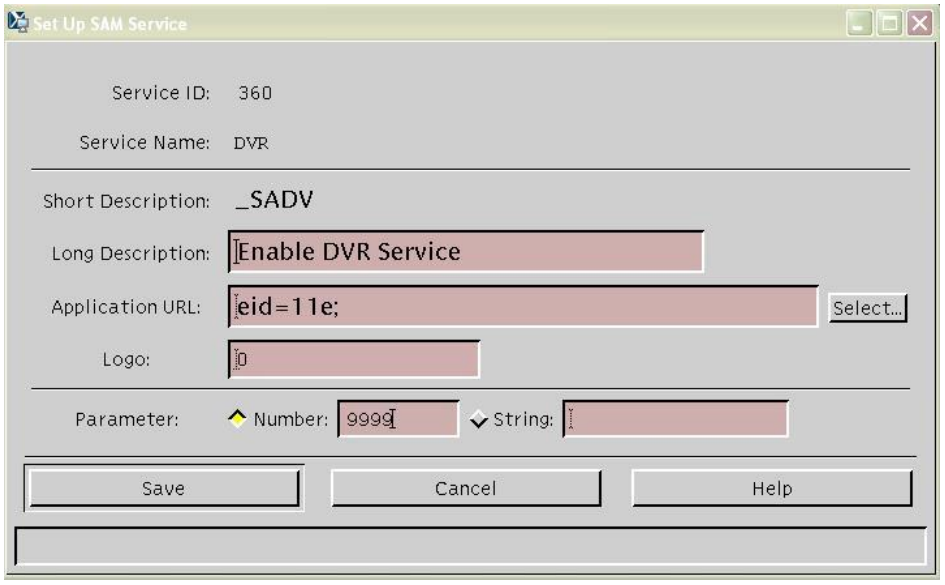
– If **no**, enter **eid=<EID value>;** using the the EID information you recorded in step x of the ***Determine the EID Value*** (on page 322) procedure.
Note: One package can support multiple services by reusing the EID information for each associated service.

- **Logo** - Are you creating a service for a Walled Garden?
  – If **yes**, enter the logo ID.
  – If **no**, leave blank; a default logo will be displayed.

  Note: The logo will also function in the EPG in the same way current channel logos function.

- **Parameter** - Select the bullet next to **Number** and type **0** in the field.

  Example: Set Up SAM Service Window



5 Click **Save**.

22

Stopping and Restarting the ISDS

Introduction

We recommend that you restart the ISDS 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 ISDS.

Important: You must restart the ISDS in the proper order. Otherwise, some processes may not function properly.

This section contains the procedures you need to follow when shutting down and restarting the ISDS.

In This Chapter

Before You Begin

Important: If you are upgrading the ISDS, do not use the procedures in this section to restart the ISDS after the upgrade. Instead, use the procedures provided in the upgrade installation instructions that came with the upgrade software.

You must have the dncs user password to complete some of the tasks necessary to restart the ISDS. If you do not know the password, contact your system administrator.

You Need to Know

Time to Complete

Performance Impact

Process Overview

Properly stopping and restarting the ISDS involves completing the following tasks in order:

1. ***Stop the Network Management System*** (on page 330) (if used)
2. ***Stop the Application Server Processes*** (on page 331)
3. ***Stop the ISDS Processes*** (on page 332)
4. ***Restart the ISDS Processes*** (on page 334)
5. ***Restart the Application Server Processes*** (on page 335)
6. ***Restart the Network Management System*** (on page 336) (if used)

Stop the Network Management System

Complete these steps to stop the network management system (NMS).

Important:

- If you use an NMS from a vendor other than Cisco, stop your NMS in accordance to that vendor's instructions.
- If you are restarting the ISDS, you must complete this procedure first. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1. On the ISDS Administrative Console Status window, click **Control** in the NMS area. The Select Host Machine window opens with the NMS Control Panel in the background.
2. Click OK. The Select Host Machine window closes and the NMS Control Panel window is in the forefront.
3. Click **Stop SpectroSERVER**. A confirmation window opens.
4. Click **OK**. The system begins shutting down the NMS. When finished, the Status field at the bottom of the NMS Control Panel changes to "Inactive."
5. Click **Exit**. A confirmation window opens.
6. Click **OK**. The NMS Control Panel window closes.
7. Are you restarting the ISDS?
   - If **yes**, your next step is to stop all of the processes on the Application Server. Go to ***Stop the Application Server Processes*** (on page 331).
   - If **no**, you are finished with this procedure.

Stop the Application Server Processes

Complete these steps to stop all of the processes on the Application Server.

Important:

- If you are using an application server from a vendor other than Cisco, stop your application server in accordance to the vendor's instructions.
- If you are restarting the ISDS, complete this procedure only after you stop your network management system (if you use one). Restarting the ISDS in the incorrect order could cause some processes to function incorrectly. Refer to ***Stop the Network Management System*** (on page 330) for more information.

1. Open an xterm window on the Application Server.
2. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
3. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all Application Server processes, along with their current working states ("running" or "stopped").
4. Use the mouse to place the cursor on any open area on the Application Server desktop click the middle mouse button, and select **App Serv Stop**. The Application Server begins shutting down all of its processes. This takes approximately 2 minutes to complete.
5. Press **Enter** to update the working states of the Application 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.
6. Are you restarting the ISDS?
   - If **yes**, your next step is to stop all of the processes on the ISDS. Go to ***Stop the ISDS Processes*** (on page 332).
   - If **no**, you are finished with this procedure.

Stop the ISDS Processes

Complete these steps to stop all of the processes on the ISDS.

CAUTION:

When you stop ISDS processes, two-way communication also stops in the network. You will not be able to offer any PPV, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage set-tops.

Important: If you are restarting the ISDS, complete this procedure only after you stop the network management system and the Application Server processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly. See ***Stop the Network Management System*** (on page 330) and ***Stop the Application Server Processes*** (on page 331) for more information.

1. On the ISDS Administrative Console Status window, click the **Control** button in the ISDS area. The ISDS Control (or Monitor) window opens with a list of all the ISDS 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 ISDS desktop (but not on the ISDS Administrative Console), click the middle mouse button and select **DNCS Stop**. The ISDS begins shutting down all of its processes.

   Note: 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 ISDS Control window should have a red working state, which indicates that they are not running.

   In addition, the ISDS area of the ISDS Administrative Console Status window will change to "Inactive."
3. Open an xterm window on the ISDS.
4. Type **dncsControl** and press **Enter**. The Dncs Control main menu opens in another xterm window.
5. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all ISDS processes, along with their current working states ("running" or "stopped").
6. Press **Enter** to update the working states of the ISDS processes.
7. 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 ISDS?

- If **yes**, your next step is to restart all ISDS processes. Go to ***Restart the ISDS Processes*** (on page 334).
- If **no**, you are finished with this procedure.

Restart the ISDS Processes

After you stop all of the processes on the ISDS, complete these steps to restart them.

Important: You must restart the ISDS and its processes in the correct order. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1. On the ISDS Administrative Console Status window, click the **Control** button in the ISDS area. The ISDS Control window opens with a list of all the ISDS processes and their working states. A red state indicates that a process is not running.
2. Use the mouse to place the cursor on any open area on the ISDS desktop(but not on the ISDS Administrative Console), click the middle mouse button and select **DNCS Start**. On the ISDS 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.
3. Your next step is to restart all of the processes on the Application Server. Go to ***Restart the Application Server Processes*** (on page 335).

Restart the Application Server Processes

Complete these steps to restart all of the processes on the Application Server.

Important:

- If you are using an application server from a vendor other than us, restart your application server in accordance to the vendor's instructions.
- If you are in the process of restarting the ISDS, complete this procedure only after you restart all the ISDS processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly. See ***Restart the ISDS Processes*** (on page 334) for more information.

1. Open an xterm window on the Application Server.
2. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
3. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. A list appears of all the Application Server processes and shows their current working states.
4. Do all processes show **Curr Stt: running(2)**?
   - If **yes**, go to step 10.
   - If **no**, continue with step 5.
5. Use the mouse to place the cursor on any open area on the Application Server desktop, click the middle mouse button and select **App Serv Start**. The Application Server begins to restart all of its processes.

   Note: This takes approximately 2 minutes to complete.
6. Press **Enter** every few seconds to update the working states until all processes show **Curr Stt: running(2)**.
7. Type **x** and press **Enter** to return to the Applications Control main menu.
8. Type **x** and press **Enter** again to close both the Applications Control main menu and the second xterm window.
9. In the first xterm window, type **exit** and press **Enter** to close the first xterm window.
10. Are you in the process of restarting the ISDS?
    - If **yes**, your next step is to restart the network management system. Go to ***Restart the Network Management System*** (on page 336)
    - If **no**, you are finished with this procedure.

Restart the Network Management System

Complete these steps to restart the NMS.

Important:

- If you are using an NMS from a vendor other than us, restart your NMS in accordance to the vendor's instructions.
- If you are in the process of restarting the ISDS, complete this procedure only after you restart the Application Server processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly. Refer to ***Restart the Application Server Processes*** (on page 335) for more information.

1. On the ISDS Administrative Console Status window, click **Control** in the NMS area. The Select Host Machine window opens with the NMS Control Panel in the background.
2. Click **OK**. The Select Host Machine window closes and the NMS Control Panel window is in the forefront.
3. Click **Start SpectroSERVER**. The system begins restarting the NMS. When finished, the Status field at the bottom of the NMS Control Panel changes to "Running."
4. Click **Exit**. A confirmation window opens.
5. Click **OK**. The NMS Control Panel window closes.

Restart a Session

Quick Path: ISDS 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 ISDS Administrative Console, click the **System Provisioning** tab.
2. Click **Source**. The Source List window opens.
3. Select the source for the session, click **File > 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 > 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 click **Next**. The Session Setup window opens.
7. If necessary, select the correct input device, and click **Next**. The Select Outputs window opens.
8. Select the modulator 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, hold down the Ctrl key on your keyboard as you click on each modulator.
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 ISDS database, and starts the session you built for it. The Source Definition List window updates to include the new source information.

23

Monitoring Your ISDP

Introduction

This section contains information on ISDS status, monitoring ISDS and Application Server processes, monitoring network elements, set-top performance, and network performance monitoring.

In This Chapter

Status at a Glance

The ISDS Administrative Console Status window helps you determine the status of the ISDS and of the Application Server.

For more information, click one of the following:

- *ISDS Status* (on page 340)
- *Application Server Status* (on page 340)

ISDS Status

The ISDS section of the Administrative Console Status window indicates whether the ISDS software is in operation based on the following conditions:

- **Running** - The ISDS software package is present and in operation
- **Inactive** - The ISDS software package is present, but not in operation

In addition, if you click the **Control** button in the ISDS section, the ISDS Control window opens, which allows you to monitor all of the major ISDS processes.

Application Server Status

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

- Running — The Application Server software package is present and in operation.
- Inactive — The Application Server software package is present, but not in operation.
- Not Responding — The Application Server does not respond when the ISDS tries to communicate with it.
- Not Installed — An Application Server host is defined in the host table, but the Application Server software package is not present; usually indicates that you are not using the Application Server, but the application server of another vendor.
- Blank — No Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using the Application Server, but the application server of another vendor.

When you click the **Control** (or **Monitor**, depending on how the Application Server was installed) button in the AppServer section, the AppServer Control window opens, which allows you to monitor all of the major Application Server processes. See ***Application Server Processes*** (on page 354) for more information.

CAUTION:

Do not attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.

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

- IPGServer-language supported (Interactive Program Guide Server) - Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, Arabic, and Japanese.

  Note: Each language that is supported has its own application. For example, if English is supported, the application would be listed as IPGServer-eng.

Network Element Status

If you are using the NMS, you can use the Alarm Manager to check on the status of your network elements Monitor button in the NMS area of the ISDS Administrative Console Status window.

The Alarms area of the ISDS Administrative Console Status window indicates the number of critical (Cr), major (Mj), and minor (Mn) alarm conditions present in the network. When you click the **Monitor** button in the Alarms area of the ISDS Administrative Console Status window, the Alarm Manager window opens.

The following example shows no critical alarms, so the associated box is gray. If there were any critical alarms, the Cr box would be red. Major alarms appear as orange, and minor alarms appear as yellow.

Alarm Severity

The following table describes each alarm severity level.

Alarm Severity	Description
Critical	A condition occurred that is affecting service.
Major	A condition occurred that will affect service if not corrected.

Minor	A condition occurred that is not affecting service, but could degrade system performance if not corrected.

Flow Monitoring

You can monitor the network flows in your system by using the Configuration Summary window.

1. From the ISDS Administration Console, click the **Utilities** tab.
2. Click **Configuration Summary**. The ISDS Configuration Summary window opens and displays the following information on the IP multicast flows:
   - **Tier -** The level in the system hierarchy of each flow. You should see the following tiers:
     - **System Wide Flow -** The IP names or address of the various video application servers in the system and a code verification table (CVT) that tells the set-tops in the system when to upgrade their code.
     - **Site Flow -** The layout of sites and determines at which sites the various hubs are located.
     - **Hub Flow -** The system information (SI) table which contains service parameters for each service in the system.
     - **Cluster Flow -** Provides a way for the ISDS to send messages to one or more set-tops.
     - **BFS Flow -** The primary interface (means of communication) between the Application Server and the set-tops that are connected to the network.
   - **Multicast IP -** Displays the multicast IP address for each component in the flow, if applicable.
   - **Enabled -** Displays whether that particular component is able to be used.
   - **Site -** If you are using an RCS, displays the site to which the flow is assigned.

   Note: For more information on the flows in the ISDS, see ***Flows*** (on page 569).

DashBoard

The DashBoard gives you an at-a-glance view of the health of your system. Graphs of key indicators provide real-time information that assist you in monitoring your system. To help you ensure the system performs as expected, troubleshooting assistance is provided for each key indicator.

DashBoard Indicators

The DashBoard provides a graph of each of the following key indicators. Each graph is displayed in a rolling 24-hour window (if 24 hours of data is available). The DashBoard begins collecting data as soon as the ISDS processes are started.

- **DNCS Idle CPU %** - Shows the percentage of the CPU that is currently not being consumed.

  Target: 20% or less for a 15-minute period. If outside this target, take troubleshooting action.

- **DNCS Database Process CPU %** - Shows the percentage of the CPU that the ISDS database is currently consuming.

  Target: 30% or less for a 15-minute period. If outside this target, take troubleshooting action.

- **DNCS Process CPU %** - Shows the percentage of the CPU that ISDS processes are currently consuming.

  Target: 50% or less for a 15-minute period. If outside this target, take troubleshooting action.

- **Free Memory %** - Shows the percentage of total memory that is available for use.

  Target: Actual percentage will vary from system to system, but should show a fairly level trend from day to day. If the trend continues to rise over a period of days (indicting an upward trend), take troubleshooting action.

Display DashBoard Indicators

Quick Path: ISDS Administrative Console Status > DashBoard area > Launch

Follow these instructions to view any of the DashBoard indicators:

1. From the ISDS Administrative Console Status, click the **Launch** button in the DashBoard area. The DashBoard window opens and displays a list of the indicators.
2. To display a DashBoard indicator, click the **+** button to the left of the indicator.A graph opens and shows the status of the indicator being monitored. All graphs show the following data:

- Each graph is displayed in a rolling 24-hour window (if 24 hours of data is available).
- Time is shown along the X-axis in one-minute increments.
- The **Page** tool appears beneath each graph. This tool shows the number of pages the graph spans and allows you to move through the pages of the graph to view all of the data.

3 Follow these instructions to move through the pages of the graph and display data from any time within the last 24 hours:

- To move backward in time, click the **<** arrow.
- To move forward in time, click the **>** arrow.
- To move forward to the most recent data available, click the **>|** arrow.
- To move backward to the oldest data available, click the **|<** arrow.
- To move to other data, enter a number in the **Page** field and click **Go**.

4 To close the DashBoard window, click **File > Quit**.

Troubleshoot with DashBoard Indicators

Quick Path: ISDS Administrative Console Status > DashBoard area > Launch > Troubleshoot

This section provides troubleshooting assistance for DashBoard indicators that are outside of their target ranges.

DNCS Idle CPU %

When this indicator shows 20% or less for a 15-minute period or more, take the following actions. Otherwise, the system is operating as expected.

Possible Causes	Check and Correct
■ A runaway process or processes ■ Too many processes are running ■ Insufficient CPU resources	Display the DashBoard indicator for **DNCS Process CPU** % and determine the status of this indicator: ■ If the DNCS Process CPU % is less than 50% over a 15-minute period, the system is functioning within normal operating levels and does not require further troubleshooting. ■ If the DNCS Process CPU % is more than 50% consistently over a 15-minute period, use the **prstat** command to identify the ISDS processes that contribute to the high utilization. Then check the ***DNCS Database Process CPU %*** (on page 345). **Note:** Refer to the man page for usage and options for this command.

DNCS Database Process CPU %

When this indicator shows 30% or greater consistently over a 15-minute period or more, contact Cisco Services. In other instances, use the following table to troubleshoot.

Possible Causes	Check and Correct
■ A runaway process or processes ■ Too many processes are running ■ Insufficient CPU resources	Use the **prstat** command to identify the ISDS processes that contribute to the high utilization. **Note:** Refer to the man page for usage and options for this command.

DNCS Process CPU %

When this indicator shows 50% or greater for a 15-minute period or more, take the following actions. If they do not resolve the memory issue, contact Cisco Services.

Possible Causes	Check and Correct
■ A runaway process or processes ■ Too many processes are running ■ Insufficient CPU resources	Use the **prstat** command to identify the ISDS processes that contribute to the high utilization. **Note:** Refer to the man page for usage and options for this command.

Free Memory %

When this indicator shows an upward trend over a period of several days, take the following actions.

Possible Causes	Check and Correct
■ Memory leaking	**1** Use the **prstat** command to identify the process or processes that contribute to the trend by manually recording the data over several days. **Note:** Refer to the man page for usage and options for this command. **2** Check the absolute memory size of the processes. If any single process is using more than 250 Mbyte of memory, contact Cisco Services for assistance.

ISDS Processes

This section discusses the various ISDS processes available, their working states, and how to stop and restart them.

Monitoring ISDS Processes

You can monitor all of the major ISDS processes by clicking the Control button in the ISDS area of the ISDS Administrative Console Status window to open the ISDS Control window. The ISDS Control window provides a list of all the major processes on the ISDS workstation, along with the working state of each.

We recommend that you leave the ISDS Control window open and visible at all times to help you monitor your system.

Working States of ISDS 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, or is tied up while processing data.
- **Red —** The process has stopped or did not start.

After the ISDS 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. Go to ***Troubleshooting Your ISDP*** (see "***Troubleshooting***" on page 531) for instructions on the corrective action to take.

CAUTION:

Do not attempt to start or stop a ISDS process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.

ISDS Processes

The following table describes each of the processes listed on the ISDS Control window.

Process	Description
bfsRemote	**Broadcast File System (BFS) Remote** — Process responsible for the establishment and maintenance of Broadcast File System (BFS) dataPump processes. These dataPump processes carouse, or continuously transmit, BFS data to the set-top population using pre-configured multicast data flows.
bfsServer	**BFS Server** — Process responsible for BFS data ingest, encode, and dispatch to the bfsRemote process, which, in turn, propagates this information to a given set-top population using pre-configured multicast data flows.
bossDiagnosticsServer	**Business Operations Support System (BOSS) Diagnostics Server** — Diagnostics server-Acts as an SNMP proxy agent between the billing systems and the set-tops by going through the ISDS to retrieve information from set-top for the billing system.
bossServer	**BOSS Server** — Responsible for receiving BOSS/BASS transactions from the billing system and dispatching them to the proper ISDS process layer subsystem for further processing. For example, set-top staging information is received by this process and forwarded to the camAm process, which will generate initial authorizations (that is, EMMs) and forward those on the given set-top.
bsm	**Broadcast Segment Manager** — Not used in the ISDS.
caaServer	**CA Authority (CAA) Server** — Not used in the ISDS.
camAm	**CA Manager (CAM) Authorization Manager** — Not used in the ISDS.
camAuditor	**CAM Auditor** — Not used in the ISDS.
camEx	**CAM Exclusive Sessions** — Not used in the ISDS.
camFastRefresh	**CAM Fast Refresh** — Not used in the ISDS.
camPsm	**CAM Program Segment Manager (PSM)** — Not used in the ISDS.
camTEDChecker	**CAM Transaction Encryption Device (TED) Checker** — Not used in the ISDS.
dncsSnmpAgent	**Digital Network Control System Simple Network Management Protocol (SNMP) Agent** — Receives alarm information from ISDS-managed network elements and forwards this information to a "North Bound Interface" for use by Network Management Systems (NMS) or the Alarm Manager.

drm	**Digital Resource Manager —** As a component of the Session and Resource Management (SRM) subsystem, DRM manages the allocation of network resources for establishment and maintenance of sessions on ISDS-controlled elements, such as Netcrypts.
dsm	**Digital Session Manager —** Manages digital video sessions on the ISDS.
EARS	**Emergency Alert Receiver Server —** Monitors a designated port on the ISDS to receive Emergency Alert Messages (EAMs). When EAMs are received this process looks for the audio file for the EAM in an ISDS resident FTP directory and sends the EAM to another ISDS resident subsystem, the Multi-media Messaging Server (MMMServer). **Note:** This process is used only on systems in the United States.
emmDistributor	**EMM Distributor —** Distributes EMMs to set-tops by applying algorithms to arrive at a time interval which ensures that all set-tops within a given video system receive new authorization "refreshes" before previous authorizations expire.
eventManager	**Event Manager —** A central, generic event manager for the platform, which operates on a Publisher/Subscriber paradigm where "Publisher Processes" publish events to the eventManager and interested subscribers "subscribe" to events brokered by the eventManager.
gemServer	**Generic Element Manager (GEM) —** A process used to provision video sources on the Cisco Visual Quality Experience (VQE) device from the ISDS.
hctmConfig	**Home Communications Terminal (HCTM) Configuration —** Exchanges and periodically transmits DSM-CC user-to-network configuration (UNconfig) information to a given set-top population. **Note:** Operating based on the DSM-CC messaging model, the UNConfig information is configuration information that is exchanged between the set-top operating in the role of the DSM-CC Client-User (U) and the ISDS in the role of the DSM-CC Network (N). This information tells DHCTs where to find system information, program information, and so on.
hctmInd	**HCTM Indications —** Handles the periodic UNConfigIndication messages transmitted from the set-top population.
idm	**Inventory and Directory Manager —** Provides a repository for public key certificates for set-tops and service providers.
ippvManager	**Impulse-Pay-Per-View (IPPV) Manager —** Not used in the ISDS.
ippvReceiver	**Impulse-Pay-Per-View (IPPV) Receiver —** Not used in the ISDS.

logManager	**Logging Manager** — This is a central, generic process, which receives logging data from other running ISDS/DNCS processes and writes it into one of the following media types for use by operations personnel: ■ ISDS application logs ■ ISDS data/text file ■ ISDS UI screen (future use) **Note:** One of the most important features of this process is the fact that its initiation for any given process is "dynamic," which means that the given process from which the operator needs log information will not require a restart to initiate the new logging.
MMMServer	**Multi-Media Message Server** — Converts audio files that reside in the ISDS resident FTP directory into the Audio Interchange File Format (AIFF) and places it on the BFS in the MMMAud Server. Then it sends the EAM to the ISDS resident "PassThru" process, which delivers the EAM to all set-tops. **Note:** This process is used only on systems in the United States.
mgrUIServer	**GUI Server Manager** — This process operates as a proxy for messages going to/from the ISDS Presentation Layer (that is, the Graphical User Interface [GUI]) and Web User Interface (WUI) screens. It receives XML/Soap messages and transmits those message on via RPC IPC to other process layer components, which will, in turn, operate on those messages.
osm	**Operating System (OS) Manager** — Allows you to load image files into the BFS that can then be distributed to set-tops (for example, OS images, resident application images, and other application images). **Important:** Will show as yellow while the manager is processing images. Do not attempt to load another image file until the osm has finished processing the previous image (when the status indicator shows green again).
PassThru	**PassThru** — Sends pass-thru Digital Storage Media Command and Control (DSM-CC) messages to set-tops.
pkeManager	**PowerKEY Element Manager** — Manages and maintains requests/reservations for stream/session encryption on our Netcrypt devices.
ResAppServer	**Resident Application Server** — Processes miscellaneous request message traffic sent from our SARA Application Server. For example, requests from the ISDS-Resident 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).

sseManager	**Server-Side Entitlement Manager** — Retrieves our entitlement information and provides it to a third-party application (Client-Side Entitlement Manager) in the format that application requires. The application then matches the information to its entitlement information so authorized clients can view the service the application provides.
stunServer	**Stun Server** — Facilitates the communication between the ISDS and the subscribers' set-top boxes.

Stop ISDS Processes

This section describes the procedures you need to follow to stop individual ISDS processes and to stop all ISDS processes.

Stopping Individual ISDS Processes

1. On the ISDS Control window, click to highlight the process name.
2. Click **Process > Stop Process**. In a few minutes, the indicator for the process changes from green to red.

   Important: Do not attempt to restart the process until the indicator has changed to red.

Stopping All ISDS Processes

Complete these steps to stop all of the processes on the ISDS.

CAUTION:

When ISDS processes are stopped, two-way communication also stops in the network. You will not be able to offer any PPV, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage set-tops.

Important: If you are restarting the ISDS, complete this procedure only after you stop the network management system and the Application Server processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1. On the ISDS Administrative Console Status window, click the **Control** button in the ISDS area.

   Note: This may be a Monitor button, instead of a Control button.
2. The ISDS Control (or Monitor) window opens with a list of all the ISDS processes and their working states. A green working state indicates that a process is running.

3 Use the mouse to place the cursor on any open area on the ISDS desktop, but not on the ISDS Administrative Console, and then click the middle mouse button. A list of options appears.

4 Click the left mouse button and select **DNCS Stop**. The ISDS 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 ISDS Control window should have a red working state, which indicates that they are not running. In addition, the ISDS area of the ISDS Administrative Console Status window will change to "Inactive."

5 Open an xterm window on the ISDS.

6 At the prompt, type **dncsControl** and press **Enter**. The Dncs Control main menu opens in another xterm window.

7 Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all ISDS processes, along with their current working states ("running" or "stopped").

8 Press **Enter** to update the working states of the ISDS 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.

9 Type **x** and press **Enter** to return to the Dncs Control main menu.

10 Type **x** and press **Enter** again to close both the Dncs Control main menu and the second xterm window.

11 Are you in the process of restarting the ISDS?

   - If **yes**, your next step is to restart all ISDS processes. Go to ***Restarting All ISDS Processes*** (on page 352).
   - If **no**, you are finished with this procedure.

Restart ISDS Processes

This section describes the procedures you need to follow to start or restart individual ISDS processes and to stop all ISDS processes.

Restarting Individual ISDS Processes

1 On the ISDS Control window, click to highlight the process name.

2 Click **Process > Start Process**. In a few minutes, the indicator for the process changes from red to green.

Restarting All ISDS Processes

After you stop all of the processes on the ISDS, complete these steps to restart them.

Important: You must restart the ISDS and its processes in the correct order. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1. On the ISDS Administrative Console Status window, click the **Control** button in the ISDS area. The ISDS Control window opens with a list of all the ISDS processes and their working states. A red state indicates that a process is not running.

   Note: 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 ISDS desktop, but not on the ISDS 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 ISDS 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 green. Do not go to the next step until all of the processes are green.

4. Are you in the process of restarting the ISDS?

   - If **yes**, your next step is to restart the Application Server processes. Go to ***Restarting Application Server Processes*** (on page 394).
   - If **no**, you are finished with this procedure.

Application Server Processes

This section discusses the various Application Server processes.

Monitoring Application Server Processes

You can monitor all of the major Application Server processes by clicking the **Control** button in the AppServer area of the ISDS Administrative Console Status window to open the AppServer Control window.

The AppServer Control window provides a list of all the major processes on the Application Server workstation, along with the working state of each. We recommend that you leave the AppServer Control window open and visible at all times to help you monitor your system.

Stop the Application Server Processes

Complete these steps to stop all of the processes on the Application Server.

Important:

- If you are using an application server from a vendor other than Cisco, stop your application server in accordance to the vendor's instructions.
- If you are restarting the ISDS, complete this procedure only after you stop your network management system (if you use one). Restarting the ISDS in the incorrect order could cause some processes to function incorrectly. Refer to ***Stop the Network Management System*** (on page 330) for more information.

1. Open an xterm window on the Application Server.
2. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
3. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all Application Server processes, along with their current working states ("running" or "stopped").
4. Use the mouse to place the cursor on any open area on the Application Server desktop click the middle mouse button, and select **App Serv Stop**. The Application Server begins shutting down all of its processes. This takes approximately 2 minutes to complete.
5. Press **Enter** to update the working states of the Application 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.
6. Are you restarting the ISDS?

- If **yes**, your next step is to stop all of the processes on the ISDS. Go to ***Stop the ISDS Processes*** (on page 332).
- If **no**, you are finished with this procedure.

Restart the Application Server Processes

Complete these steps to restart all of the processes on the Application Server.

Important:

- If you are using an application server from a vendor other than us, restart your application server in accordance to the vendor's instructions.
- If you are in the process of restarting the ISDS, complete this procedure only after you restart all the ISDS processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly. See ***Restart the ISDS Processes*** (on page 334) for more information.

1. Open an xterm window on the Application Server.
2. Type **appControl** and press **Enter**. The Applications Control main menu appears in another xterm window.
3. Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. A list appears of all the Application Server processes and shows their current working states.
4. Do all processes show **Curr Stt: running(2)**?
   - If **yes**, go to step 10.
   - If **no**, continue with step 5.
5. Use the mouse to place the cursor on any open area on the Application Server desktop, click the middle mouse button and select **App Serv Start**. The Application Server begins to restart all of its processes.

   Note: This takes approximately 2 minutes to complete.
6. Press **Enter** every few seconds to update the working states until all processes show **Curr Stt: running(2)**.
7. Type **x** and press **Enter** to return to the Applications Control main menu.
8. Type **x** and press **Enter** again to close both the Applications Control main menu and the second xterm window.
9. In the first xterm window, type **exit** and press **Enter** to close the first xterm window.
10. Are you in the process of restarting the ISDS?
    - If **yes**, your next step is to restart the network management system. Go to ***Restart the Network Management System*** (on page 336)
    - If **no**, you are finished with this procedure.

Set-Top Performance

You can monitor the set-top performance by turning on the performance monitoring function. Monitoring this performance can help you in troubleshooting your system should the need arise.

The set-top performance monitoring feature allows you to monitor certain data transactions that occur during the life cycle of the set up and tear down of set-tops. When you activate the set-top 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 set-top performance monitoring for the first time,you must create the **hctmpm.time** file in the /dvs/dncs/tmp/PerformanceMonitoring directory.

Create 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.

Note: UNIX commands are case-sensitive.

1. Open an xterm window on the ISDS.
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.

   Note: The zero ("0") in the previous command indicates the number of seconds between reporting intervals. Any value that is 10 or less indicates that set-top performance monitoring is turned off. The ISDS checks to see if set-top performance monitoring is turned on every three minutes (180 seconds).
4. Type **exit** and press **Enter**. The xterm window closes.

Activate or Modify Set-Top Performance Monitoring

After you create the hctmpm.time file, you can complete these steps to activate set-top performance monitoring. You can also use these steps to modify the reporting intervals.

Note: UNIX commands are case-sensitive.

1. Open an xterm window on the ISDS.
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 in the vi editor.
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 set-top data transactions.

   Example: If you want the system to perform this check every 5 minutes, type **300**.

   Note: Any value of 10 or less de-activates set-top performance monitoring.
5. Type **:wq** and press **Enter**. The system saves your change and closes the hctmpm.timefile. A prompt appears.
6. Type **exit** and press **Enter**. The xterm window closes.

De-Activate Set-Top Performance Monitoring

Complete these steps to de-activate set-top performance monitoring.

Note: UNIX commands are case-sensitive.

1. Open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/tmp/PerformanceMonitoring** and press **Enter**. A prompt appears.
3. Open the **hctmpm.time** file in a UNIX text editor.
4. Replace the value in the top line with any number that equals 10 or less.
5. Save and close the file. The system saves your change and closes the hctmpm.time file. A prompt appears.
6. Type **exit** and press **Enter**. The xterm window closes.

Read Set-Top Performance Report Files

When you turn on the set-top 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 a spreadsheet program, such as Microsoft Excel.

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 set-top 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.

Monitored Set-Top Data Transactions

The set-top 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 (not valid in ISDS) ■ Number of DAVIC connections lost (not valid in ISDS) ■ 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.

GUI Servers

Quick Path: ISDS 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 ISDS servers and database to the Web servers that provide the actual content for the Web-based windows on the ISDS Administrative Console.

Check Status of UI Managers

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > Select Server Manager screen

Follow these steps to view the status of UI Servers belonging to a particular Manager.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Utilities** tab.
3. Click **GUI Servers**. The Select Server Manager window opens and lists the UI Server Managers.

   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.
4. To close the Select Server Manager window, click **Exit**.

Modify UI Server Managers

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > [Select Server] > File > Open

From the primary UI management window, you can modify the parameters listed for a UI Server Manager. Follow these instructions to modify a UI Server Manager.

Note: This action is not normally performed on a production system.

1 From the ISDS Administrative Console, click the **ISDS** tab.
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**.
6 To close the Select Server Manager window, click **Exit**.

Manage UI Servers

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > Select Server Manager screen > Configure UI Servers > Configure UI Servers screen

From this screen, you can obtain an at-a-glance status of each application (UI Server) in your system. UI servers provide a link from the ISDS servers and database to the Web servers that provide the actual content for the Web-based windows on the ISDS 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.

Check Status of UI Servers

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > [Select Manager] > Configure UI Servers

Follow these steps to view the status of UI servers belonging to a particular manager.

Note: Applications (UI servers) provide a link from the ISDS servers and database to the Web servers that provide the actual content for the Web-based windows on the ISDS Administrative Console.

1 From the ISDS Administrative Console, click the **ISDS** tab.
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 Select button next to the Manager whose applications (UI Servers) you want to examine.
5 Click **Configure UI Servers**. 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 **Exit**.

Modify a UI Server

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > [Select Manager] > Configure UI Servers > [Enter Changes] > Save

Follow these instructions to modify an application (or UI Server).

Note: This action is not normally performed on a production system.

1 From the ISDS Administrative Console, click the **ISDS** tab. The ISDS 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 **Select** button next to the Manager whose applications (UI servers) you want to modify.
5 Click **Configure UI Servers**. 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**.
8 To close this window, click **Exit**.

Stop a UI Server

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > [Select Manager] > Configure UI Servers > [Select UI Server] > Stop

Sometimes you may need to stop and restart a UI server. For example, if the database is restarted, you will need to stop and restart the database UI server. Follow these steps to stop a UI Server.

1. From the ISDS Administrative Console, click the **ISDS** tab.
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 **Select** button next to the Manager whose UI Server you want to stop.
5. Click **Configure UI Servers**. 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**. The UI Server stops.
8. You can now start the UI Server you have stopped, or close this page by clicking **Exit**.

Start a UI Server

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > GUI Servers > [Select Manager] > Configure UI Servers > [Select UI Server] > Start

Sometimes you may need to stop and restart a UI server. For example, if the database is 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 ISDS Administrative Console, click the **ISDS** tab.
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 **Select** button next to the Manager whose UI Server you want to start.
5. Click **Configure UI Servers**. 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**. The UI Server starts.
8. To close this page, click **Exit**.

PCG Monitoring

The PCG uses a monitor application to ensure uptime and to manage upgrading.

The monitor daemon constantly monitors the health of the PCG. Data obtained from the monitor application is only intended for system maintenance and should never be required during normal system operation.

Important: Do not shut down or restart the monitor application.

If you issue a **quit** command from the **PCG>** prompt, the PCG software, as well as the monitor application, shuts down.

You can restart the monitor application by following the PCG setup procedure again. After the monitor application has been started, the PCG starts automatically. From that point on, the monitor application checks the health of the PCG.

Performance Monitoring

The Performance Monitoring tool allows you to display data collected from ISDS processes in a graphical format, such as a line chart. DHCT and VOD performance data is gathered from ISDS processes in comma separated value (CSV) files and is displayed in a graphical format to help you in maintaining and troubleshooting your system should the need arise.

Performance Monitoring Reports

The Performance Monitoring tool allows you to display data from the following reports in a graphical format, such as a line chart. For each Report, you can display the results of a single transaction or a combination of transactions as summarized in the following table.

Report Name	Process Monitored	Transactions Displayed in Graphical Format
Digital Resources Performance Flow	drm	■ Number of "allocate resources" requests and successes ■ Number of "release resources" requests and successes
QAM Manager Performance Flow	qamManager	■ Not valid in ISDS
Digital Sessions Performance Flow	dsm	■ Number of "create session" requests and responses ■ Number of "delete session" requests and responses
DHCT Signon Performance Flow	hctmMac	■ Number of DAVIC connections made (not valid in ISDS) ■ Number of DAVIC connections lost (not valid in ISDS) ■ 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

DHCT UNCONFIG Performance Flow	hctmConfig	■ Number of "UNConfig receive" requests ■ Number of "UNConfig request" confirms ■ Number of times the config input queue was detected as full
New DHCT Provisioning Performance Flow	hctmProvision	■ Number of "verify request received by provisioning" ■ Number of "verify response sent" ■ Number of "verify response sent" errors

Configure the Performance Monitoring Tool

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > Performance Monitoring > Configuration

The Configuration window allows you to control how frequently the Performance Monitor feature collects performance data.

Follow these instructions to change the data collection interval for the Performance Monitoring feature.

1. Click the **Data Collection Interval (seconds)** field and change the interval to the interval you desire.
2. Click **Save**. The Status area of the window displays "Configuration Saved Successfully."
3. To close the Configuration window, click **Exit**.

Display Performance Data

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > Performance Monitoring

To show transactions for any of the available reports in a graphical format, follow these instructions. When the report displays, follow the on-screen instructions to set or change how the data is displayed.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Utilities** tab.
3. Click **Performance Monitoring**. The main Digital Network Performance Monitoring window opens.
4. Make a selection from each of the following areas to set parameters for the data you would like to display.
   - Type of Graph
   - Start Date
   - End Date
   - Available Reports

5 Click **Display**. The Performance Flow window opens for the report you selected. Follow the on-screen instructions to set or change how you would like to view the data.

6 To close the main window, click **Exit**.

Note: To update the list of reports, select **Refresh List**.

Reports

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > Reports

The Report Writer software enables you to generate reports that collect data from the ISDS database, poll set-tops for information, and collect system information.

The reports are created in a Hypertext Markup Language (HTML) format, so you can view them online or through a Web browser and you can print them.

This section only contains information on running reports. For troubleshooting reports, see ***Reports Troubleshooting*** (on page 537). For information on installing and configuring Report Writer, refer to *Report Writer Version 4.3 for DNCS and ISDS User Guide* (part number 4021181).

Access to Report Writer requires that the user ID and password are different and unrelated to the system user ID and passwords.

Report Writer is shipped with the user name *sareports* and the password *report*. When adding users or changing passwords, follow these guidelines:

- The user name *sareports* should be the first entry after the group name.
- Each user name is separated by a space.
- In the following example, only the "normal" group has access to the reports.

  Example: normal: sareports [username] [username]

  Note: To remove a user, remove the user's name from the groups file.

Follow these instructions to add report writer users or to change a user's password.

1. Log in as **root** on the ISDS.
2. Type **cd /usr/local/apache2/bin** and press **Enter**.
3. Type **./htpasswd /usr/local/apache2/conf/users [username]** and press **Enter**. Replace [username] with the user you are adding or the user whose password you are changing. Do not type the brackets **[ ]** in the command.
4. Type and confirm the **password**.
5. Add the user to the groups file. Use a text editor to open the **/usr/local/apache2/conf/groups** file and append the user name to the line that begins with the word “normal.“

Display Reports

Quick Path: ISDS Administrative Console >ISDS tab > Utilities tab > Reports > [Select Report]

CAUTION:

Before opening Report Writer to display reports, exit all instances of your web browser associated with your UNIX user ID. When you try to open Report Writer with more than one instance of the browser associated with your UNIX user ID, a message appears on the screen stating that your browser has detected a locked file. Do not continue. If you attempt to continue, Report Writer may exhibit unpredictable behavior.

Follow these instructions to display reports.

1. From the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Utilities** tab.
3. Click **Reports**. A browser opens and displays the web server Welcome page.
4. Click **Report Manager**. A prompt for the user ID and password appears for the server where Report Writer software is located.
5. Type your **User ID** and **Password** and click **OK**.

   Note: The default user name is **sareports** and the default password is **report**. The browser displays the Reports page. Notice the hyperlinks to the specific reports and a brief description of each report. For more information about reports and how to access them, refer to Generating Reports.

Customize Reports

You can customize your reports by inserting your company logo or by sorting the reports to a format you prefer.

Insert Your Company Logo

You can customize reports by inserting your company's logo, in GIF format, at the top of each Report Writer page. To do this, exit your browser, name your logo file **top.gif**, and place it in the **/dvs/RepWriter/current/webspace/images** directory.

Sort the Generated Reports

You can display report data in a different order by sorting any column field. To sort a generated report, click the underlined column heading. After you click the column heading, it is no longer underlined. This indicates that the report was sorted by the selected column.

Note: Sorting a report does not regenerate the report data; it only displays the report data in a different order.

Generating Reports

This section describes the different report categories and provides instructions for generating the reports. Also included in this chapter are detailed descriptions of the reports within each category.

You Need to Know

Before You Begin

Generating Database Reports

1 From the ISDS Reports page, click the hyperlink for one of the ISDS Database reports. Did the selected report appear?

- If **yes**, the report generation is completed, the report name, the resulting data, and the message **Data Refreshed on MM/DD/YYYY @ HH:MM** appears, along with a **Run Report** button. (The HH:MM portion of the date/time stamp is in 24-hour time.)
- If **no**, continue with step 2.

2 Click **Run Report**. While the report is being generated, you may see the following message: **Running [report name]. Please wait.** A message appears stating that the report is completed and the number of records processed.

Note: If there is not any qualifying data for the report, only the report name, date/time stamp, and the Run Report button appear on the screen.

Descriptions of Database Report

The following table provides a description of each of the reports that collect data only from the ISDS database. These reports are listed in the order in which you will see them when you open Report Writer.

Notes:

- Not all of the following reports are applicable to the ISDS. Available reports are based on the implementation of your ISDS. If a report is not supported by the implementation, it will not appear in your options.
- Not all of the reports will contain data, depending on the unique implementation of the ISDS.

Report Title	Description
PPV Events	**Data listed:** All pending pay-per-view (PPV) events. **Data sorted by**: Service description and then by start date and time.
Zero Credit	**Data listed:** All In Service-Two Way DHCTs that have impulse pay-per-view (IPPV) events enabled and a credit limit of 0 (zero). **Data sorted by:** IP address **Normal condition:** Report should not show any data. **Troubleshooting:** DHCTs listed may have been incorrectly staged using the BOSS API. Restage and then re-run the report.

Report Title	Description
CableCARD Report	**Data listed:** All CableCARD™ modules that are bound to the system. **Data sorted by:** CableCARD MAC Address
CableCARD-DHCT Combo Device Report	**Data listed:** All CableCARD-DHCT combo devices that are bound to the system. **Data sorted by:** CableCARD MAC Address
Channels, Sources and Sessions Report	**Data listed**: Each display channel in the system, including all information about "carriage" of that channel. Duplicate sources will appear in this report; however, they will not display an associated session or access criteria information on the report. **Data sorted by:** Channel number
DHCT Report	**Data listed:** All DHCTs (set-tops) in the ISDS database and some DHCT configuration information. **Normal conditions:** This report can be extensive and not viewable on a workstation that has little free memory. It may take several minutes to generate/display this report. This report is most useful if you have a small number of DHCTs in your system. A DHCT listed in the database will not appear on this report if it is associated with a DHCT type that is not in the ISDS database.*
DHCT Packages Report	**Data listed:** All DHCTs and their associated packages with package details. **Note:** This report can be generated using the DHCT MAC Address or Package Name filtering options.
ISDS Packages Report	**Data listed:** All packages and their associated sources on the ISDS. Includes details of the sources which are assigned to a package. Reports can be run based on the package name or the source name. **Note:** The data in this report can be filtered by the name of the package or the name of the source.
PCG Report	**Data listed:** All PowerKEY® Conditional Access Gateways in the system and their status. **Note:** This report *only* appears if PCG is enabled on the ISDS.

Report Title	Description
PCG Session Report	**Data listed:** Details of the sources and sessions that belong to a VHO and are built on the PCGs in an ISDS 55-1 system. The PCG Session Report will not display records for a duplicate source. Since the duplicate source is using the session from the original source, there is no additional session on the PCG; therefore, no additional session appears on the PCG Sessions Report. **Note:** The data can be filtered by Frequency, MPEG Program Number, PCG IP Address, PCG Name, Source ID, and Access Criteria. This report only appears if RF+IP and 55-1 features are enabled.
SDV Servers Report	**Data listed:** All switched digital broadcast servers in the ISDS database and their settings. **Note:** This report *only* appears if SDV is enabled on the ISDS.
Service Group Report	**Data listed:** The service groups created on the ISDS. **Note:** No filtering options are provided for this report.
QPSK Modems	**Data listed:** All QPSK Modulators in the database and information about their configuration. **Normal condition:** A QPSK Modulator listed in the database will not appear on the report if it is associated with a hub that is not in the ISDS database.*
In Service One-Way	**Data listed:** DHCTs with an administrative status of In Service-One Way. **Normal condition:** Report Writer queries the ISDS database to identify DHCTs that have been configured for one-way service.
Non-Responding DHCTs-Never Connected	**Data listed:** DHCTs with an administrative status of In Service-Two Way or Deployment that do not have an IP address. **Normal condition:** Queries the ISDS database to identify DHCTs configured for two-way service that have never established a two-way connection in a DNCS or IP-only ISDS system. These DHCTs should have an IP address, but they do not. In and ISDS RF+IP 55-1 environment, these DHCTs have an Operational status of Unknown.

Report Title	Description
Non-Responding DHCTs-Lost Connection	**Data listed:** DHCTs with an administrative status of In Service-Two Way which have an IP address, but whose operational status is "Unknown," "MAC initialization failed," or "DSMCC boot failed." **Normal condition:** Queries the ISDS database to identify DHCTs configured for two-way service that have lost a previous two-way connection.
TSID List	**Data listed:** Lists transport stream IDs (TSIDs) used by QAMs from Cisco and other vendors. **Normal condition:** Queries the database to identify all TSIDs that have been used in the system.

*This situation should occur infrequently, if at all, and could indicate that some sort of ISDS database corruption has occurred. Try to open the applicable ISDS Administrative Console GUIs to ensure that the data is intact for a particular device.

Generating SNMP Poll Reports

1 From the ISDS Reports page, click **SNMP Poll Reports**.

2 Click the hyperlink of one of the SNMP Poll Reports.

3 Does the report appear on the screen:

- If **yes**, the data is from the last time the SNMP Poll Report was run. Click **Back** to return to the SNMP Poll Reports page; then click **Run Report** to refresh the report data.
- If **no**, go to step 4.

4 Does the following message appear on the screen?
This report has not yet been generated on your system. Please press the back button on your browser to return to the SNMP page.

- If **yes**, click **Back** to return to the SNMP Poll Reports page.
- If **no**, click **Run Report** to generate all of the SNMP Poll Reports.

Important: The SNMP Poll Reports can take a significant amount of time to complete, depending on the number of DHCTs (set-tops) in your system. While the SNMP Poll Reports are being generated, do not exit your browser. Exiting the browser while the reports are being generated can cause errors in the Report Writer software that will require some manual clean-up steps (see ***Reports Troubleshooting*** (on page 537)). We recommend that you do not click anywhere in your browser until the SNMP Poll Reports are completely generated.

Notes:

- While the reports are being generated, the following message appears: **Running [report name]. Please wait**.
- Concurrently, a table appears on the screen, and as each SNMP Poll report is generated, its status is updated from "working" to "complete."

5 When all the SNMP Poll reports are generated, click the browser **Back** button.

6 Click the hyperlink for a specific SNMP Poll Report.

7 Does the report appear on the screen?

- If **yes**, you have completed this procedure and all of the SNMP Poll Reports have been generated.
- If **no**, repeat this procedure.

Descriptions of SNMP Reports

The SNMP Poll Reports collect data by issuing up to three SNMP poll requests to each candidate DHCT (set-top).

- For DNCS environments, the term *candidate DHCTs* refers to DHCTs in the DNCS database that have an associated MAC address, IP address, QPSK Modulator, and QPSK Demodulator, along with an administrative status of In Service-Two Way. If a DHCT listed in the ISDS database does not meet all of these criteria, it will be excluded from the SNMP Poll Report. The SNMP poll request determines the current two-way communication ability of each DHCT.
- For ISDS environments, the term refers to DHCTs in the ISDS database that have an associated MAC address, and operational status equal to IP_Initialized or IP_55_1_Initialized, along with an administrative status of In Service-Two Way.

When the SNMP Poll Report is run, each candidate DHCT is polled (this is also called an SNMP "get" request). This SNMP poll collects all of the data necessary for generating the four SNMP Poll reports. The SNMP Poll reports are different views into the data collected.

If a DHCT does not respond to the initial SNMP poll, it is polled up to two more times (for a maximum of three attempts). If the SNMP poll is unsuccessful after three attempts, the DHCT is considered to be a non-responder and will appear only on the Non-Responding DHCTs-SNMP Poll Report. However, if at least one of the three SNMP poll attempts succeeds, then the DHCT will appear in the OS/App Version, Memory, and DHCT Uptime Reports.

Note: You can view the list of candidate DHCTs from the last SNMP Poll Report that was run by examining the **/dvs/RepWriter/current/bin/maclist** file.

The following table provides a description of each of the SNMP Poll Reports. These reports are listed in the order in which you will see them when you open Report Writer.

Note: Not all of the following reports are applicable to the ISDS.

Report Title	Description
Non-Responding DHCTs-SNMP Poll	**Data listed:** All DHCTs that did not respond to one of three SNMP "get" requests.

OS/App Version*	**Data listed:** The PowerTV® Operating System and Resident Application versions installed in each DHCT. **Notes:** ■ SARA is a Cisco resident application that is run on the DHCT that provides all basic functionality for the DHCT, including navigation, changing channels, volume control, etc. ■ Set-tops manufactured by other vendors have a different resident application installed to handle this functionality.
Memory Report*	**Data listed:** The total memory in each DHCT, and the amount of memory currently free.
DHCT Uptime*	**Data listed:** The amount of time since each DHCT last rebooted.

*The OS/App Version, Memory, and DHCT Uptime reports display data collected from both the SNMP "get" request and from the ISDS database.

Generating System Reports

1. From the ISDS Reports page, click **System Reports**.
2. The data for all the following reports are on this page. Click the hyperlink for a specific report to generate that report.

Descriptions of System Reports

The following table provides a description of each of the reports that collect and display information to provide a quick overview of the health of the ISDS system. These reports are listed in the order in which you will see them when you open Report Writer.

Note: Not all of the following reports are applicable to the ISDS.

Report Title	Description
General System Information	**Data listed:** ISDS system information (CPU, memory, and processes currently running).
File System Information	**Data listed:** Total and available disk space for the ISDS system.
Network Information	**Data listed:** Network interfaces and the routing table.
Database Information	**Data listed:** Information about the INFORMIX database on the ISDS. **Note:** This is the database used by the ISDS.

24

Maintaining Your ISDP

Introduction

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 network. To provide continuous, quality service to your subscribers, you must keep your system in top condition by performing certain tasks on a regular basis.

This section contains maintenance tasks and descriptions of tools available to help you keep your network in the best possible condition.

In This Chapter

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.

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. If you have questions about any of these tasks, contact Cisco Services.

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, see ***doctor*** (on page 397).

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.

Item	Objective	Doctor?	Notes
ISDS Processes	All running	Yes	saManager does not usually run on systems with Aptiv Digital Application Servers.
Application Server Processes	All running	Yes	Does not apply to systems with third-party Application Servers.
System Time Messages (STMs)	Delivered within the last 12 seconds	Yes	Need to enable siManager logging. Can also verify with a set-top. The set-top time comes from the STMs. Reboot a set-top. 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 third-party 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	Not valid in ISDS.
BFS Status	■ All carousels up ■ Sessions active ■ One process per carousel ■ BFSDir updated within the last 60 minutes	Yes	Make sure all data rates are under their recommended maximum.

Alarms	No alarms present	No
1 Minute DHCT 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

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.

Item	Objective	Doctor?	Notes
DNCS Corefiles	No core files	Yes	Capture all corefiles and deliver to Cisco Services, especially if they occur near the time of another problem.
Application Server Corefiles	No core files	Yes	Capture all corefiles and deliver to Cisco Services.
DNCS Disk Utilization	Each volume using less than 80%	Yes	
DNCS Swap Space	More than 200 Megabytes	Yes	
DHCT Software Associations	Make sure each set-top type is set to CVT	No	You can use the Image List GUI to view CVT associations.
Time Sync	■ DNCS synchronized with an external source ■ Application Server synchronized with the DNCS	Yes	
IPG	Seven days' worth of grid information available, along with long descriptions	Yes*	Doctor Report shows IPG file sizes only. You must manually check the IPG information through a set-top.
Third-Party Applications	Applications load and run successfully	No	
Clear Services	All services run	No	
Subscription Services	All services run	No	

Purchase Report	Information collected	No	
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	
DHCT Resets	Monitor number	No	■ Need to enable cmd2000 or hctmMac tracing. ■ Run signonCount for set-top 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 you 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.

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.

Item	Objective	Doctor?	Notes
Password Expiration for Critical Accounts	Review the status of password aging for critical Solaris accounts	No	■ See ***Password Expiration Check*** (on page 554) for information on running this check.
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% used	Yes	Use Informix utilities and the Doctor Report.
Tempspace	Less than 75% 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 set-tops	Monitor for growth	Yes	
Number of Source Definitions	Monitor for growth	Yes	
BFS Carousel Rates	Remain within recommended rates	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

- ***Every Two Weeks*** (on page 385)

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

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.

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.

After Every EMM CD Installation

After every EMM CD installation, run the Doctor Report to determine how many set-top types are installed in your system. You should have as few set-top types as possible and absolutely no "0 set-top" types.

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.

Spring and Fall Time Changes

After every Spring and Fall time change, run the Doctor Report to make sure that all hubs and set-tops have the correct DST settings.

Schedule Service Updates

Quick Path: ISDS Administrative Console > Application Interface Modules tab > SAM Config

In addition to various other functions, the SAM also communicates service operation attributes to the set-tops 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 ISDS waits after you make changes to the SAM or to a channel map before the ISDS generates new SAM files to be broadcast to set-tops. 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.

You Need to Know

- Before You Begin
- Time to Complete
- Performance Impact

Complete these steps to schedule the service updates through the SAM Update Timer setting.

1. On the ISDS 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 ISDS should wait after you make changes to the SAM or to a channel map before generating new SAM files to broadcast to the set-tops 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 that set-tops are 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 ISDS database and reconfigures the SAM to send broadcast service updates accordingly.
6. Click **Cancel** to close the SAM Configuration window and return to the ISDS Administrative Console.

Utilities

The ISDP utilities contains several utility programs that system operators and support engineers can use to manage and troubleshoot the network.

Logging into ISDS as Root User

The ISDP utilities require you to log into the ISDS as root user. Follow these instructions to log into the ISDS as root user.

1. If necessary, open an xterm window on the ISDS.
2. Type **su -** and press **Enter** to log in as root user.
3. Type the **root password** and press **Enter**.
4. Type **. /dvs/dncs/bin/dncsSetup** and press **Enter**. This command establishes the ISDS environment as a root user.

   Important: Type the period (**.**) followed by a space before typing **/dvs**.

   Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

Starting and Stopping Processes

Before following several of the ISDS Utilities procedures, you must first stop the Application Server and the ISDS. Follow these instructions to stop the Application Server and the ISDS.

Note: The act of stopping and starting processes is sometimes referred to as *bouncing* the process ("bounce the process").

Stopping All ISDS Processes

Complete these steps to stop all of the processes on the ISDS.

CAUTION:

When ISDS processes are stopped, two-way communication also stops in the network. You will not be able to offer any PPV, other on-demand services, or other third-party applications during this time. In addition, you will be able to offer only limited IPG functionality, and you will not be able to stage set-tops.

Important: If you are restarting the ISDS, complete this procedure only after you stop the network management system and the Application Server processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1. On the ISDS Administrative Console Status window, click the **Control** button in the ISDS area.

Note: This may be a Monitor button, instead of a Control button.

2 The ISDS Control (or Monitor) window opens with a list of all the ISDS processes and their working states. A green working state indicates that a process is running.

3 Use the mouse to place the cursor on any open area on the ISDS desktop, but not on the ISDS Administrative Console, and then click the middle mouse button. A list of options appears.

4 Click the left mouse button and select **DNCS Stop**. The ISDS 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 ISDS Control window should have a red working state, which indicates that they are not running. In addition, the ISDS area of the ISDS Administrative Console Status window will change to "Inactive."

5 Open an xterm window on the ISDS.

6 At the prompt, type **dncsControl** and press **Enter**. The Dncs Control main menu opens in another xterm window.

7 Type **2** to select **Startup/Shutdown Single Element Group** and press **Enter**. The system displays a list of all ISDS processes, along with their current working states ("running" or "stopped").

8 Press **Enter** to update the working states of the ISDS 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.

9 Type **x** and press **Enter** to return to the Dncs Control main menu.

10 Type **x** and press **Enter** again to close both the Dncs Control main menu and the second xterm window.

11 Are you in the process of restarting the ISDS?

- If **yes**, your next step is to restart all ISDS processes. Go to ***Restarting All ISDS Processes*** (on page 352).
- If **no**, you are finished with this procedure.

Stopping Application Server Processes

Complete these steps to stop all of the processes on the Application Server. If you are using an application server from a vendor other than us, stop your application server according to the vendor's instructions.

Important: If you are restarting the ISDS, complete this procedure only after you stop your network management system. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1 Use the mouse to place the cursor on any open area on the Application Server desktop,and 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 Application 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 Application Server desktop,and click the middle mouse button. A list of options appears.

6 Click the left mouse button and select **App Serv Stop**. The Application 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 Application 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 ISDS?

   - If **yes**, your next step is to stop all of the processes on the ISDS. Go to ***Stopping All ISDS Processes*** (on page 351)
   - If **no**, you are finished with this procedure.

Restarting All ISDS Processes

After you stop all of the processes on the ISDS, complete these steps to restart them.

Important: You must restart the ISDS and its processes in the correct order. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1 On the ISDS Administrative Console Status window, click the **Control** button in the ISDS area. The ISDS Control window opens with a list of all the ISDS processes and their working states. A red state indicates that a process is not running.

   Note: 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 ISDS desktop, but not on the ISDS 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 ISDS 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 green. Do not go to the next step until all of the processes are green.

4 Are you in the process of restarting the ISDS?

   - If **yes**, your next step is to restart the Application Server processes. Go to ***Restarting Application Server Processes*** (on page 394).

- If **no**, you are finished with this procedure.

Restarting Application Server Processes

Complete these steps to restart all of the processes on the Application Server. If you are using an application server from a vendor other than us, restart your application server according to the vendor's instructions.

Important: If you are in the process of restarting the ISDS, complete this procedure only after you restart all the ISDS processes. Restarting the ISDS in the incorrect order could cause some processes to function incorrectly.

1. Is the xterm window open on the Application Server that shows the working states of all Application 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 Application Server desktop,and 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 Application Server processes and shows their current working states.
6. Do all processes show **Curr Stt: running(2)**?
   - If **yes**, go to step 13.
   - If **no**, go to step 7.
7. Use the mouse to place the cursor on any open area on the Application Server desktop,and click the middle mouse button. A list of options appears.
8. Click the left mouse button and select **App Serv Start**. The Application 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.
13. Are you in the process of restarting the ISDS?
    - If **yes**, your next step is to restart the network management system. Go to ***Restart the Network Management System*** (on page 336).
    - If **no**, you are finished with this procedure.

Using Text Files With ISDS Utilities

Several utilities described in this section can act upon a single set-top or on a series of set-tops.

When a utility acts upon a series of set-tops, those set-tops are usually identified to the utility by a list of MAC addresses or serial numbers that are contained in a pre-prepared text file. This section provides general guidelines in preparing a text file containing a list of MAC addresses or serial numbers.

Some ISDS Utilities can accept, as an argument, an input text file containing a list of set-top MAC addresses or serial numbers. This section provides general guidelines that you should use when you prepare the input text file.

Guidelines for Preparing the Text Files

Use the following guidelines when preparing the input text file:

- Prepare the file using a standard text editor, such as vi.
- Prepare the file with one MAC address or serial number per line.

  Examples: (two examples using MAC addresses followed by one example using serial numbers)

  - 00:02:DE:4A:11:92
  - 00:02:DE:4A:11:93
  - 00:02:DE:4A:11:94
  - 0002DE4A1192
  - 0002DE4A1193
  - 0002DE4A1194
  - SABFXHXSB
  - SABFXHZQX
  - SABFXHXNQ
- Each MAC address or serial number must be left-justified on each line of text.
- Save the file using a name that is relevant to the contents of the file. Append the current date to the end of the file name.

  Examples:

  tellDhct-in_06.13.08 for a file that was created on June 13, 2008

  tellDhctInfo-in_06.13.08 for a file that was created on June 13, 2008
- We recommend that you save a file that you will use only once to the **/tmp**

directory on the ISDS. For a file that you may re-use, create a directory for the file under **/export/home**.

Preparing Text Files for ISDS Utilities

Follow these instructions to prepare a text file for use with an ISDS utility.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /tmp** and press **Enter**.
3. Open the text file with a UNIX text editor.
4. Insert your list of MAC addresses, SMSNs, or serial numbers into the file you have just opened.

   Important: Type only one MAC address or serial number per line.
5. Save the file and close the text editor.

ISDS Utilities

The ISDP Utilities CD includes a collection of utility programs called ISDS Utilities.

The following list contains the utilities available to the ISDS administrator and support engineer:

- ***doctor*** (on page 397): Compiles a report on system configuration.
- ***dncsDbData*** (on page 414): Unloads and loads the ISDS and Application Server database.
- ***hostnmchg*** (on page 429): Changes the hostname and IP address of the ISDS and the Application Server.
- ***checkDB*** (on page 432): Identifies and corrects set-top records in the ISDS database that do not contain serial numbers, required corresponding records in other tables, or that have EMMs ready to expire.
- ***keyFileFinder*** (on page 438): Compiles a list of customized files that need to be backed up separately before upgrading the ISDS system release (SR).
- ***listTftpConfigs*** (on page 440): Examine device configuration data quickly.
- ***ncdsGen*** (on page 443): Provides a mechanism for synchronizing channel map, service group, and VOD information between the NCDS server and the ISDS.
- ***podDataChk*** (on page 445): Quickly determine which CableCARD module/host pairs are being transmitted via the BFS carousel.
- ***slotchk*** (on page 449): Examines the Peripheral Component Interconnect (PCI) card configuration on the ISDS before an SR upgrade.
- ***runCvtGroup*** (on page 450): Expedites the process by which set-tops are assigned to download groups.

- ***cronCvt*** (on page 451): Easily place the DHCT host of a DHCT/embedded CableCARD pair into a download group.
- ***check_metadevices*** (on page 457): Monitors the status of system metadevices.
- ***qtail*** (on page 457): Monitors the log files of ISDS processes.
- ***sesstail*** (on page 460): Monitors the ISDS logfiles.
- ***syncwait*** (on page 462): Monitors the progress of mirrored disks as they synchronize their data.

Installation of the ISDS Utilities occurs automatically when you install the ISDP Utilities. Refer to *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (part number 4031374) for installation instructions for the ISDP utilities (see Printed Resources).

doctor

The Doctor Report is one of the most important tools that you can use to evaluate the configuration and operation of an ISDP. Output from the Doctor Report appears on the screen of the ISDS and is written to an output file for later analysis.

The Doctor Report was developed to generate a snapshot of system configuration. The following list contains some of the system configuration information reported by the Doctor Report:

- Installed software versions
- ISDS and Application Server disk partition utilization
- Status of ISDS and Application Server processes
- Summary of supported set-top types
- Summary of sources, source definitions, segments, and sessions
- Summary of PPV services and events (if applicable)
- Data carousel/pump status and rates
- Configuration data for remote sites
- Common configuration errors that may lead to problems later

Important: We strongly recommend that you run the Doctor Report at least once a day.

Options

You can run the Doctor Report with any of the options listed in the following table.

Each parameter causes the Doctor Report to generate output with specific configuration information.

Notes:

- One or more of the a, g, e, s, t, p, b, i, n, c, x, or q options is required.
- Options d and v are optional but should be used with a required option.

Option	Result
a	(Almost) All options (except q and x)
g	General ISDS information: ■ Installed software ■ ISDS and Application Server disk utilization ■ ISDS and Application Server swap space ■ Database utilization ■ Database extents ■ Load average ■ ISDS and Application Server debug flags ■ Tracing levels ■ ISDS and Application Server processes ■ ISDS and Application Server corefiles ■ DNS ■ Check force tune for valid service ■ ISDS license check ■ Large log file check ■ ISDS installation options
e	Element information: ■ Set-top state summary ■ Set-top type summary ■ Active elements ■ Mod slot tolerance ■ Source ■ Source definitions ■ Segments ■ Sessions ■ Subscription packages ■ EMMs expiring soon

s	SI information: ■ SI_INSERT_RATE ■ System time message ■ Distinguished SI QAM (not valid in ISDS) ■ SI out of band interval (not valid in ISDS)
t	Time information: ■ ISDS and Application Server time sync ■ Timezone ■ DST
p	PPV information: ■ PPV services and events ■ PPV and SAM service discrepancies ■ Event use services ■ PPV files ■ phoneactivetime ■ EUT ■ GBAMs
b	BFS information: ■ BFS carousels ■ BFS sessions ■ BFS source definitions
n	Ping elements: ■ QPSK (55-1) ■ QAM (optional) ■ TED ■ PCG
g	Not valid in ISDS.
x	Check one-one correspondence of set-tops and serial numbers. Not included in all (-a)
v	Verbose mode. Detailed output, even if OK.
d	Suppress screen output. Write to output file only.
h	Generate help text.

c	Clean up (delete) all but the last [number] of Doctor Reports. Use this switch independently of all others. A report is **not** generated using this switch.
r	...and use one of the following options: ■ **hubqamlist:** Not valid in ISDS. ■ **smdgInfo:** Not valid in ISDS. ■ **sdbsgInfo:** List SDB Service Group Mini Carousel info. ■ **genericQamInfo:** Not valid in ISDS. ■ **dualGbeqamInfo:** Not valid in ISDS. ■ **sdbInfo:** Display SDB server information and status. ■ **pcgInfo:** Display PCGs information and status.

Using doctor

Use the following procedures to run the Doctor Report on the ISDS:

- Running the Doctor Report
- ***Customizing the Doctor Report*** (on page 401)

Use the following procedure to run the Doctor Report on the ISDS.

1. Open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The /dvs/dncs/Utilities/doctor directory becomes the working directory.
3. Type **doctor** and press **Enter**. The system generates a list of parameters that you can use to run the Doctor Report.

   Note: Each parameter causes the Doctor Report to generate output with specific configuration information.
4. To generate a complete Doctor Report, type **doctor -av** and press **Enter**.

   Results:

   - The system generates the Doctor Report listing all system configuration information and directs the output of the report to the screen.
   - The system also saves the output of the Doctor Report to a file in the current directory on the ISDS.

   Example: The system saves the report with a name similar to **report.061026_0921.doc**.

   Notes:

   - Depending upon the size of your system, it may take a few minutes for the report to generate.
   - The final line of the report generated to the screen lists the file to which the output was saved.

- The report is a plain text file. You can view the report in a text editor of your choice.

Customizing the Doctor Report

Follow these instructions to customize your Doctor Report with the name of your system.

1. Open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/Utilities/doctor** and press **Enter**. The /export/home/dncs/doctor directory becomes the working directory.
3. Type **view doctor** and press **Enter**. The doctor file opens using the UNIX vi editor.
4. Type **/SYS_NAME** and press **Enter**. The system places the cursor on the line that contains SYS_NAME.
5. Type **:s/`uname -n`/"Site Name, location"/** and press **Enter**. The UNIX search and replace function automatically replaces the uname **-n** variable with the name and location of your headend.

   Note: Substitute the site name and location (city), for Site Name, location.

   Important: Be sure to enclose the site name and location in quotes.
6. Type **:wq** to save the file and exit the vi editor. When you generate a Doctor Report, your system name is clearly displayed at the top of the output file.

Understand the Data in a Doctor Report

The information in this section provides an explanation of the data produced by generating the Doctor Report. Some of the data is only for informational purposes. Other data is preceded by the words OK, Error, or Warning.

- **OK** indicates that the data meets our recommendations regarding the field to which the data applies.
- **Error** might indicate that some system process or function is not operating as it should. Where appropriate, this section includes troubleshooting tips so that system operators can investigate and correct a situation producing an error in a data field.
- **Warning** indicates that a potentially serious condition has been detected, such as a disk partition nearing capacity, or that certain data does not meet our recommendations.

Important: Any time an unexpected or new error appears in the Doctor Report output or if defined thresholds are about to be reached, contact Cisco Services for assistance.

System Name

The System Name field appears at the top of the Doctor Report, and displays the operational mode of the system (RF or IP/ISDS). This field can be customized to display the name of the system whose data is displayed in the report.

Note: If the System Name field does not reflect the name of your system, follow the instructions in ***Customizing the Doctor Report*** (on page 401).

All SAI Installed Package Information

The data in the All SAI Installed Package Information field contains the following information about the software packages installed on your system:

- The name of the package
- The version number of the package
- The date the package was installed
- The platform on which the package was installed

ISDS Info

Data fields included under ISDS Info contain information that pertains to the hardware configuration of your ISDS.

ISDS Uptime

The ISDS Uptime field shows how long the ISDS processes have been running without interruption.

Note: To determine how long the ISDS processes have been running without interruption, the Doctor Report examines the **bootpd** process and determines how long the bootpd process has been running without interruption. The bootpd process is usually only restarted when the ISDS processes are reset.

Solaris Uptime

The Solaris Uptime field shows how long the Solaris operating system processes have been running without interruption.

Swap Space

The Swap Space field lists the configured swap partitions in the ISDS and how large they are.

System Configuration

The System Configuration field contains configuration information that pertains to the central processing unit (CPU) of the ISDS.

Memory Size

The Memory Size field displays how much physical memory is installed in the ISDS.

Virtual CPUs

The Virtual CPU field is seen only on the UltraSPARC T2 sun4v architecture. The two CPUs have a total of 16 cores (2x8). However, they configure themselves as 128 virtual processors. Each of these processors acts like a real processor, which allows the sun4v architecture to support multi-threaded applications.

This section lists all 128 virtual processors (0-127) and reports if they are online.

Physical Memory Configuration

This field reports on the amount of installed memory in the server, as well as how that memory is arranged (for example, in banks of 4 GB). The banks of memory may change due to changes in the dual in-line memory module (DIMM) design, but the overall memory will remain constant.

IO Devices

This field lists all of I/O devices attached to the server.

Disk Info

The Disk Info field displays configuration information for the server from a partition point of reference (rather than a metadevice point of reference).

Additionally, the Disk Info field reports on the configuration of the server's mirrors.

Checking the Status of the Meta Devices of the System

The Checking the Status of the Meta Devices of the System field reports on the status of the system’s mirrored disks and reports any disks that have failed.

ISDS Service Delivery Server

The ISDS Service Delivery Server field contains the host names or IP addresses of various components of the ISDS.

ISDS Configuration Summary

The Hub Summary portion of the ISDS Configuration Summary field lists the ID, name, and multicast IP address if the configured hubs on the server.

The Cluster Summary portion of the ISDS Configuration Summary field lists configuration data for the system's clusters.

The Periodic UN-Config interval field shows the interval for UN-Config messages.

ISDS Disk Partition Utilization

The data in the ISDS Disk Partition Utilization field lists all the disk partitions on the ISDS and displays the “in-use” percentage of each partition.

Important: Our engineers recommend that no partition exceed 85 percent utilization.

Note: To decrease partition utilization, you can delete files that are no longer needed and core files that do not require analysis.

ISDS Swap Space

The data in the ISDS Swap Space field lists the amount of available swap space on the ISDS.

Important: Our engineers recommend that the ISDS swap space be greater than 200 MB.

Note: Completing the following tasks may increase your swap space:

- Close windows that do not need to be open.
- Stop and restart the ISDS.
- Run the **/usr/local/bin/top** utility and look for processes that use more than 50 MB of swap space. Use the dncsControl utility to stop and restart those processes.
- Look for large files in the /tmp directory. You can delete them or move them to another file system.

Basic System Performance Stats

There are 5 sets of performance statistics reported under the Basic System Performance Stats header. An explanation of each set follows.

CPU Performance

The CPU Performance field uses the prstat utility to iteratively examine all active processes on the system. As used in the Doctor Report (prstat -c 5 5), the prstat utility sorts output according to CPU usage, takes CPU measurements in 5-second intervals, and issues five separate reports.

Memory Usage

The Memory Usage field uses the prstat utility to iteratively examine all active processes on the system and report upon memory usage of the processes. As used in the Doctor Report (prstat -s size -c 5 5), the utility sorts output according to the size of the process image, takes memory measurements in 5-second intervals, and issues five separate reports.

Per-Processor Stats

The Per-Processor Stats field uses the mpstat utility to report processor statistics in tabular form. Each row in the tabular output represents the activity of one processor. The first table summarizes all processor activity since the last reboot. Subsequent tabular output summarizes activity for the preceding, specified interval. All values in the output are rates listed as events/second, unless specifically noted.

The mpstat utility, as used in the Doctor Report (mpstat 5 5), collects processor statistics in 5-second intervals and produces five reports.

Virtual Memory Stats

The Virtual Memory Stats field uses the vmstat utility to report statistics about kernel threads in the run and wait queue, memory, paging, disks, interrupts, system calls, context switches, and CPU activity.

As used in the Doctor Report (vmstat 5 5), the vmstat utility collects virtual memory statistics every 5 seconds and issues five separate reports.

Disk Stats

The Disk Stats field uses the iostat utility to iteratively examine terminal, disk, and tape input/output activity, as well as CPU utilization. The first line of output pertains to the time since the last reboot. Subsequent lines pertain to the specified prior interval, only.

For the Doctor Report (iostat -xPnMz 5 5), the utility produces extended statistics and displays names in descriptive per-partition format (rather than per-device format). Data is displayed in MB/second terms. The utility collects statistics every 5 seconds and issues five separate reports.

ISDS Database Check

The data in the ISDS Database Check field summarizes the usage of tempspace and dataspace in the ISDS database.

Important: This data should be interpreted only by those individuals knowledgeable in database management.

Database Spaces and Chunks

The Database Spaces and Chunks field reports on the contents and structure of the database shared memory by running the Informix *onstat -d* command.

Important: This data should be interpreted only by those individuals knowledgeable in database management.

Database Extents for dncsdb

The data in the Database Extents for dncsdb field lists the number of extents associated with specific tables in the ISDS database.

Note: The number of database extents refers to the number of times a specific table is fragmented across the hard drive.

Database Extents for appdb

The data in the Database Extents for appdb field lists the number of extents associated with specific tables in the Application Server database.

Database Backup Check

This field reports on the presence of a cron job to automatically back up the ISDS databases. If a cron job is present, this field reports whether the previous database backup was successful or if it failed.

Notes:

- A cron job is a program that runs automatically, without user intervention.
- The program that automatically backs up the database is a shell script called noinputDbBackup.sh. Your most recent system upgrade installation instructions may contain an appendix that describes how to configure your system for the automated database backup. The title of the appendix is **Setting Up an Automated Database Backup**.

Check for clearDbSessions Activity

The Doctor Report checks to ensure that the clearDbSessions entry in the crontab file of the ISDS is active, and has not been converted into a comment.

ISDS Load Average

The data in the ISDS Load Average field shows the average number of ISDS processes simultaneously waiting for CPU time on the previous day.

Important: Our engineers recommend that your ISDS load average remain under 2.0.

Note: The Doctor Report can determine the ISDS Load Average only if the Solaris **sar** utility is running. Refer to the UNIX man pages if you need to enable the sar utility.

Appserv Tracing Levels

The Application Server on the ISDS allows you to configure the level of detail reported by various system processes. The data in the Appserv Tracing Levels field lists all Application Server tracing levels that are set higher than 0 (zero).

Notes:

- Tracing is logged into the /var/log/dncsLog file on the ISDS.
- Tracing levels set higher than 0 (zero) run the risk of filling up hard drives and slowing system performance.

Important: Unless you are using tracing for a specific reason, we recommend that you set all of your Application Server tracing levels to 0 (zero). Call Cisco Services if you need help setting your Application Server tracing levels.

ISDS Logging Levels

The ISDS Logging Levels field lists all ISDS processes and the level of logging activity that is associated with each process.

System operators can set logging levels for the ISDS processes by clicking **Logging** from the **Utilities** tab of the Administrative Console.

ISDS Processes

The data in the ISDS Processes field lists all the ISDS processes and reports whether those processes are running, or not. Processes that are running are listed as **OK**; processes that are not running are listed as **Error**.

Important: Note the following recommendations regarding other processes that may not be running:

- Check the ISDS for core files.

  Note: The ***Recent ISDS Corefiles (last 2 days)*** (on page 407) field, lists recent ISDS core files.

- If the ISDS has a core file, contact Cisco Services.

  Note: Cisco Services may request that you send them the core file for analysis.

- Use the dncsControl utility to restart the stopped process(s).

App Server Processes

The data in the App Server Processes field lists all the Application Server processes that are running on the ISDS and reports whether those processes are running, or not.

Note: It may be normal for the orbixd process to show as not running.

Important: Note the following recommendations regarding other processes that may not be running:

- Check the ISDS for core files.
- If the ISDS has a core file, contact Cisco Services.

  Note: Cisco Services may request that you copy the core file and send it to them for analysis.

- Use the appControl utility to restart the stopped process(s).

Recent ISDS Corefiles (last 2 days)

The data in the Recent ISDS Corefiles (last 2 days) field lists any core files saved to the ISDS within the last 48 hours.

Note: A core file indicates that a process on the ISDS failed unexpectedly.

Important: Call Cisco Services if the Recent ISDS Corefiles (last 2 days) section lists any core files. Cisco Services may request that you copy the core file and send it to them for analysis.

Recent App Server Corefiles (last 2 days)

The data in the Recent App Server Corefiles (last 2 days) field lists any core files saved to the Application Server on the ISDS within the last 48 hours.

Note: A core file indicates that a process has failed unexpectedly.

Important: Call Cisco Services if the Recent App Server Corefiles (last 2 days) section lists any core files. Cisco Services may request that you copy the core file and send it to them for analysis.

DNS Check

The data in the DNS Check field reports whether the Domain Name Service (DNS) is running on the ISDS. The system lists **OK** when the DNS is not running; the system lists **Error** when the DNS is running.

Note: Having the DNS enabled on the ISDS may result in communication failures between the ISDS and modulators.

Important: If the DNS is enabled on the ISDS, disable it by editing the **/etc/nssswitch.conf** file so that the **hosts:dns** line reads as **hosts:files**.

Force Tune / Valid Service Check

The data in the Force Tune / Valid Service Check field lists all force-tune service IDs in the system that do not correspond to a valid SAM service. If the Doctor Report lists a service ID that is not associated with a valid service, reconfigure the service ID so that it is associated with a valid service.

ISDS License Check

The data in the ISDS License Check field reveals whether the following ISDS optional features are licensed or unlicensed:

- EAS FIPS Code Filtering
- DOCSIS DHCT Support
- Enhanced VOD Session Throughput
- VOD Session Encryption

Note: These optional features pertain only to sites running SR 2.1 and later system software. Contact Cisco Services to obtain licensing for a feature.

Unused SAM URL Check

The Unused SAM URL Check field provides a warning and a recommendation to run the chkSamUrl utility when the size of the bulk.tbl file is in danger of growing too large. When the bulk.tbl file grows too large, DHCTs may reboot and display a black screen.

ISDS File Size Check

The ISDS File Size Check field lists files 50 MB or larger in the /dvs/dncs/tmp, /var/log, and /tmp directories on the ISDS.

Last Logging Time Stamp for Selected Processes

The Last Logging Time Stamp for Selected Processes field reports the current time and then lists the timestamp associated with the last time the emmDistributor and camAuditor processes wrote to their respective logfiles. System operators can compare the timestamps with the current time to determine whether the emmDistributor and camAuditor processes are running properly.

Note: The timestamp should not be more than a few minutes behind the current time. If you notice that the timestamp associated with the logfiles is more than 15 minutes behind the current time, contact Cisco Services.

DHCT Status Summary

The data in the DHCT Status Summary field provides a status summary of all DHCTs in the database, local and remote sites.

DHCT Type Summary

The data in the DHCT Type Summary field summarizes the number of DHCTs in the database, using each unique combination of DHCT type, revision, OUI, and software table of contents file (if any).

Notes:

- The system also reports the number of DHCTs in the database of type NULL.
- A DHCT of type NULL represents a DHCT that has no record in the database, but has attempted to sign on to the system.

  Important: Call Cisco Services if you have a large number of DHCTs, relative to system size, with a type of NULL.

DHCTs with EMMs Expiring in 15 days

The data in the DHCTs with EMMs Expiring in 15 days field lists the MAC addresses of up to 50 DHCTs in the database that have EMMs set to expire within 15 days.

Notes:

- If the number of DHCTs with EMMs set to expire within 15 days exceeds 50, the system creates a file containing a complete list of those DHCTs.
- The file is called emms.expiring.soon and is found in the /dvs/dncs/Utilities/doctor directory.

Important: Call Cisco Services if you have any DHCTs with EMMs set to expire within 15 days.

EMM Distributor Cycle Summary

The EMM Distributor Cycle Summary field shows data from the emmDistributor process at two moments in time: just prior to the start of a cycle, and then at end of a cycle.

Data pertaining to the start of a cycle (which is actually shown in the second block of output), **EMM Distributor Cycle Start**, lists the parameters that the emmDistributor process is using to calculate the expected cycle duration. Additionally, a summary of the allocation of bridges (and associated DHCT population numbers) to emmDistributor threads, is also displayed.

The second snapshot, **EMM Distributor Cycle Complete**, displays data that was captured as the cycle completes. This data contrasts the expected cycle completion time to the actual cycle completion time.

Download Server Information

The Download Server Information field contains configuration data for each Download Server defined on the system.

CVT Configuration Check

The data in the CVT Configuration Check field includes the names and sizes of all of the DHCT image files loaded onto the system. In addition, the CVT Configuration Check field lists all of the DHCT groups that currently have DHCT download assignments.

DHCT counts per 55-1 QPSK

The data in the DHCT counts per 55-1 QPSK field lists the number of DHCTs that communicate with each 55-1 QPSK modulator and demodulator in the system.

Sources, Source Definitions and Segments

The data in the Sources, Source Definition and Segments field lists the number of the following items configured on the ISDS:

- Digital Sources
- Encrypted Digital Sources
- Active Source Definitions
- Pending Source Definitions
- Segments
- Encrypted Segments

In addition, the Sources, Source Definition and Segments field flags as an error source IDs that have multiple segments.

Active Subscription Packages

The data in the Active Subscriber Packages field lists the number of active subscriber packages configured on the ISDS.

SI Out-of-band Interval

The SI Out-of-band Interval lists how often out-of-band data is sent to DHCTs.

System Time Message Delivery

If debug flag **+DE** is set for the siManager process, the data in the System Time Message Delivery field confirms whether the system time message (STM) has been sent to DHCTs within the past 12 seconds.

Important: If the Doctor Report reports that STMs are not being delivered every 12 seconds, use the dncsControl utility to restart the siManager process.

PCG Information

The PCG Information field provides configuration data for each PowerKEY® CAS Gateway (PCG) defined on the system.

Timezone and Daylight Savings Time Check

The data in the Timezone and Daylight Savings Time Check field summarizes the time zone and daylight savings time (DST) settings for hubs and DHCTs.

Note: The DHCT Summary section should show **Follow hub** in the columns **Timezone Offset** and **DST Observed**.

Important: If the DHCT Summary section shows **Yes** or **No** in the **DST Observed** column, contact Cisco Services for assistance in configuring all DHCTs to follow the time of the hub to which they belong.

PPV File Check

The PPV File Check field indicates whether the PPVMapFile has been updated with PPV events.

Important: If the Doctor Report indicates an error, call Cisco Services for assistance in making any necessary corrections.

GBAM Delivery

Assuming debug flag **+DE** is enabled for the camPsm process, the data in the GBAM Delivery field verifies that time of day (TOD) and purchase GBAMs are delivered.

Notes:

- Purchase GBAMs can be verified only if there are PPV events with an open Buy window.
- Ideally, purchase GBAMs are delivered every 20 seconds and TOD GBAMs every 15 seconds. However, the Doctor Report verifies that these GBAMs have been delivered within the previous 60 seconds.

Important: If the Doctor Report indicates that GBAMs are not being delivered in a timely manner, call Cisco Services.

BFS Carousel and OSM Sessions Status

The data in the BFS Carousel and OSM Sessions Status field reports on the status of the BFS carousels and the OSM sessions. The output identifies whether carousels are inband (IB) or out-of-band (OOB), the source ID, the operational status of the carousels, the data rate, the amount of data carried, the indication interval of each carousel, the enabled state, as well as the total time required for each carousel to transmit all its data in one cycle (ACCT).

Additionally, the output lists the aggregate data rate for the inband and out-of-band carousels, which does not include data rates for disabled sources. This field reports for site ISDS as well as any remote site, if applicable.

BFS Session Status

The data in the BFS Session Status field verifies the following conditions:

- All BFS sources have an active session
- All sessions have a defined source

Important: If a BFS source does not have an active session, or if all sessions do not have a defined source, you have to create them. Call Cisco Services if you need help in creating a session or a source.

Miscellaneous BFS Check

The data in the Miscellaneous BFS Check field verifies the following conditions:

- No more than one dataCarousel process is running for a given BFS source.
- All BFS source definitions are present and are not duplicated.

  Note: If a BFS source definition is not present, the source definition will not be in SI and the DHCT will be unable to tune to that carousel.
- No BFS source is encrypted.

Ping All Active Elements

The data in the Ping All Active Elements field reports whether the communication path between the ISDS and the following system devices is active:

- QAM modulator (if applicable)

- QPSK modulator
- PCG
- TED

Important: If the Doctor Report reports an error, complete the following tasks to troubleshoot the error:

- Visually check that the device is powered on and that the cabling is secure.
- Use a network analyzer to confirm that IP traffic is reaching the device.
- Reboot the device.

DoctorRemote

The Doctor Report reports on the configuration of any remote site supported by the system. The information collected from remote sites is similar to the information collected from the ISDS. The following list contains the fields reported on for the remote sites:

- System Name
- All SAI Installed Package Information
- LIONN Info
- Virtual CPUs
- Physical Memory Configuration
- IO Devices
- Disk Info
- Checking the Status of the Metadevices
- LIONN Disk Partition Utilization
- LIONN Swap Space
- LIONN Basic System Performance Stats
- LIONN Database Log Check

  Note: This field appears only for remote sites. The LIONN Database Log Check field reports on the size of the /dvs/lionndb/liondb.log and /dvs/lionndb/lionnconnection.log files.
- LIONN Database Process Check

  Note: This field appears only for remote sites. The LIONN Database Process Check field reports on whether the Informix daemon processes are running.
- LIONN Load Average

- Current LIONN Debug Flags Set
- LIONN Processes
- Recent LIONN Corefiles (last 2 days)
- DNS Check
- Force Tune / Valid Service Check
- LIONN File Size Check
- Timezone and Daylight Savings Time Check
- EUT Update Check
- Ping All Active Elements

dncsDbData

The dncsDbData utility unloads and loads the ISDS and Application Server database.

Notes:

- To **unload** the database means to write the contents of the database to a file.
- To **load** the database means to insert data from a file into an existing database.

Options

Follow these steps to generate a list of options that you can use when you run the dncsDbData utility.

1. Open an xterm window on the ISDS.
2. Log into the ISDS as root user.
3. Type **. /dvs/dncs/bin/dncsSetup** and press **Enter**. This command establishes the ISDS environment as a root user.

   Important: Type a period followed by a space before typing /dvs.

   Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.
4. Type **dncsDbData** and press **Enter**. The system displays a list of options you can use when you run the dncsDbData utility.

Notes on Three Options

The following dncsDbData options require special comment:

- **-U and -L**. Cisco Services engineers may occasionally want to unload and load a database without using the high-performance features.

  Important: Cisco Services recommends that use of the -U and -L options be restricted to Cisco Services engineers only.

- **-g.** Cisco Services engineers designed the -g option to implement the gzip and gunzip file compression and uncompression utilities when loading and unloading database tables to the hard drive.

  In some cases, a database unload operation that would otherwise not fit into an existing file system on the ISDS or Application Server, will fit if the -g option is used in conjunction with the -u option. Instructions later in this section advise you to call Cisco Services if you discover that an unload of their database will not fit into an existing file system.

  Important: Cisco Services recommends that system operators do not use the -g option when unloading their database unless instructed to do so by Cisco Services.

Using dncsDbData

Several of the utilities contained in the ISDS Utilities are designed to help you minimize the effects of database fragmentation. System operators who want to avoid a fragmented database should follow the recommendations set forth in the remainder of this section.

Monitor and Eliminate Database Fragmentation

Over time, the database on the ISDS becomes fragmented as related data is divided into pieces and stored at various locations throughout the hard drive.

Database fragmentation occurs normally as the system is continually creating, deleting, and modifying records.

A badly fragmented database slows down system performance as the system must search the entire hard drive to build or retrieve a record.

Run and Analyze the Doctor Report

Run and analyze the output of the Doctor Report on a regular basis. Pay attention to the headings in the report called Database Table Extents for dncsdb and Database Table Extents for appdb.

The number of extents associated with a few specific tables provides you with some warning that the database is becoming fragmented.

Note: The number of table extents refers to the number of times a specific table is fragmented across the hard drive.

You should monitor the Doctor Report for the number of extents associated with the following ISDS database tables:

- emm
- hct_profile
- pdkeycertificate

- pdsernummap
- secure_micro
- sm_auth_profile
- sm_pkg_auth

Additionally, you should monitor the Doctor Report for the number of extents associated with the prvdrneutraldata table in the Application Server database.

If the Doctor Report indicates that the number of extents for any of these tables has reached 10, you should plan to run specific utilities designed to defragment the database. Once the number of extents has reached 30, system performance is negatively affected.

Example of a Fragmented Database

The following example from the Doctor Report illustrates a fragmented database.

```
DNCS Database Check
==========================================================
Total tempspace =    20520 pages ( 40.0  M)
Free tempspace  =    20083 pages ( 39.2  M)
Database tempspace is at 2.2% used capacity.
Total dataspace =  2097150 pages ( 4095.9  M)
Free dataspace  =  1919078 pages ( 3748.1  M)
OK: Database dataspace is at 8.5% used capacity.
Database Table Extents
================================================
=Database Table= =Extents=
atm_connection 7
displaychannels 2
elementary_stream 5
elementtable 5
elementtosource 3
emm 161
filemoduleinfo 6
hct_profile 65
================================================
```

This example shows output from two headings of the Doctor Report: DNCS Database Check and Database Table Extents. Notice that two of the tables under the Database Table Extents heading consist of more than ten extents. The emm and hct_profile tables consist of 161 and 65 extents, respectively. You should take steps to defragment this database.

Note: Because ISDS system operators regularly load EMM CDs, the emm table is especially subject to fragmentation.

Notice also the last line of data under the DNCS Database Check heading. This line of data indicates that the database is at 8.5 percent used capacity. The Doctor Report displays an error condition once the database reaches 75 percent used capacity.

Example of a Defragmented Database

The following example from the Doctor Report depicts the same database after you have used the dncsDbData utility to defragment the database.

```
DNCS Database Check
==================================================
Total tempspace =    20520 pages ( 40.0  M)
Free tempspace  =    20467 pages ( 39.9  M)
Database tempspace is at 0.3% used capacity.
Total dataspace =  2097150 pages ( 4095.9  M)
Free dataspace  =   565463 pages ( 1104.4  M)
OK: Database dataspace is at 73.1% used capacity.
Database Table Extents
==================================================
=Database Table=    =Extents=
authorization 3
elementtable 2
pdsegment 2
==================================================
```

In the preceding example, no table lists more than 10 extents. Therefore, the database has been successfully defragmented.

Notice, however, the last line of data under the DNCS Database Check heading. The Doctor Report now shows that the database is at 73.1 percent used capacity. This significant increase in database used capacity might be disconcerting. Refer to ***An Explanation of Database Used Capacity*** (on page 417) for an explanation of how the database increased from 8.5 percent used capacity to 73.1 percent used capacity after defragmenting the database.

An Explanation of Database Used Capacity

The reload function of the dncsDbData utility preallocates a significant amount of space to the emm table. By preallocating space to the emm table, the table can grow substantially without it becoming fragmented across the hard drive as it grows.

The Doctor Report considers this preallocated space as used, even though it may consist largely of empty space. Therefore, Doctor Reports generated after defragmenting the database are likely to show a significant increase in the percentage of database used capacity.

Note: The amount of space preallocated to the emm table is based upon the following factors:

- The number of database spaces configured on the system
- The hardware platform of the ISDS
- The number of disks assigned to the database

```
Defragment the ISDS Database
```

When the Doctor Report indicates that the number of extents associated with any of the previously mentioned database tables has reached 10, system operators should plan to run the following procedures.

Important: The following procedure is in outline form only. Be sure to refer to the specific procedures referenced in each step when eliminating database fragmentation.

1. Run the dbOptimizer program to delete unneeded EMMs from the database.
2. Back up the database. See ***Database Backup and Restore*** (on page 510) for more information.

   Note: When you back up the database, the system backs up both the ISDS database and the Application Server database.
3. Run the dncsDbData utility using the -z option to determine whether you can unload the ISDS database to the hard drive of the ISDS. See ***Unload the Database*** (on page 419) for more information.
4. Run dncsDbData with the -u option to unload the ISDS database. See ***Unload the Database*** (on page 419) for more information.

   Note: You may have old backup files on your ISDS that you can remove in order to conserve space. Contact Cisco Services for help in removing old files.
5. Run dncsDbData with the -l option to drop the ISDS database and reload it. See ***Load the Database*** (on page 424) for more information.

   Note: Dropping the database and reloading it eliminates the fragmentation.
6. Restart the system components after reloading the database.
7. Back up the database again. See ***Database Backup and Restore*** (on page 510) for more information.

```
Defragment the Application Server Database
```

When the Doctor Report indicates that the number of extents associated with the prvdrneutraldata table in the Application Server database has reached 10, you should plan to run the following procedures on the ISDS.

Important: The following procedure is in outline form only. Be sure to refer to the specific procedures referenced in each step to eliminate database fragmentation.

1. Run the dbOptimizer program to delete unneeded EMMs from the database.
2. Back up the database. See ***Database Backup and Restore*** (on page 510) for more information.

   Note: When you back up the database, the system backs up both the ISDS database and the Application Server database.
3. Run the dncsDbData utility using the -z option to determine whether you can unload the Application Server database to the hard drive of the ISDS. See ***Unload the Database*** (on page 419) for more information.
4. Run dncsDbData with the -u option to unload the Application Server database. See ***Unload the Database*** (on page 419) for more information.
5. Run dncsDbData with the -l option to drop the Application Server database and reload it. See ***Load the Database*** (on page 424) for more information.

   Note: Dropping the database and reloading it eliminates the fragmentation.
6. Restart the system components after reloading the database.
7. Back up the database again. See ***Database Backup and Restore*** (on page 510) for more information.

Unload the Database

The dncsDbData utility enables you to unload the ISDS and Application Server database to tape or to the hard drive on the ISDS. Follow the instructions in this section to unload the ISDS or Application Server database.

Note: When you unload a database, you write the contents of the database to a file.

You Need to Know

Before You Begin

Unloading the Database to Tape

Note: If you want to unload your ISDS or Application Server database to the hard drive of the ISDS, go to ***Unloading the Database to a Local Drive*** (on page 421).

You need a blank 4-mm or 8-mm tape (depending upon your tape drive) to unload the ISDS or Application Server database to tape. See ***Database Backup and Restore*** (on page 510) for tape drive and tape recommendations and configuration procedures.

Follow these instructions to unload your ISDS or Application Server database to tape.

1. Stop all third-party applications.
2. Shut down the Application Server and the ISDS. See ***Starting and Stopping Processes*** (on page 391) for more information.

Important: All processes on the ISDS and the Application Server must be stopped when you unload or load the database.

3 Open an xterm window on the ISDS.

4 Log into the ISDS as root user.

5 Type **/etc/rc2.d/S75cron stop** and press **Enter**. The system stops all cron jobs on the ISDS.

6 Follow these instructions to stop cron jobs on the Application Server.

   a Open another xterm window on the ISDS, type **rsh appservatm** and press **Enter**.

   b Type **/etc/rc2.d/S75cron stop** and press **Enter**.

   c Type **exit** and press **Enter**.

7 In the original xterm window, type **. /dvs/dncs/Utilities/dncsSetup** and press **Enter**. This command establishes the ISDS environment as a root user.

   Important: Type the period followed by a space before typing **/dvs**.

   Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

8 Type **showActiveSessions** and press **Enter**. A display showing any active ISDS sessions appears.

9 Are there any active ISDS sessions?

   - If yes, type one of the following commands:
     - To kill all active sessions at once, type **killActiveSessions** and press **Enter**. Go to step 10.
     - To kill each process individually, type **kill [PID]** and press **Enter**, where [PID] is the process ID associated with the active session (do not type the brackets **[ ]** in the command. Go to step 10.
   - If no, the ISDS will display a message similar to **dncsDbServer is idle**. Go to step 10.

10 Label a blank tape with the following information:

   [DNCS or Application Server] Database Unload

   [Site Name]

   [Date]

   Notes:

   - Substitute ISDS or Application Server for [ISDS or Application Server], depending on which database you are unloading.
   - Substitute your site name for [Site Name].
   - Substitute today's date for [Date]

11 Insert the blank tape into the tape drive of the ISDS.

12 Choose one of the following options:

- If you are unloading the ISDS database to tape, type **dncsDbData -u** and press **Enter**.
- If you are unloading the Application Server database to tape, type **dncsDbData -u -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and press **Enter**.

  Note: The directory path following the **-c** option specifies the location of the appdb configuration files.

Result: The Unload Database window appears.

13 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

Note: The tape drive is the default destination.

14 Type **y (for yes)** and press **Enter**. The following message appears:

```
Please wait while unloading data to tape.
Performing export on database [dncsdb or appdb].
Please mount the tape and press return to continue.
```

15 When the database has been unloaded, eject the tape and store it in a safe place.

16 Are you planning to load your database immediately?

- If **yes**, go to ***Load the Database*** (on page 424).
- If **no**, type **/etc/rc2.d/S75cron start** and press **Enter**.

  Note: You should still be root user.

  Result: The system restarts the ISDS cron jobs.

17 Restart the ISDS and the Application Server.

18 Follow these instructions to restart the Application Server cron jobs.

a Type **rsh appservatm** and press **Enter**.

b Type **/etc/rc2.d/S75cron start** and press **Enter**.

c Type **exit** and press **Enter**.

19 Examine the cron files on both the ISDS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

Note: You might have to manually execute these cron jobs.

Unloading the Database to a Local Drive

Follow these instructions to unload your ISDS or Application Server database to the local hard drive of the ISDS.

1 Stop all third-party applications.

2 Shut down the Application Server and the ISDS.

Important: All processes on the ISDS and the Application Server must be stopped when you unload or load the database.

3 Open an xterm window on the ISDS.

4 Log into the ISDS as root user.

5 Type **/etc/rc2.d/S75cron stop** and press **Enter**. The system stops all cron jobs on the ISDS.

6 Follow these instructions to stop cron jobs on the Application Server.

   a Type **rsh appservatm** and press **Enter**.

   b Type **/etc/rc2.d/S75cron stop** and press **Enter**.

   c Type **exit** and press **Enter**.

7 Type **cd /dvs/backups** and press **Enter**. The /dvs/backups directory becomes the working directory.

   Note: We recommend that you store your database backups in a subdirectory within the /dvs/backups directory.

8 Type **showActiveSessions** and press **Enter**. A display showing any active ISDS sessions appears.

9 Are there any active ISDS sessions?

   - If yes, type one of the following commands:
     - To kill all active sessions at once, type **killActiveSessions** and press **Enter**. Go to step 10.
     - To kill each process individually, type **kill [PID]** and press **Enter**, where [PID] is the process ID associated with the active session (do not type the brackets **[ ]** in the command. Go to step 10.
   - If no, the ISDS will display a message similar to **dncsDbServer is idle**. Go to step 10.

10 Choose one of the following options:

   - If you are unloading the ISDS database to the hard drive of the ISDS, type **dncsDbData -z** and press **Enter**.
   - If you are unloading the Application Server database to the hard drive of the ISDS, type **dncsDbData -z -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and press **Enter**.

     Note: The directory path following the -c option specifies the location of the appdb configuration files.

     Result: The system displays how much disk space is required to store the unloaded database.

11 Write down the number of 1024-blocks required to store the database.

12 Type **df -k** and press **Enter**. The system displays the number of free disk blocks available in the mounted file systems on the ISDS.

13 Do any one of the /disk1, /var, or /export/home file systems have more free disk blocks than the number you recorded in step 11?

   - If **yes**, go to step 14.
   - If **no**, call Cisco Services.

     Notes:

- Cisco Services engineers may instruct you to unload your database using the **-g** option. The -g option compresses your database as the database unloads.
- If Cisco Services engineers advise you against using the -g option, they may advise you to remove unneeded files from your system.
- If you still do not have enough room on your hard drive to unload your database, you have no alternative than to unload your database to a tape. Follow the instructions in ***Unloading the Database to Tape*** (on page 419).

14 Follow these instructions.

a Type **cd [filesystem]** and press **Enter**.

Example: cd /export/home

b Type **df -k .** and press **Enter**. The system displays how much space is available in the selected filesystem.

Important: Be sure to type a space followed by a period after typing **df -k**.

c Double-check that the selected filesystem has more space available than the number you recorded in step 11.

Note: Try another filesystem if the filesystem you selected does not have enough space.

15 Type **mkdir db_dir.[MM.DD.YY_HH.MM]** and press **Enter** to create a subdirectory within the current directory.

Note: Substitute the current month, date, year, hour, and minute for [MM.DD.YY_HH_MM]. Do not type the brackets **[ ]** in the command.

Example: mkdir db_dir.12.15.00_08.45

16 Type **cd [directory you just created]** and press **Enter**. The directory you just created becomes the working directory.

Example: cd db_dir.12.15.00_08.45

17 Type **pwd** and press **Enter**. The system displays the complete path to the directory you just created.

18 Write down the complete path name so you can refer to it later.

Note: You will need this path name when you load the database.

19 Choose one of the following options:

- If you are unloading the ISDS database to the hard drive of the ISDS, type **dncsDbData -u** and press **Enter**.
- If you are unloading the Application Server database to the hard drive of the ISDS, type **dncsDbData -u -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and press **Enter**.

  Note: The directory path following the -c option specifies the location of the appdb configuration files.

Result: The Unload Database window appears.

20 Type **2** and press **Enter**. The **Is the above information correct? (Y/N)** message appears.

21 Type **y** and press **Enter**. The **Enter backup directory (Default: Current Directory)** message appears.

22 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

23 Type **y** and press **Enter**. The system unloads your database to the current directory.

24 Have you just unloaded your database as part of the defragmentation process, as described in the ***Monitor and Eliminate Database Fragmentation*** (on page 415) section?

- If yes, go to ***Load the Database*** (on page 424).

  Note: System components must remain stopped when you load the database.

- If no, type **/etc/rc2.d/S75cron start** and press **Enter**. The system restarts the ISDS cron jobs.

25 Restart the ISDS and the Application Server.

26 Follow these instructions to restart the Application Server cron jobs.

   a Type **rsh appservatm** and press **Enter**.

   b Type **/etc/rc2.d/S75cron start** and press **Enter**.

   c Type **exit** and press **Enter**.

27 Examine the cron files on both the ISDS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

   Note: You might have to manually execute these cron jobs.

Load the Database

The dncsDbData utility enables you to load and unload the ISDS or Application Server database from tape or from your local hard drive.

Note: To load the database means to insert data from a file into an existing database.

CAUTION:

If your ISDS has been running since you unloaded the database, the load process will overwrite any changes to the database since the unload process began.

Defragment the Database

When you load the database, the following actions occur:

- The system drops the existing database.
- The system rebuilds the database as it reloads the data from the ASCII files created during the unload procedure.
- The system turns on database logging.

When your system rebuilds the database, it rebuilds it at one contiguous location on the hard drive, which eliminates any previous database fragmentation. As a result, system performance is improved.

Loading the Database from Tape

Follow these instructions to load your ISDS or Application Server database from tape.

1. Stop all third-party applications.
2. Shut down the Application Server and the ISDS.

   Important: All processes on the Application Server and the ISDS must be stopped when you unload or load the database.
3. If necessary, open an xterm window on the ISDS and log into the ISDS as root user.
4. Have you just unloaded your database?
   - If **yes**, you have already stopped the ISDS and Application Server cron jobs; go to step 6.
   - If **no**, type **/etc/rc2.d/S75cron stop** and press **Enter**. The system stops all cron jobs on the ISDS.
5. Follow these instructions to stop cron jobs on the Application Server.
   - **a** Type **rsh appservatm** and press **Enter**.
   - **b** Type **/etc/rc2.d/S75cron stop** and press **Enter**.
   - **c** Type **exit** and press **Enter**.
6. Insert the tape containing your most recent unload of the database into the tape drive of the ISDS.
7. Type **showActiveSessions** and press **Enter**. A display showing any active ISDS sessions appears.
8. Are there any active ISDS sessions?
   - If yes, type one of the following commands:
     - To kill all active sessions at once, type **killActiveSessions** and press **Enter**. Go to step 9.
     - To kill each process individually, type **kill [PID]** and press **Enter**, where [PID] is the process ID associated with the active session (do not type the brackets **[ ]** in the command). Go to step 9.
   - If **no**, the ISDS will display a message similar to **dncsDbServer is idle**. Go to step 9.
9. Choose one of the following options:
   - If you are loading the ISDS database from a tape in the tape drive of the ISDS, type **dncsDbData -**l and press **Enter**.

- If you are loading the Application Server database from a tape in the tape drive of the ISDS, type **dncsDbData -l -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and press **Enter**.

  Note: The directory path following the **-c** option specifies the location of the appdb configuration files.

Result: The Load Database window appears.

10 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

Note: The tape drive is the default destination.

11 Type **y** and press **Enter**. The **Please mount tape #1 and press Return** message appears.

12 Press **Enter**.

Note: You already inserted the tape in an earlier step.

13 Wait for the **Process is complete** message to appear.

Note: This message signifies that the database is finished loading.

14 Eject the tape and store it in a safe place.

15 Restart the ISDS and the Application Server.

16 Type **/etc/rc2.d/S75cron start** and press **Enter**. The system restarts cron jobs on the ISDS.

17 Follow these instructions to restart the Application Server cron jobs.

a Type **rsh appservatm** and press **Enter**.

b Type **/etc/rc2.d/S75cron start** and press **Enter**.

c Type **exit** and press **Enter**.

18 Generate the Doctor Report and examine the output file for system conditions that may present a problem.

Note: Refer to ***doctor*** (on page 397) for instructions on generating the Doctor Report and examining the output file.

19 Examine the cron files on both the ISDS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

Note: You might have to manually execute these cron jobs.

Loading the Database from a Local Drive

Follow these instructions to load your ISDS or Application Server database from the hard drive of the ISDS.

1 Stop all third-party applications.

2 Shut down the Application Server and the ISDS.

Important: All processes on the Application Server and the ISDS must be stopped when you unload or load the database.

3 If necessary, open an xterm window on the ISDS and log into the ISDS as root user.

4 Have you just unloaded your database?

- If yes, you have already stopped the ISDS and Application Server cron jobs; go to step 6.
- If no, type **/etc/rc2.d/S75cron stop** and press **Enter**. The system stops all cron jobs on the ISDS.

5 Follow these instructions to stop cron jobs on the Application Server.

a Type **rsh appservatm** and press **Enter**.

b Type **/etc/rc2.d/S75cron stop** and press **Enter**.

c Type **exit** and press **Enter**.

6 Type **cd [directory name]** and press **Enter**.

Notes:

- The [directory name] is the complete path and directory name of where you previously unloaded your database. You recorded the path and directory name when you unloaded the database to the hard drive.
- Do not type the brackets **[ ]** in the command.

Example: Type **cd /dvs/backups/db_dir.12.15.00_08.45** and press **Enter**.

7 Type **showActiveSessions** and press **Enter**. A display showing any active ISDS sessions appears.

8 Are there any active ISDS sessions?

- If **yes**, type one of the following commands:
  - To kill all active sessions at once, type **killActiveSessions** and press **Enter**.
  - To kill each process individually, type **kill [PID]** and press **Enter**, where [PID] is the process ID associated with the active session. Do not type the brackets in the command.
- If **no**, the ISDS will display a message similar to **dncsDbServer is idle**.

9 Choose one of the following options:

- If you are loading the DNCS database from the hard drive of the ISDS, type **dncsDbData -l** and press **Enter**.
- If you are loading the Application Server database from the hard drive of the ISDS, type **dncsDbData -l -d appdb -c /dvs/appFiles/dbConfig/appDbConfig** and press **Enter**.

  Note: The directory path following the -c option specifies the location of the appdb configuration files.

Result: The Load Database window appears.

10 Type **2** and press **Enter**. The **Is the above information correct? (Y/N)** message appears.

11 Type **y** and press **Enter**. The **Enter backup directory (Default: Current Directory)** message appears.

12 Press **Enter**. The **Is the above information correct? (Y/N)** message appears.

13 Type **y** and press **Enter**. The database loads from the hard drive.

14 When the database has loaded, follow the procedures in ***Restart the ISDS Processes*** (on page 334) and ***Restart the Application Server Processes*** (on page 335) to restart the DNCS and the Application Server.

15 Type **/etc/rc2.d/S75cron start** and press **Enter**. The system restarts its cron jobs.

16 Follow these instructions to restart the cron jobs on the Application Server.

   a Type **rsh appservatm** and press **Enter**.

   b Type **/etc/rc2.d/S75cron start** and press **Enter**.

   c Type **exit** and press **Enter**.

17 Generate the Doctor Report and examine the output file for system conditions that may present a problem.

   Note: Refer to ***Using doctor*** (on page 400) and ***Understand the Data in a Doctor Report*** (on page 401) for instructions on generating the Doctor Report and examining the output file.

18 Examine the cron files on both the ISDS and Application Server and determine whether any cron jobs should have executed during the period when the cron jobs were stopped.

   Note: You may have to manually execute these cron jobs.

Obtain System Platform Information

Using the **-s** option, you can use the dncsDbData utility to obtain information about the ISDS hardware platform. Follow these instructions to use the dncsDbData utility to obtain system platform information.

1 Open an xterm window on the ISDS.

2 Type **su -** and press **Enter** to log in as root user.

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

4 Type **. /dvs/dncs/Utilities/dncsSetup** and press **Enter**. This command establishes the ISDS environment as a root user.

   Important: Type the period followed by a space before typing **/dvs**.

   Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.

5 Type **dncsDbData -s** and press **Enter**. The system displays ISDS hardware platform information.

6 Type **exit** and press **Enter** to log off as root user.

Obtain Utility Version Number

Using the **-v** option, you can obtain the version number of the dncsDbData utility. Follow these instructions to obtain the version number of the dncsDbData utility.

1. Open an xterm window on the ISDS.
2. Type **su -** and press Enter to log in as root user.
3. Type the **root password** and press **Enter**.
4. Type **. /dvs/dncs/Utilities/dncsSetup** and press **Enter**. This command establishes the ISDS environment as a root user.

   Important: Type the period followed by a space before typing **/dvs**.

   Note: The system may also return a message that ends with **-o bad options** or **-o: bad options**. Ignore this message; it is normal.
5. Type **dncsDbData -v** and press **Enter**. The system displays the version number of the dncsDbData utility.
6. Type **exit** and press **Enter** to log off as root user.

hostnmchg

You can change the ISDS and Application Server hostnames and the IP addresses if you want to connect your ISDS and Application Server to a different network.

The hostnmchg script changes the hostname, the IP address, and all associated files required to connect the ISDS and Application Server to the local network.

Important: The /etc/hosts file in the ISDS **must** always have the following entry:

192.168.1.1 dncs

This interface is used for communication between the ISDS and the TED. Do not change this entry in the /etc/hosts file.

Note: You can run the hostnmchg utility on both the ISDS and on the Application Server.

Running hostnmchg on the ISDS

1. Shut down the ISDS and the Application Server.
2. Click **EXIT** on the bottom of the ISDS terminal, and click **OK**.
3. Log out of the ISDS and the CDE Login window appears.
4. Log in to the ISDS as root user.
5. From an xterm window on the ISDS, type **su - informix** and press **Enter**. You become informix user in the xterm window.
6. Type **onmode -ky** and press **Enter**. The Informix database shuts down.
7. Type **exit** and press **Enter**. You log out as informix user in the xterm window.
8. Type the following command:

/dvs/dncs/Utilities/hostnmchg.sh [new_hostname] [new_ip_address] and press **Enter**.

Notes:

- Substitute your new hostname for [new_hostname]. Do not type the brackets **[ ]** in the command.
- Substitute your new IP address for [new_ip_address]. Do not type the brackets in the command.

Result: The following message appears:

```
This script will modify the system as follows:
Old hostname = <old_hostname>
Old IP address = <old_IP_address>
New hostname = <new_hostname>
New IP address = <new_ip_address>
Primary network interface file = /etc/hostname.hme1
Continue [y,n,?,q]
```

9 Type **y** to continue and press **Enter**.

Result: The script displays a list of affected files as it changes the hostname variable and IP address.

Note: If the script detects that the hostname variable has been changed before, the script requires confirmation from the operator before changing some hostname variables. The system displays a **You MUST reboot your system NOW** message.

Important: Ignore this message now; you will reboot the ISDS later.

10 Does your Application Server run SARA?

- If yes, go to ***Running hostnmchg on the Application Server*** (on page 430).
- If no (your system runs another resident application), go to ***Restart the Applications*** (on page 431).

Running hostnmchg on the Application Server

1 At the ISDS, type **cd /dvs/dncs/bin** and press **Enter**. The /dvs/dncs/bin directory becomes the working directory.

2 At the ISDS, type **rcp -p hostnmchg.sh appservatm:/dvs/appserv/bin** and press **Enter**. The ISDS copies the hostnmchg.sh script to the Application Server.

3 Are you already logged in to the Application Server?

- If yes, go to step 4.
- If no, log in to the Application Server CDE Login window as root user.

4 In an xterm window on the Application Server, type **id** and press **Enter**. The system displays the user id in the xterm window.

5 Choose one of the following options:

- If you are root user in the xterm window, go to step 7.
- If you are dncs user in the xterm window, go to step 6.

6 Follow these instructions to log on to the xterm window on the Application Server as root user.

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

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

7 Type **chmod +x /dvs/appserv/bin/hostnmchg.sh** and press **Enter**. Executable permissions are applied to the hostnmchg.sh file.

8 Type **/dvs/appserv/bin/hostnmchg.sh [new_hostname] [new_ip_address]** and press **Enter**.

   Notes:

   - Substitute your new hostname for [new_hostname]. Do not type the brackets **[ ]** in the command.
   - Substitute your new IP address for [new_ip_address]. Do not type the brackets in the command.

   Result: The following message appears:

```
This script will modify the system as follows:
Old hostname = <old_hostname>
Old IP address = <old_ip_address>
New hostname = <new_hostname>
New IP address = <new_ip_address>
Primary network interface file = /etc/hostname.hme0
Continue [y,n,?,q]
```

9 Type **y** to continue and press **Enter**.

   Results:

   - The script changes the hostname of the Application Server.
   - A message instructing you to reboot the Application Server appears.

10 Type **/usr/sbin/shutdown -y -g0 -i0** and press **Enter**. The Application Server shuts down.

11 Go to ***Restart the Applications*** (on page 431).

Restart the Applications

After running the hostnmchg script on the ISDS and the Application Server, follow these instructions to restart the system applications.

1 In the xterm window on the ISDS, type **/usr/sbin/shutdown -y -g0 -i6** and press **Enter**. The ISDS reboots.

2 After the ISDS reboots, log in to the CDE of the ISDS as dncs user.

3 If necessary, follow the instructions in ***Restarting All ISDS Processes*** (on page 352) and ***Restarting Application Server Processes*** (on page 394) to restart the ISDS and the Application Server.

   Note: The system applications may have restarted after you rebooted the ISDS and the Application Server.

checkDB

The checkDB script identifies and corrects various potential problems in the ISDS database. This section describes some of the potential database problems identified by the checkDB script, and provides instructions for running the script.

Types of Database Problems

The following list identifies some of the potential problems that the checkDB script identifies:

- Set-top records in the database that do not have serial numbers

  Notes:

  - Set-top serial numbers are used mainly with third-party applications.
  - If the output of the checkDB script shows that you have set-tops in your database without serial numbers, you can contact Cisco Services to assign serial numbers to those set-tops.

- Records in various tables in the database that do not have required corresponding records in other tables

  Notes:

  - Records that do not have required corresponding records in other tables are known as "orphaned" records.
  - You can configure the checkDB script to automatically remove orphaned records from the database.

- Set-tops with a status of in-service that have EMMs ready to expire

  Note: The checkDB.sh script will prompt you to either restage or delete set-tops with EMMs ready to expire.

- Sites that are likely to experience a problem due to the ISDS generating duplicate subscription EMMs. (This is a very rare condition and is included in the checkDB utility as a precaution.)

  Notes:

  - The checkDB script identifies this condition through the Highest eu_eid used for subscription pkgs field.
  - Sites where this value exceeds 220 should report this condition to Cisco Services.

Prerequisites

Consider the following important prerequisites before you run the checkDB script:

- Be sure that you have a current backup of your database before running the checkDB script with the **-f** or **-F** options. Refer to ***Database Backup and Restore*** (on page 510) for detailed instructions on how to back up the ISDS database.

Note: The checkDB script makes no database changes when run with no options or with the **-v** option. The script may change the database when run with the **-f** or **-F** options. Refer to ***Using checkDB*** (on page 433) for additional information concerning the options associated with the checkDB script.

- If you configure the checkDB script to automatically remove orphaned records from the database, you need the deleteDhct utility installed on your ISDS to complete the task. This utility is included on the Utilities CD.

  Note: Refer to ***The deleteDhct Utility*** (on page 433) for information about the deleteDhct utility.

The deleteDhct Utility

When used with the **-f** or **-F** options, the checkDB script calls the deleteDhct utility to delete set-top records from the database.

The logic of the checkDB script is such that all references to the deleteDhct utility occur automatically; no user intervention is required. The deleteDhct utility is included on the Utility CD.

We designed the deleteDhct utility to completely delete set-top records from the database. It deletes a single set-top or it can delete all set-tops in a list containing set-top MAC addresses that are presented in a text file.

The logic in the deleteDhct utility is very good at finding all database rows in all the different set-top tables that contain or used to contain records for the specified set-top(s). The deleteDhct utility deletes orphaned set-top records. While orphaned set-top records are less common now than they have been in the past, at one time duplicate database rows were generated for RMA set-tops when they were returned from repair with a changed secure_micro address.

Using checkDB

The checkDB utility examines the following tables in your ISDS database for possible error conditions:

- emm
- hct_profile
- pdkeycertificate
- pdsernummap
- secure_micro
- sm_auth_profile
- sm_pkg_auth

Options

You can run the checkDB utility in three possible modes:

- Run the checkDB utility in default mode (with no options) to generate a detailed report listing possible error conditions in the database. When you run the checkDB utility in default mode, the script does not correct any error conditions it finds. The utility merely generates a report listing potential error conditions.
- Run the checkDB utility in "fix" mode (with the -f or -F option) to automatically delete certain orphaned records from the database. When you run the checkDB utility in fix mode , the script generates a report listing potential error conditions and lists any changes it made to the database as a result of running the utility in fix mode.

  Important: We recommend that you run the utility with no options before running the utility with one of the "fix" mode options.
- Run the checkDB utility with the -v option to display only the version number of the checkDB utility.

Running checkDB with No Options

Follow these instructions to run the checkDB utility with no options and to examine the logfile.

1. If necessary, open an xterm window on the ISDS.
2. Type **checkDB.sh > /dvs/dncs/tmp/checkDB.[today's date]** and press **Enter**.

   Notes:

   - Substitute today's date for [today's date]. Do not type the brackets **[ ]** in the command.

   Example: checkDB.sh > /dvs/dncs/tmp/checkDB.081601

   - This command directs the output from the checkDB script to a file in the /dvs/dncs/tmp directory on the ISDS. We recommend that you direct the output to a file for you to examine later because the output would otherwise scroll too quickly off the screen for you to examine.
3. After the utility has finished running, type **cd /dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes your working directory.
4. Type **more [name of logfile]** and press **Enter**. The logfile opens using the UNIX more utility.

   Note: Substitute the name of the logfile you created in step 2 for [name of logfile]. Do not type the brackets in the command.

   Example: more checkDB.081601
5. Refer to ***Sample Logfile and Analysis*** (on page 435) as you examine the logfile created by the checkDB script.

   Notes:

   - Press the **Spacebar** to page through the output file.

- Press the **Ctrl** and **C** keys at the same time to close the output file when you are finished.

Sample Logfile and Analysis

Use the following example when you examine the logfile you opened in Running the checkDB Utility with No Options.

Note: The following example of the logfile contains line numbers. Line numbers do not actually appear in the logfile, but are included here to facilitate an explanation of some of the items contained in the logfile.

Sample Logfile

```
==============================================================
1  Tue Dec 2 15:25:43 EST 2008
2  The total number of rows in hct_profile = 156278.
3  The total number of rows in secure_micro = 40378.
4  Highest eu_eid used for subscription pkgs = 111.
5  DHCT Registration is set to 'Administrative Gateway'.
6  There are 65407 MAC addresses with No DHCT Serial Number
7  Rows defining SN/MAC should be added for these boxes in 'pdsernummap'
   00:02:DE:11:72:EE
   00:02:DE:14:C3:72
   (65405 other addresses listed here)
8  There are 233 SN/MAC matches that should be DELETED from 'pdsernummap'
   SABBGZJWC|00:02:DE:49:F7:6C|
   SABBHCQTS|00:02:DE:4A:73:20|
   SABBHBQRF|00:02:DE:4A:34:3A|
   (230 other addresses listed here)
9  There are 0 secure_micro rows with mac_addr not in 'hct_profile'
10 There are 5 secure_micro MACs with sm_serial_num not in 'hct_profile'
11 These sm_host_mac_addr rows MUST be deleted from 'secure_micro'!
12 (They cause 'mismatch' problems with EMM regeneration in camAuditor)
13 (Use the 'deleteDhct' utility to delete these.)
   00:01:A6:05:33:70|00:02:DE:FC:50:14|
   00:01:A6:20:66:1A|00:02:DE:F0:A0:5B|
   00:01:A6:41:B2:80|00:02:DE:F0:93:8E|
   00:01:A6:30:A3:A4|00:01:A6:7C:53:F6|
   00:01:A6:41:35:64|00:01:A6:80:EE:8E|
14 There are 0 sm_auth_profile rows with no secure_micro parent
15 There are 0 sm_pkg_auth SMSNs with no secure_micro parent
16 There are 502 boxes having EMMs with sm_serial_num not in 'hct_profile'
17 All rows having these sm_serial_num should be deleted from 'emm'
   00:01:A6:5D:10:92
   00:01:A6:67:54:24
```

```
   (500 other addresses listed here)
18 There are 0 pdkeycertificates having no parent 'hct_profile'
19 There are 0 boxes with no 'pdkeycertificates'
20 There are 14 boxes with no 'secure_micro', but with very-old EMMs.
21 These boxes are in the database, but were incompletely staged
22 over 90 days ago.  They should be re-staged or deleted.
   00:02:DE:1D:4C:5A
   00:02:DE:1B:6E:6A
   00:02:DE:53:E4:6A
   00:02:DE:58:6A:64
   00:02:DE:1C:13:D6
   00:02:DE:B2:9F:E6
   00:02:DE:14:E1:18
   00:02:DE:14:67:EA
   00:02:DE:49:BF:3A
   00:02:DE:14:16:B8
   00:02:DE:13:21:52
   00:02:DE:16:5A:36
   00:02:DE:A1:04:D0
   00:02:DE:10:D9:9C
23 There are 0 'In-Service' boxes with 'almost-expired' EMMs.
24 No orphaned authorizations exist...
25 3600 boxes have NULL in the hctt_oui, hctt_id, or hctt_revision parameters!
26 2 percent is MORE than should be tolerated!!
   ==========================================================
```

Logfile Analysis

Refer to the preceding logfile as you read through this analysis. Your logfiles are likely to contain similar points of interest.

Line Number	Analysis
2 and 3	Lines 2 and 3 indicate how many records exist in the hct_profile and secure_micro tables in the database.
4	Line 4 indicates the maximum value for subscription packages in the eu_eid column in the package table. **Important:** Sites where this value exceeds 220 should report this condition to Cisco Services.
5	Line 5 reports registration configuration. ■ Options are Open Registration and Administrative Gateway. ■ We recommend Administrative Gateway to prevent set-tops from being added to your system without your knowledge.

6 - 10	These lines identify set-tops that are in the database without serial numbers. ■ Line 6 indicates that there are 65,407 set-tops in the database without serial numbers. ■ Line 8 begins to list them, but the list has been truncated in this example to conserve space. ■ Contact Cisco Services if your logfile indicates that you have set-tops in the database without serial numbers. Cisco Services will retrieve the list from your ISDS and will insert the correct serial numbers into your database.
11 - 15	These lines identify 233 set-tops with serial number and MAC address entries in the pdsernummap table, but without a required corresponding entry in the hct_profile table. The checkDB script concludes that these are orphaned records and recommends that they be deleted.
16	This line reports that there are no entries in the secure_micro table of set-tops that have MAC addresses but have no corresponding entry in the hct_profile table.
17 - 25	These lines identify 5 set-tops with MAC address entries in the secure_micro table, but without a required corresponding entry in the hct_profile table. The checkDB script concludes that these are orphaned records and recommends that they be deleted.
26 and 27	These lines indicate that there are no orphaned records in the sm_auth_profile and the sm_pkg_auth tables with respect to the secure_micro table.
28 - 32	These lines identify 502 set-tops with serial number entries in the emm table, but without a required corresponding entry in the hct_profile table. The checkDB script recommends that they be deleted.
33 and 34	These lines indicate that there are no potential error conditions with the pdkeycertificates table.
53	Line 53 indicates that there are no orphaned authorization records in the database.
54 and 55	These lines indicate that there are 3600 set-top entries in the hct_profile table with NULL values in the hctt_oui, hctt_id, or hctt_revision fields. These NULL values result from running a script for handling mismatched hardware type errors. Note: When the quantity of set-tops with NULL values in the previously mentioned fields exceeds 1 percent of the set-tops in the hct_profile table, the checkDB script notifies you.

Running checkDB in Fix Mode

Follow these instructions to run the checkDB script in fix mode.

1. If necessary, open an xterm window on the ISDS.
2. Choose one of the following options:
   - To run the checkDB script with the -f option, type
     checkDB.sh -f > /dvs/dncs/tmp/checkDB.[today's date] and press **Enter**.
     Example: checkDB.sh -f > /dvs/dncs/tmp/checkDB.081601
   - To run the checkDB script with the -F option, type
     checkDB.sh -F > /dvs/dncs/tmp/checkDB.[today's date] and press **Enter**.
     Example: checkDB.sh -F > /dvs/dncs/tmp/checkDB.081601

   Notes:
   - Substitute today's date for [today's date]. Do not type the brackets **[ ]** in the command.
   - These commands direct the output from the checkDB script to a file in the /dvs/dncs/tmp directory on the ISDS. We recommend that you direct the output to a file for you to examine later because the output would otherwise scroll too quickly off the screen for you to examine.

Conditions Addressed by Fix Mode

The following conditions are addressed by running the checkDB script in "fix" mode, using either the -f or the -F option:

- Set-top serial numbers with missing parent (extra rows in pdsernummap table)
- Records in hct_profile table with no corresponding record in the pdkeycertificate table
- Records in secure-micro table (with MAC address or serial number) with no corresponding record in the hct_profile table
- Records in sm_pkg_auth table with no corresponding record in sm_auth_profile table
- Records in emm table with no corresponding record in hct_profile table
- Orphaned authorization packages
- The -F option can also remove records in the sm_auth_profile table when there is no corresponding record in secure_micro table

keyFileFinder

The keyFileFinder utility detects files or packages that may be lost or replaced during an ISDS system software upgrade and records these files or packages in a logfile. You can then send the logfile to Cisco Services for examination.

Important: You should run the keyFileFinder utility at least 1 week prior to upgrading your system software.

Cisco Services will examine the logfile and highlight any files or packages that should be backed up separately prior to the upgrade. The field service engineer responsible for upgrading an ISDS will have this list of files during the upgrade, and will ensure that any special files or packages are backed up prior to the upgrade and restored after the upgrade.

How keyFileFinder Works

When you run the keyFileFinder utility, the utility compares the set of files installed during the upgrade with the files that currently exist on the system to be upgraded.

The keyFileFinder utility reports on the following three categories of files:

- Files that were installed as part of a Solaris package and have since been changed or customized.
- Files that have been installed or modified on the system, but are not part of any Solaris package.

  Example: The keyFileFinder utility lists any software added to the system that is not in Solaris format, as well as any dedicated utilities used only at the site to be upgraded.
- Packages that have been installed on the system that will not be installed as part of the upgrade.

  Note: Field service engineers may need to reinstall these packages after the upgrade.

Using keyFileFinder

Follow these instructions to run the keyFileFinder utility.

1. If necessary, open an xterm window on the ISDS.
2. Log into the ISDS as root user.
3. Type **cd /export/home/dncs/check** and press **Enter**. The /export/home/dncs/check directory becomes the working directory.
4. Type **./keyFileFinder.ksh -r** and press **Enter**. The keyFileFinder utility executes and displays to the screen files and packages that may have to be backed up separately and a logfile is generated in the /export/home/dncs/check directory.

   Note: The logfile is named **keyFileFinder.log**.
5. Contact Cisco Services for instructions on how to send the logfile to Cisco Services.

listTftpConfigs

Each device on the network has configuration data for that device stored in a specific file on the ISDS. Through the listTftpConfigs file, system operators and support engineers can examine this data at a glance, without having to access the GUI or WebUI for each device, one at a time.

Options

The following options are available for use by the listTftpConfigs utility:

- *-a* — The listTftpConfigs utility examines all network element configuration files in the ISDS database for the ISDS and remote sites. When complete, the utility lists those files to the screen of the ISDS. Displayed information includes the name and path of the configuration file, the site ID, the name of the network element, as well as the IP address and MAC address of the network element.

  Additionally, the output concludes by listing what are known as drop point values ("droppoint" in the output). Drop point values include the current version of code for each component of the network element, as well as the IP address that the network element uses to communicate with the various processes associated with the network element.

- *-f* — The listTftpConfigs utility, by nature, uses cached data to increase speed of reporting. Use of the *-f* option forces the utility to remove cached data and to reload data from the database.

- *-v* — Verbose mode. The *-v* option forces the utility to increase the detail in the data it reports.

- *-V* — The utility displays its version number.

- *-c CFGFILE* — Use [CFGFILE] to display configuration data and drop point values for the specified configuration file, only.

- *-n NENAME* — Use [NENAME] to display configuration data and drop point values for the specified network element, only.

  Example: QAM1

- *-s SITE* — Use [SITE] to display configuration data and drop point values for the specified site, only.

  Example: DNCS(1)

Examine All Configuration Files

When run with the *-a* option, the listTftpConfigs utility displays configuration data and drop point values for all devices on the network. Output from the listTftpConfigs utility, when the *-a* option is used, includes the following:

- Name of the configuration file
- Site (local ISDS or remote server), plus ID

- Name of the network device
- IP address
- MAC address

Complete these steps to run the listTftpConfigs utility with the *-a* option.

1 If necessary, open an xterm window on the ISDS.

2 Type **listTftpConfigs.ksh -a** and then press **Enter**.

Note: This is an intentional break in the data represented by the following image.

```
Tftp Config DB Report for ALL sites from DB=dncsdb for scooby on Wed Nov 28 10:35:20 EST
==========================================================================
Config File          Site(ID)     NE Name/Oid   IP Addr       Mac Addr
===========          ========     ===========   =======       ========

/tftpboot/qpsk.config   DNCS(1)   QPSK1         172.20.1.1    00:02:DE:81:EB:8C
/tftpboot/qpsk.config   DNCS(1)   QPSK2         172.21.1.1    DE:BB:EE:02:BA:BE
/tftpboot/qpsk.config   DNCS(1)   tstC          10.24.32.11   23:71:29:32:44:22
/tftpboot/qpsk.config   DNCS(1)   tstingCore98  10.23.24.98   12:32:11:11:11:11
/tftpboot/qam.config    DNCS(1)   BFSQam        172.16.4.100  00:02:DE:82:F3:BC
/tftpboot/qam.config    DNCS(1)   Hub01Qam01    172.16.4.101  00:02:DE:81:EA:3D
/tftpboot/gqam.config   DNCS(1)   EmulGQAM01    172.29.0.2    17:20:29:00:00:02
/tftpboot/mqam.config   DNCS(1)   Hub02Mqam     172.15.4.101  00:02:DE:81:F5:28

DNCS:/tftpboot/ droppoints:
        qpsk_man_ip 10.253.0.1
        hct_man_ip 10.253.0.1
        nms_man_ip 10.253.0.1
        stat_mgr_ip 10.253.0.1
          appver app_A62
            %s :
        BootCodePath caqam_boot212.bin
        ApplCodePath caqam_app254.bin
      RpcServerIpAddr 10.253.0.1
     AlarmServerIpAddr 10.253.0.1
        BootCodePath mqam_boot_1_2_3.bin
        ApplCodePath mqam_app_2_6_16.bin
         RFCodePath mqam_rf_23.bin
      RpcServerIpAddr 10.253.0.1
     AlarmServerIpAddr 10.253.0.1
```

Examine a Specific Configuration File

When run with the -c [CFGFILE] option, the listTftpConfigs utility displays configuration data and drop point values for the specific configuration file.

1 If necessary, open an xterm window on the ISDS.

2 Type **listTftpConfigs.ksh -c [CFGFILE]** and then press **Enter**.

Note: Substitute the name of the specific configuration file for [CFGFILE].

Example: listTftpConfigs.ksh -c mqam.config

```
xterm
jeckle1:/export/home/dncs>listTftpConfigs.ksh -c mqam.config

Tftp Config DB Report for ALL sites from DB=dncsdb for jeckle1 on Saturday, May 23, 2009  7:01:16 AM EDT
==========================================================================================================
Config File                    Site(ID)          NE Name/Oid     IP Addr          Mac Addr
===========                    ========          ===========     =======          ========
/tftpboot/mqam.config          DNCS(1)           testMQ          10.1.44.121      00:02:DE:01:44:12

Tftp Config File Report for CFGFILE='mqam.config' for jeckle1 on Saturday, May 23, 2009  7:01:18 AM EDT
==========================================================================================================
DNCS:/tftpboot/mqam.config: No such file
jeckle1:/export/home/dncs>
```

Examine the Configuration Files for a Specific Network Element

When run with the -n [NENAME] option, the listTftpConfigs utility displays configuration data and drop point values for the specific network element.

1. If necessary, open an xterm window on the ISDS.
2. Type **listTftpConfigs.ksh -n [NENAME]** and then press **Enter**.

   Note: Substitute the name of the specific network element for [NENAME].

   Example: listTftpConfigs.ksh -n PCG2

```
xterm
jeckle1:/export/home/dncs>listTftpConfigs.ksh -n PCG2

Tftp Config DB Report for ALL sites from DB=dncsdb for jeckle1 on Saturday, May 23, 2009  7:13:39 AM EDT
==========================================================================================================
Config File                    Site(ID)          NE Name/Oid     IP Addr          Mac Addr
===========                    ========          ===========     =======          ========
/tftpboot/pcg.cfg              DNCS(1)           PCG2            172.18.0.2       00:0E:0C:E5:F1:20

Tftp Config File Report for NENAME='PCG2' for jeckle1 on Saturday, May 23, 2009  7:13:41 AM EDT
==========================================================================================
DNCS:/tftpboot/pcg.cfg droppoints:
jeckle1:/export/home/dncs>
```

Examine the Configuration Files for a Specific Site

When run with the -s [SITE] option, the listTftpConfigs utility displays configuration data and drop point values for the specified site.

1. If necessary, open an xterm window on the ISDS.
2. Type **listTftpConfigs.ksh -s [SITE]** and then press **Enter**.

   Note: Substitute the name of the specific site for [SITE].

Example: listTftpConfigs.ksh -s DNCS

```
xterm
jeckle1:/export/home/dncs>listTftpConfigs.ksh -s DNCS

Tftp Config DB Report for Site=DNCS from DB=dncsdb for jeckle1 on Saturday, May 23, 2009  7:15:41 AM EDT
==============================================================================================
Config File                    Site(ID)          NE Name/Oid     IP Addr         Mac Addr
===========                    ========          ===========     =======         ========
/tftpboot/qam.config           DNCS(1)           test            172.0.0.4       00:00:00:00:00:00
/tftpboot/mqam.config          DNCS(1)           testMQ          10.1.44.121     00:02:DE:01:44:12
/tftpboot/pcg.cfg              DNCS(1)           PCG1            172.18.0.1      00:0E:0C:E5:F6:42
/tftpboot/pcg.cfg              DNCS(1)           PCG2            172.18.0.2      00:0E:0C:E5:F1:20

Tftp Config File Report for SITE='DNCS' for jeckle1 on Saturday, May 23, 2009  7:15:43 AM EDT
==============================================================================================
DNCS:/tftpboot/mqam.config: No such file
DNCS:/tftpboot/pcg.cfg droppoints:
DNCS:/tftpboot/qam.config: No such file
jeckle1:/export/home/dncs>
```

Display the Version Number of the listTftpConfigs Utility

Use the *-V* option to display the version number of the listTftpConfigs utility that is currently loaded on the ISDS.

1. If necessary, open an xterm window on the ISDS.
2. Type **listTftpConfigs.ksh -V** and then press **Enter**.

```
xterm
jeckle1:/export/home/dncs>listTftpConfigs.ksh -V
listTftpConfigs.ksh: version: 2
jeckle1:/export/home/dncs>
```

ncdsGen

The Network Configuration Discovery Service (NCDS) server provides a storage location for channel map, service group, and VOD information for your video system. The ncdsGen utility was developed in order to provide a mechanism for synchronizing this data between the NCDS server and the ISDS.

The ncdsGen utility can be configured to either post its collected data to the NCDS, or the NCDS can query the ncdsGen script for the necessary data. The ncdsGen script formats the required data in an XML format.

This chapter provides instructions for running the ncdsGen utility. Running this utility keeps the channel map, service group, and VOD QAM information in sync between the NCDS and the ISDS.

The ncdsGen utility uploads the ISDS channel maps and VOD information to the NCDS server.

You can use the following methods to run the utility:

- Push the information from the ISDS to the NCDS server

  Note: The ncdsPush utility, a utility within ncdsGen, triggers ncdsGen to generate the xml files; ncdsPush then transfers those xml files to the appropriate server.

- Poll the ISDS for the information for the NCDS server to fetch

- **Note:** The ncdsPoll utility, a utility within ncdsGen, is responsible for the polling action.

You Need to Know

When to Run the ncdsGen Utility

Pushing the Information to the NCDS Server

To push the information from the ISDS to the NCDS server, complete the following steps.

1. Type the following command to push the information to the NCDS server.

   ```
   ./ncdsPush -v http://< ipaddress:port >
   ```

   Note: Use the IP address and port of the NCDS server.

2. To verify that the script has run, look for output similar to the following:

   ```
   ./ncdsPush -v http://10.191.11.102:7091
   Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-ControllerAdd.xml
   Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-InputManifest.xml
   Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-CHM.xml
   Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-DSG.xml
   Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-OOB.xml
   Success for file /dvs/dncs/bin/ncdsGen/ncdsGen-Input-VOD.xml
   ```

Polling for the Information

To poll the ISDS for the information to be fetched for the NCDS server, complete the following steps.

1. Type the following command to poll the ISDS for the information:

   ```
   ./ncdsPoll.cgi
   ```

2. To verify that the script has run, look for output similar to the following:

   ```
   /dvs/dncs/bin/ncdsGen/htdocs/ncdsPoll
   -rw-r--r--   1 dncs     dncs           0 Oct 25 14:09 ncdsGen.out
   -rw-r--r--   1 dncs     dncs           0 Oct 25 14:09 ncdsGen.err
   -rw-r--r--   1 dncs     dncs        6083 Oct 25 14:09 ncdsGen-Input-
   CHM.xml
   -rw-r--r--   1 dncs     dncs         600 Oct 25 14:09 ncdsGen-Input-
   DSG.xml
   -rw-r--r--   1 dncs     dncs         684 Oct 25 14:09 ncdsGen-Input-
   OOB.xml
   ```

```
-rw-r--r--   1 dncs     dncs        4245 Oct 25 14:09 ncdsGen-Input-
VOD.xml
-rw-r--r--   1 dncs     dncs         714 Oct 25 14:09 ncdsGen-
InputManifest.xml
```

3 For instruction on transferring the xml files to the NCDS server, contact TVWorks, the vendor supplying the NCDS server.

podDataChk

Using the podDataChk utility, you can examine, in summary form, the contents of the /dvs/dvsFiles/CCardServer/podData file. The podData file contains data that is communicated to CableCARD modules through the Broadcast File System (BFS) carousel, such as CableCARD configuration data, and data that pertains to the authorization and deauthorization of copy protection for CableCARD modules.

The podDataChk utility helps you determine what CableCARD module/host (Pod/Host) pairs are included in the podData file, and therefore transmitted via the BFS carousel. Furthermore, because the podData file is limited to 1,500 records, the podDataChk utility helps you monitor the growth of the file. If the podData file grows larger than 1,500 records, data in the file might not be transmitted on the BFS carousel in a timely fashion.

The podData file contains only "active" records—records for CableCARD module/host pairs that are currently authorized or deauthorized. It does not include records that were authorized or deauthorized in the past.

Each time the podDataChk utility runs, it generates the /dvs/dvsFiles/CCardServer/podData.txt file, which contains a complete summary of the data in the podData file. You can then use the UNIX *more* utility to examine the podData.txt file. However, only data that pertains to the option you used when you ran the podDataChk utility is displayed on the screen of the ISDS. Read through this section for a description of all the options that are supported by the podDataChk utility.

Options for the podDataChk Utility

The help window reveals that the following options are available for use by the podDataChk utility:

- *-c* — Number (count) of records in the Forced Key Refresh, Pod/Host Pairs Auth, and Pod/Host Pairs Deuth sections of the podData file.
- *-?* — Displays the help window of the podDataChk utility.
- *-h* — Displays the help window of the podDataChk utility.
- *-s* — Displays data that pertains to the CableCARD server.
- *-f* <*File*> — Allows the user to specify a podData file other than the podData file in the working directory.

- *-m* <*Pod MAC address*> — Displays the host ID for the specified pod (CableCARD module).
- *-H* <*host ID*> — Displays the pod (CableCARD module) MAC address for the specified host.

Each of these options is demonstrated later in this section.

Count the Records in the podData File

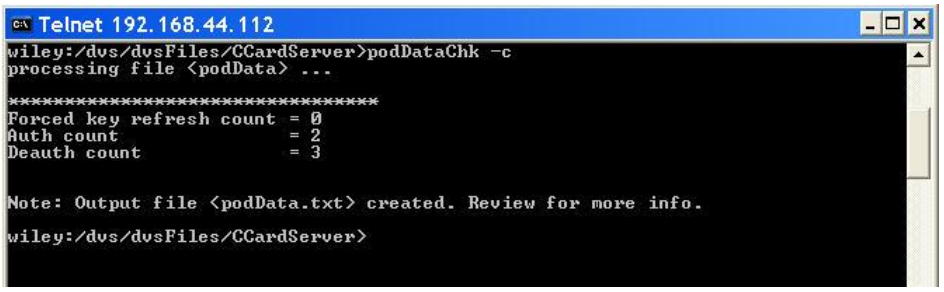
The podDataChk utility sorts the data in the podData file into various categories, or sections. One section, called the **Forced Key Refresh** section, contains the MAC addresses of CableCARD modules that need to initiate a new key exchange with its bound host for the purpose of obtaining secure transmission of data.

Another section, called the **Pod/Host Pairs Auth** section, contains the MAC addresses of CableCARD modules that have active copy protection authorization. A third section, called the **Pod/Host Pairs Deauth** section, contains the MAC addresses of CableCARD modules that have active copy protection deauthorization.

When run with the *-c* option, the podDataChk utility provides a count of the number of records in each section, and displays that data to the screen of the ISDS. In addition, the podDataChk utility generates a detailed summary of the podData file and writes that summary to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-c* option.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.
3. Type **podDataChk -c** and then press **Enter**. The system displays the count of records in the three previously mentioned sections of the podData file.



4. If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display Configuration Data for the CableCARD Server

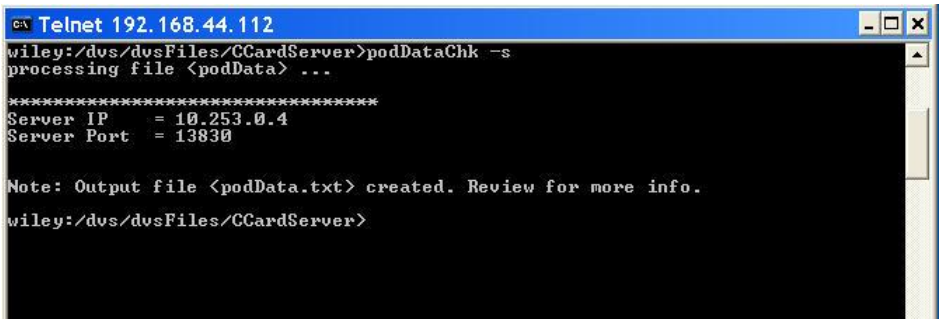
When run with the *-s* option, the podDataChk utility displays configuration data for the CableCARD server. The system directs output to the screen of the ISDS, as well as to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-s* option.

1 If necessary, open an xterm window on the ISDS.

2 Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.

3 Type **podDataChk -s** and then press **Enter**. The system displays configuration data for the CableCARD server.



4 If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display the Host ID for a Specific Module

When run with the *-m* option, the podDataChk utility displays the host ID for the specified CableCARD module. The system directs the output to the screen of the ISDS, as well as to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-m* option.

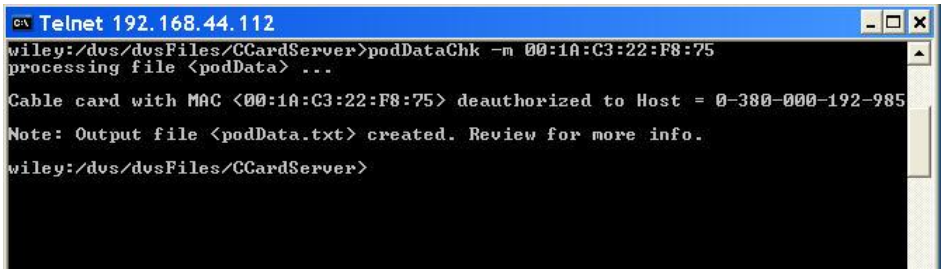
1 If necessary, open an xterm window on the ISDS.

2 Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.

3 Type **podDataChk -m <MAC Address of CableCARD module>** and then press **Enter**. The system displays the host ID for the specified CableCARD module, provided the CableCARD module/host pair is contained in the podData file.

Note: Substitute the MAC address of the CableCARD module for <MAC Address of CableCARD module>.

Example: podDataChk -m 00:1A:C3:22:F8:75



4 If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display the CableCARD MAC Address for a Specific Host

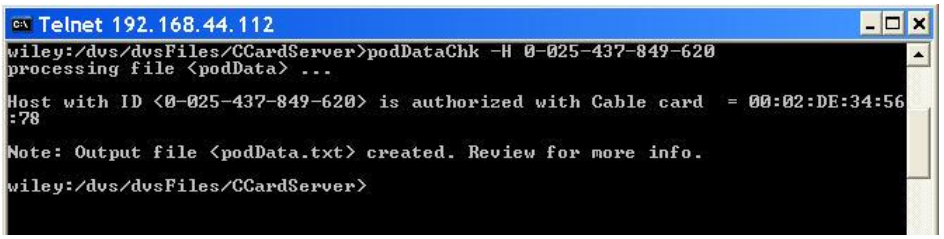
When run with the *-H* option, the podDataChk utility displays the CableCARD MAC address for the specified host. The system directs the output to the screen of the ISDS, as well as to the /dvs/dvsFiles/CCardServer/podData.txt file.

Follow these instructions to run the podDataChk utility with the *-H* option.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /dvs/dvsFiles/CCardServer** and then press **Enter**. The /dvs/dvsFiles/CCardServer directory becomes the working directory.
3. Type **podDataChk -H <Host ID>** and then press **Enter**. The system displays the CableCARD MAC address for the specified host, provided the CableCARD/host pair is contained in the podData file.

   Note: Substitute the specific host ID for <Host ID>.

   Example: podDataChk -H 0-025-437-849-620

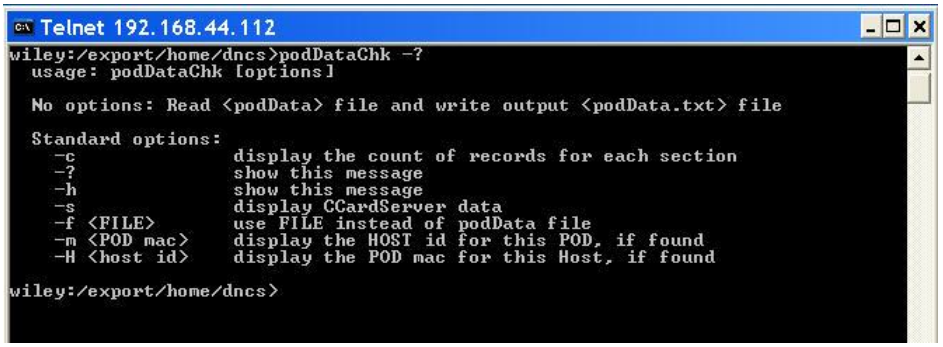


4. If desired, type **more podData.txt** and then press **Enter** to view the complete contents of the podData.txt file.

Display the Help Window for the podDataChk Utility

The podDataChk utility includes a help window that enables you to examine the various options supported by the utility. Follow these instructions to display the help window of the podDataChk utility.

1. If necessary, open an xterm window on the ISDS.
2. Type **podDataChk -?** and then press **Enter**. The system displays the help window for the podDataChk utility.



Note: Alternatively, you could type **podDataChk -h** and then press **Enter** to display the help window. Both the *-?* and *-h* options accomplish the same task.

slotchk

Run the slotchk utility to ensure that the Peripheral Component Interconnect (PCI) cards required for system upgrades are installed in the proper ISDS slots.

Embedded within the slotchk utility is an array listing the expected PCI card configuration for the Sun Fire V880 ISDS servers.

Note: The slotchk utility also reports on the Sun Enterprise 250 and V440 servers; however, these servers are not applicable to the ISDS.

The slotchk utility compares the actual PCI card configuration with the expected configuration and records the results in a logfile. You can send the logfile to Cisco Services for examination.

Important: You should run the slotchk utility at least a week prior to upgrading your systems. Cisco Services will examine the logfile and report any discrepancies found.

Expected PCI Card Configurations

This section lists the expected PCI card configuration for the the Sun Fire V880 server.

Note: The slotchk utility also reports on the Sun Enterprise 250 and 440 servers; however, these servers are not applicable to the ISDS.

The slotchk utility will log an error if a PCI slot does not contain the expected card, or if a slot that is supposed to be empty contains a card.

The following table lists the expected PCI card configuration for an Enterprise V880 ISDS server.

Slot Number	Expected PCI Card
0	Graphics card (XVR-100)
1	ATM card (FORE or OC3)
2	ASI card (video-pci5555) or empty
3	Empty
4	Empty
5	Empty
6	Network adaptor
7	ASI card (video-pci5555) or empty
8	Fiber channel card (SUNWqlc)

Using slotchk

Follow these instructions to run the slotchk utility.

1. If necessary, open an xterm window on the ISDS.
2. Log into the ISDS as root user.
3. Type **cd /export/home/dncs/check** and press **Enter**. The /export/home/dncs/check directory becomes the working directory.
4. Type **./slotchk.pl** and press **Enter**.

   Result: The slotchk utility runs and displays the following information on the screen:

   - The PCI card configuration found on the DNCS server.
   - Whether the configuration passes or fails.
   - A logfile is generated in the /export/home/dncs/check directory that also reports on the PCI card configuration.

     Note: The logfile is named slotchk.log.
5. Contact Cisco Services for instructions on how to send them the logfile.

runCvtGroup

When you use the CVT method to download set-top code, you sometimes want to restrict the download to set-tops that belong to a specific download group.

The runCvtGroup utility was developed to expedite the process by which set-tops are assigned to download groups. You can prepare a text file that contains one set-top MAC address per line. The runCvtGroup utility reads that text file and quickly assigns the set-tops associated with those MAC addresses to the specified download group.

Note: The download group must already exist before you assign set-tops to it.

Using runCvtGroup

Use these instructions to run the runCvt utility.

1. Do you need to create a download group?
   - If **yes**, go to step 2.
   - If **no**, go to step 10.
2. From the Administrative Console, select the **Network Element Provisioning** tab.
3. Click **Image**. The Image List window opens.
4. Select the **DHCT Groups** tab.
5. Click **File > New**. The Set Up DHCT Group window opens.
6. Enter information as described in CVT Group Settings.

7 Click **Add**. The MAC Address of the device moves to the Associated DHCTs column.

8 Repeat steps 5 through 7 for each device you want to add to the group.

9 Click **Save**.

10 If necessary, open an xterm window on the ISDS.

11 Type **runCvt [group ID] [file name]** and press **Enter**. The system assigns the set-tops in the text file to the specified download group.

Example: Type **runCvtGroup 2 /tmp/runCvtGroup-in_03.04.03** and press **Enter** to assign the set-tops in the text file in_03.04.03 to download group 2.

Notes:

- Refer to ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396) for instructions on preparing a text file for use with the runCvtGroup utility.
- Substitute the ID of the download group for [group ID]. Do not type the brackets **[ ]** in the command.
- Substitute the name of the text file for [file name]. Do not type the brackets **[ ]** in the command.

cronCvt

The cronCVT utility was developed so that system operators could place the DHCT host of a DHCT/embedded CableCARD pair into a download group. This is accomplished by assigning a package to the CableCARD module of the DHCT/CableCARD pair. The package that is assigned to the CableCARD module must already be associated with a download group by means of a configuration file.

The cronCVT utility reads a user-specified configuration file which links a package to a download group. If no configuration file is specified, then the /dvs/dncs/Utilities/croncvt.ini file is used, by default. The configuration file can support up to two packages and two download groups.

The cronCVT utility is typically run as a cron entry.

Note: The cronCVT utility pertains to DHCT/embedded CableCARD pairs, only. Legacy DHCTs cannot be placed into download groups through use of this utility.

Options Supported by cronCVT

As the Help window shows, the cronCVT utility supports three options: *-c, -r, and -z*. These options are used to place the DHCT into specific download groups. The utility links a package with a download group so when that package is assigned to a CableCARD module (through the ISDS or through the billing system), the DHCT host is placed in a download group.

With the *-c* option, removal of the package from the CableCARD module does not change the download group assignment of the DHCT. Should the user want to place the DHCT into a different download group, then the first package must be removed from the CableCARD module and a second package must be assigned which is associated with a second download group. If both packages are assigned to the CableCARD module, then the DHCT host is placed into the first download group specified in the configuration file, by default.

With the *-r* and *-z* options, if the package is removed from the CableCARD module, the DHCT host is placed into the default download group.

Configuring the cronCVT Utility

Follow these general instructions to configure the cronCVT utility to run on the ISDS. These instructions use the *-z* option as an example.

1. Use the Set Up Package window to create a package(s) to use with the cronCVT utility, or you can use an existing package(s).
2. Use the Set Up DHCT Group window to create a group9s) to use with the cronCVT utility, or you can use an existing group(s).
3. Create a "rule" file using the package(s) and CVT download group(s) that you configured in steps 1 and 2. In an xterm window on the ISDS, use a text editor to add entries similar to the following examples to the /dvs/dncs/Utilities/croncvt.ini file:

   PKG2GRP=CleanScreen1,1111

   PKG2GRP=CleanScreen2,2222

   PKG2GRP=CleanScreen3,3333

   Notes:

   - When the package CleanScreen1 is added to the DHCT, the DHCT will be assigned to CVT download group 1111
   - When the package CleanScreen2 is added to the DHCT, the DHCT will be assigned to CVT download group 2222
   - When the package CleanScreen3 is added to the DHCT, the DHCT will be assigned to CVT download group 3333
4. In an xterm window on the ISDS, follow these instructions to add an entry to the crontab file so that the cronCVT utility runs automatically.

   a In the dncs role, type **crontab -e** and then press **Enter**. The crontab file opens for editing.

   b Add an entry similar to the following. The first example configures the cronCVT utility to run every minute. The second example configures the cronCVT utility to run every 10 minutes.

   – `*****[-f/dvs/dncs/bin/dncsSetup] && (./dvs/dncs/bin/dncsSetup ;/dvs/dncs/Utilities/cronCVT -z . /dev/null`

- `0,10,20,30,40,50*****[-f/dvs/dncs/bin/dncsSetup] && (./dvs/dncs/bin/dncsSetup ;/dvs/dncs/Utilities/cronCVT -z . /dev/null`
- Save and close the crontab file.

The cronCVT Configuration File

Consider the following points about the configuration file used by the cronCVT utility:

- When DBDS Utilities is loaded onto the ISDS, the system automatically places the croncvt.sample.ini file into the /dvs/dncs/Utilities directory of the ISDS. The system operator should then copy this file to croncvt.ini, and then edit the file to suit their system's configuration.
- The croncvt.ini file can be moved to another directory, if desired. However, the path to that directory then needs to be explicitly specified when setting up the crontab file. Likewise, the file can be renamed to suit the system operator, but the new name must be reflected accurately in the crontab file.

Some examples of the croncvt.ini file follow.

croncvt.ini (with -c)

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #

#

# Package to Group assignment:
# The tool supports two packages and two CVT groups
# assignment. Once it has been determined that a
# given CableCard has received PKG1 or PKG2,
# the tool will assign the Host that is bound to
# the CableCARD to the CVT Group ID GRP1 or GRP2
# respectively. Only certain Hardware IDs specified
# in the Hardware Id Section will be affected.
#

# First Package and CVT group assignment
PKG1=tru2way
GRP1=7779

# Second Package and CVT group assignment
PKG2=SARA
GRP2=1234

# Hardware IDs (Type,Revision)
#HWID=8300,63
HWID=4300,43
HWID=5000,10
HWID=8300,63
```

croncvt.ini (with -c and the S25 stack)

Important: When using the *-c* option with the S25 stack, be sure to comment out, or delete, references to the hardware ID (HWID) parameters from this file.

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #

#

# Package to Group assignment:
# The tool supports two packages and two CVT groups
# assignment. Once it has been determined that a
# given CableCARD has received PKG1 or PKG2,
# the tool will assign the Host that is bound to
# the CableCARD to the CVT Group ID GRP1 or GRP2
# respectively.



# When using the S25 option, comment out or
# delete the HWID parameters from this
# config file.

# First Package and CVT group assignment
S25PKG1=S25
S25GRP1=999

# Second Package and CVT group assignment
S25PKG2=Brick
S25GRP2=999
```

croncvt.ini (with -r)

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #
#

# Package to Group assignment:
# The tool supports two packages and two CVT groups
# assignment. Once it has been determined that a
# given CableCARD has received PKG1 or PKG2,
# the tool will assign the Host that is bound to
# the CableCARD to the CVT Group ID GRP1 or GRP2
# respectively. Only certain Hardware IDs specified
# in the Hardware Id Section will be affected.
#
```

```
# First Package and CVT group assignment
PKG1=tru2way
GRP1=7779


# Second Package and CVT group assignment (Not used with -r)
#PKG2=SARA
#GRP2=1234

# Hardware IDs (Type,Revision)
#HWID=8300,63
HWID=4300,43
HWID=5000,10
HWID=8300,63
```

croncvt.ini (with -z)

```
#This is a comment
#you may place as many comments in this file as you want.
#the comment line must begin with an #

#

PKG2GRP=CleanScreen1,1111

PKG2GRP=CleanScreen2,2222

PKG2GRP=CleanScreen3,3333
```

Examples of the cronCVT Utility in the crontab File

This section provides two examples for adding an entry for the cronCVT utility to the crontab file of the ISDS.

Every Minute

To configure the cronCVT utility to run every minute, follow these instructions.

1. As dncs user in an xterm window, type the following command and then press **Enter**.

   ```
   crontab -l > /tmp/dncs.cron
   ```

2. Open the /tmp/dncs.cron file with a text editor.
3. Add an entry (on one line), similar to the following, to the crontab file:

   ```
   * * * * * [ -f /dvs/dncs/bin/dncsSetup ] && (. /dvs/dncs/bin/dncsSetup ;
   /dvs/dncs/Utilities/cronCVT -z ) > /dev/null
   ```

4. Save and close the file.
5. Type the following command and then press **Enter**.

   ```
   crontab /tmp/dncs.cron
   ```

6. Type `crontab -l` and then press **Enter** to verify that the entry was added successfully.

Every 10 Minutes

To configure the cronCVT utility to run every 10 minutes, follow these instructions.

1. As dncs user in an xterm window, type the following command and then press **Enter**.

   ```
   crontab -l > /tmp/dncs.cron
   ```

2. Open the /tmp/dncs.cron file with a text editor.
3. Add an entry (on one line), similar to the following, to the crontab file:

   ```
   0,10,20,30,40,50 * * * * [ -f /dvs/dncs/bin/dncsSetup ] && (.
   /dvs/dncs/bin/dncsSetup ; /dvs/dncs/Utilities/cronCVT -z ) > /dev/null
   ```

4. Save and close the file.
5. Type the following command and then press **Enter**.

   ```
   crontab /tmp/dncs.cron
   ```

6. Type `crontab -l` and then press **Enter** to verify that the entry was added successfully.

Troubleshooting the cronCVT Utility

Should the host fail to properly download code for the correct group, consider these troubleshooting tips:

- Does the /dvs/dncs/tmp/cronCVT.<yyyymm> file contain any errors?
- Is the correct package assigned to the CableCARD module?
- Is the CableCARD module assigned more than one package for download groups?

  Note: It should have only one package assigned.
- Is the cronCVT utility set up as a cron job correctly?
  - It should be set up for the **dncs** user and not the **root** user.
  - How frequently does the cron execute?

    Note: Recommended values are every 1 to 10 minutes.
  - Does the cronCVT utility specify the use of a specific file?

    Note: If not, the /dvs/dncs/Utilities/croncvt.ini file is used by default.
- Is the croncvt.ini file (or other specified file) configured correctly?

  Notes:
  - Is package 1 and group 1 configured?
  - Is the customer using package 2 and group 2?
  - Are the package names spelled correctly with the correct capitalization?
  - Are the Group IDs correct?
  - Are the Hardware types and revisions correct?

- Is the Host Hardware ID of the device included in the HWID section of the file?

check_metadevices

The check_metadevices utility constantly monitors the state of the metadevices on a Sun Fire V880 and V890 server, and then reports any errors it finds.

The utility runs automatically after you install the DBDS Utilities; you do not have to invoke any specific commands to run the check_metadevices utility.

Note: A metadevice is a group of physical devices accessed through a virtual or logical device.

Three Ways to Report Errors

The check_metadevices utility reports any metadevice errors it finds in the following three ways:

1. The utility displays a window on the ISDS that describes the error, as well as the time and date the error occurred.
2. The utility sends e-mail that notifies the dncs user and root user of the error.
3. If the site supports the Alarm Manager network management system, the check_metadevices utility reports those errors to the Alarm Manager software.

Call Cisco Services

You should always call Cisco Services before troubleshooting or trying to correct any errors reported by the check_metadevices utility.

Important: Do not try to correct any errors reported by the check_metadevices utility yourself. Always call Cisco Services first.

qtail

The logfiles in the /dvs/dncs/tmp directory contain important information about how the ISDS processes are operating.

As the processes run, they typically write entries into their associated logfiles that provide valuable debugging information. A typical entry into a logfile contains a time-stamp, as well as the current values of the software parameters and variables coded into the processes.

The qtail utility helps system operators and engineers monitor the ISDS logfiles.

Design of the qtail Utility

The UNIX operating system includes a utility called **tail**. The tail utility allows you to monitor a file in real time; as a new line is written to a file, that line is instantly displayed by the tail utility.

Note: To learn more about the tail utility, from an xterm window on the ISDS, type **man tail** and press **Enter**.

In theory, you can use the tail utility to monitor the logfile of a ISDS process in real time. The problem, however, comes when that logfile reaches its 50,000 line limit. The tail utility has no way of knowing that a limit has been reached and that a new logfile has been created. Hence, no new data can be observed in the logfile monitored by the tail utility.

The qtail utility uses the UNIX tail utility to monitor logfiles of ISDS processes in real time. When the limit of a specific logfile is reached, however, the qtail utility automatically starts monitoring the newly created file.

Design of the System Logfiles

A limit is placed on how large the logfiles in the /dvs/dncs/tmp directory can grow. If the logfiles were designed to grow without limit, the logfiles might eventually grow so large that they would slow down the performance of the ISDS. By default, we place a 50,000 line limit on individual logfiles. Each ISDS process supports up to 10 logfiles; the first logfile has a **.000** extension, the second logfile has a **.001** extension, and so on.

Example:

- camPsm.000
- camPsm.001
- camPsm.002

When a process reaches its 10-logfile limit, the system overwrites the first logfile with new data. By supporting 10 logfiles, the ISDS allows system operators and engineers plenty of time to save a specific logfile for later examination.

Using qtail

The logfiles in the /dvs/dncs/tmp directory of the ISDS have a default limit of 50,000 lines. After 50,000 lines, the system creates a new logfile. The qtail utility allows system operators or support engineers to monitor log activity and automatically switches to the next logfile when the 50,000 line limit has been reached.

The qtail utility was designed to monitor an entire logfile, or you can configure it to display only those lines that contain a particular pattern. When you configure the qtail utility to display lines in a logfile that contain a particular pattern, the utility uses the UNIX grep utility to search for that pattern.

You can run the qtail utility to either monitor an entire logfile, or to display only those lines that fit a pattern from a logfile.

Monitor an Entire Logfile

Follow these instructions to to use the qtail utility to monitor an entire logfile.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
3. Type **qtail [process_name]** and press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

   Notes:

   - Substitute the process name whose logfile you want to monitor for [process_name]. Do not type the brackets **[ ]** in the command.
   - You do not have to type the complete process name; you can type just enough to uniquely identify the process name from other processes.
     - Type **siM** for siManager.
     - Type **camAu** for camAuditor.

     Example: Type **qtail camAu** and press **Enter** to display the logfile associated with the camAuditor process.
4. Press the **Ctrl** and **c** keys simultaneously to exit from the qtail utility.

Display Only Lines that Fit a Pattern

Follow these instructions to use the qtail utility to monitor a logfile and display only those lines that contain a particular pattern.

1. If necessary, open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/tmp** and press **Enter**. The /dvs/dncs/tmp directory becomes the working directory.
3. Type **qtail [process_name] [pattern]** and press **Enter**. The qtail utility begins monitoring the logfile of the selected process.

   Notes:

   - Substitute the process name whose logfile you want to monitor for [process_name]. Do not type the brackets **[ ]** in the command.
   - You do not have to type the complete process name; you can type just enough to uniquely identify the process name from other processes.
     - Type siM for siManager.
     - Type camAu for camAuditor.
   - Substitute the pattern you want to find for [pattern].

   Example: Type **qtail camAu timeout** and press **Enter** to display only those lines that contain the word timeout in the logfiles associated with the camAuditor process.
4. Press the **Ctrl** and **c** keys simultaneously to exit from the qtail utility.

sesstail

The logfiles in the /dvs/dncs/tmp directory contain important information about how the ISDS processes are operating.

As the processes run, they typically write entries into their associated logfiles that provide valuable debugging information. A typical entry into a logfile contains a time-stamp, as well as the current values of the software parameters and variables coded into the processes.

The sesstail utility helps system operators and engineers monitor the ISDS logfiles.

Design of the sesstail Utility

The UNIX operating system includes a utility called **tail**. The tail utility allows you to monitor a file in real time; as a new line is written to a file, that line is instantly displayed by the tail utility.

Note: To learn more about the tail utility, from an xterm window on the ISDS, type **man tail** and press **Enter**.

In theory, you can use the tail utility to monitor the logfile of a ISDS process in real time. The problem, however, comes when that logfile reaches its 50,000 line limit. The tail utility has no way of knowing that a limit has been reached and that a new logfile has been created. Hence, no new data can be observed in the logfile monitored by the tail utility.

The sesstail utility is very similar to the qtail utility but is specifically designed to monitor the dsm process logfiles video-on-demand (VOD) session-related activities.

Design of the System Logfiles

A limit is placed on how large the logfiles in the /dvs/dncs/tmp directory can grow. If the logfiles were designed to grow without limit, the logfiles might eventually grow so large that they would slow down the performance of the ISDS. By default, we place a 50,000 line limit on individual logfiles. Each ISDS process supports up to 10 logfiles; the first logfile has a **.000** extension, the second logfile has a **.001** extension, and so on.

Example:

- camPsm.000
- camPsm.001
- camPsm.002

When a process reaches its 10-logfile limit, the system overwrites the first logfile with new data. By supporting 10 logfiles, the ISDS allows system operators and engineers plenty of time to save a specific logfile for later examination.

Using sesstail

The sesstail utility is similar to the qtail utility, except that it is designed to monitor the logfiles of the dsm process for session-related information. Examples of session-related information include session set up and tear-down activity.

You can use the sesstail utility to monitor the logfiles of the dsm process for session-related activity in real time or to search for session-related activity in existing dsm logfiles.

Note: By searching for session-related activity in existing dsm logfiles, you can troubleshoot VOD problems that have already occurred.

Follow these instructions to run the sesstail utility.

1. If necessary, open an xterm window on the DNCS.
2. Choose one of the following options:
   - To monitor the dsm logfiles in real time for session-related activity, go to step 3.
   - To review existing dsm logfiles for session-related activity, go to step 5.
3. To monitor the dsm logfiles for session-related activity in real time, type **sesstail** and then press **Enter**. The sesstail utility begins monitoring the dsm logfiles for session-related activity.

   Example: Sample output from the sesstail utility is displayed in the following example.

   $ sesstail

   ```
   ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientSessReq:    Feb 19 07:23:50.008
   ServerSessInd:    Feb 19 07:23:50.016
   ServerAddRsrReq:  Feb 19 07:23:50.207
   ServerAddRsrCnf:  Feb 19 07:23:50.270 (response=0)
   ServerSessRsp:    Feb 19 07:23:50.335 (response=0)
   ClientSessCnf:    Feb 19 07:23:50.346 (response=0)
   ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientRelReq:     Feb 19 07:23:58.683
   ServerRelInd:     Feb 19 07:23:58.687
   ServerRelRsp:     Feb 19 07:23:58.709 (Response=0)
   ClientRelCnf:     Feb 19 07:23:58.713 (Response=0)
   ```

4. Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.
5. To review an existing dsm logfile for session-related activity, type **sesstail [filename]** and then press **Enter**. The selected file opens for review.

   Note: Substitute the path and name of the logfile you want to review for [filename].

   Example: sesstail /dvs/dncs/tmp/dsm.000
6. Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.

Running the sesstail Utility

Follow these instructions to run the sesstail utility.

1. If necessary, open an xterm window on the DNCS.
2. Choose one of the following options:
   - To monitor the dsm logfiles in real time for session-related activity, go to step 3.
   - To review existing dsm logfiles for session-related activity, go to step 5.
3. To monitor the dsm logfiles for session-related activity in real time, type **sesstail** and then press **Enter**. The sesstail utility begins monitoring the dsm logfiles for session-related activity.

   Example: Sample output from the sesstail utility is displayed in the following example.

   $ sesstail

   ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientSessReq: Feb 19 07:23:50.008
   ServerSessInd: Feb 19 07:23:50.016
   ServerAddRsrReq: Feb 19 07:23:50.207
   ServerAddRsrCnf: Feb 19 07:23:50.270 (response=0)
   ServerSessRsp: Feb 19 07:23:50.335 (response=0)
   ClientSessCnf: Feb 19 07:23:50.346 (response=0)
   ++++ 00:40:7B:D6:B5:B3/515 ++++
   ClientRelReq: Feb 19 07:23:58.683
   ServerRelInd: Feb 19 07:23:58.687
   ServerRelRsp: Feb 19 07:23:58.709 (Response=0)
   ClientRelCnf: Feb 19 07:23:58.713 (Response=0)
4. Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.
5. To review an existing dsm logfile for session-related activity, type **sesstail [filename]** and then press **Enter**. The selected file opens for review.

   Note: Substitute the path and name of the logfile you want to review for [filename].

   Example: sesstail /dvs/dncs/tmp/dsm.000
6. Type the **Ctrl** and **c** keys simultaneously to exit from the sesstail utility.

syncwait

Disk mirroring is supported on the Sun Fire V880 and V890 servers.

Through disk mirroring, the ISDS stores identical information across sets of hard drives. The syncwait utility monitors the progress of mirrored disks as they synchronize their data.

Options

Run the syncwait utility with the **-?** option to display a list that shows the other options with which you can run the syncwait utility.

You can also run the syncwait utility with the **-v** option to display the version number of the utility.

Using syncwait

Mirrored disks lose their synchronization whenever the disk mirroring function of the Sun Fire V880 or V890 server is disabled.

For example, system operators or support engineers may disable disk mirroring on these servers just prior to a system upgrade. Then, after a successful upgrade, the disk mirroring function is re-enabled on the server and the secondary mirrored disk synchronizes with the primary mirrored disk.

Additionally, mirrored disks are out of synchronization whenever disk mirroring is first configured on a Sun Fire V880 or V890 ISDS, or when a hard drive that failed is replaced.

System operators and support engineers can use the syncwait utility to monitor progress as mirrored disks synchronize their data.

1. If necessary, open an xterm window on the ISDS.
2. Type **syncwait.ksh** and press **Enter**. The system displays a message stating the percentage of the mirror-synchronization process that is complete.

   Note: The syncwait utility updates the display every 20 seconds.
3. When the system displays the following message, type **n** (for no) and press **Enter**:

   ```
   No Resync in progress …
   Continue monitoring status?
   ```

   Result: The syncwait utility exits.

Application Server Utilities

The ISDP Utilities CD includes a collection of utility programs called Application Server Utilities. The following list contains the utilities available to the ISDS administrator and support engineer:

- ***purge_ipg_data*** (on page 464): Deletes Interactive Program Guide (IPG) data from the ISDS database.
- ***ipgUpdate*** (on page 465): Forces an immediate update of the BFS server with IPG data.
- ***ipgFileDump*** (on page 469): Converts binary IPG data to text format.

Installation of the Application Server Utilities occurs automatically when you install the ISDP Utilities. Refer to *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (part number 4031374) for installation instructions for the ISDP utilities.

purge_ipg_data

The purge_ipg_data.sh utility removes all existing IPG data from the Informix database.

When to Run purge_ipg_data

You should run this utility only when changing Interactive Program Guide (IPG) data providers or if you detect a problem with IPG data just downloaded from a data provider.

Important: Never run this utility just prior to a scheduled update of IPG data.

Using purge_ipg_data

To prepare to run the purge_ipg_data utility on the Application Server, you first have to stop the IPG Server.

Stopping the IPG Server

Important: When you stop and restart the IPG Server, IPG data is purged from set-tops and subscribers will not have IPG data in their guides until the IPG Collector has finished running.

1. Open an xterm window on the Application Server.
2. Type **appControl** and press **Enter**. The main menu of the Applications Control window appears.
3. Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The system displays all Application Server processes and servers.
4. Type the number that corresponds to the **IPG Server** and press **Enter**. The system displays a message that prompts you to enter a target status for the selected server.
5. Type **1** (for Stopped) and press **Enter**. The system displays a confirmation message.
6. Type **y** (for yes) and press **Enter**. The system updates the status of processes and servers on the Application Control window.

   Note: The Application Control window updates periodically, or you can press **Enter** to force an update.
7. When the **Curr Stt** (Current State) field of the Applications Control window indicates that the IPG Server has stopped, continue with step 8.
8. Type **x** and press **Enter** to return to the main menu of the Applications Control window.

Running ipg_purge_data

Important: Before you run ipg_purge_data, you must stop the IPG server. See *Stopping the IPG Server* (on page 464) for more information.

1. Open an xterm window on the Application Server.
2. Type **purge_ipg_data.sh** and press **Enter**. The system runs the purge_ipg_data utility.
3. Wait for the xterm window to update with a **Purging IPG data: DONE** message. Existing IPG data has been removed from the database.
4. Once you have purged your IPG data, you need to restart the IPG server.

Restarting the IPG Server

1. Open an xterm window on the Application Server.
2. Type **appControl** and press **Enter**. The main menu of the Applications Control window appears.
3. Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The system displays all Application Server processes and servers.
4. Type the number that corresponds to the **IPG Server** and press **Enter**. The system displays a message that prompts you to enter a target status for the selected server.
5. Type **2** (for Running) and press **Enter**. The system displays a confirmation message.
6. Type **y** (for yes) and press **Enter**. The system updates the status of processes and servers on the Application Control window.

   Note: The Application Control window updates periodically, or you can press **Enter** to force an update.
7. When the **Curr Stt** (Current State) field of the Applications Control window indicates that the IPG Server is running, go to step 8.
8. Type **x** and press **Enter** to return to the main menu of the Applications Control window.
9. You are now ready to collect IPG data from your service providers. Depending on what time you have configured your IPG Collector to run, you can either let it run normally or you can run it manually.

ipgUpdate

When you set up a new Service Application Manager (SAM) service you may want to map that service to Interactive Program Guide (IPG) data.

The IPG grid displayed at set-tops normally does not reflect a newly added SAM service unless the ipgServer is stopped and restarted, or until the ipgServer has finished applying collected changes to the IPG files on the Broadcast File System (BFS) server.

You may not want to stop and restart the ipgServer because it updates the system with 7 days worth of IPG data when it restarts, which is a lengthy process.

Additionally, you may not want to wait for the ipgServer to finish applying collected changes to the IPG files on the BFS server because it may take as long as 7 days for the ipgServer to collect and apply all of the changes.

We developed the ipgUpdate utility so that you can immediately rebuild IPG files on the BFS server. Use the instructions in this section to run the ipgUpdate utility.

Using ipgUpdate

When you set up a new Service Application Manager (SAM) service you may want to map that service to Interactive Program Guide (IPG) data.

The IPG grid displayed at set-tops normally does not reflect a newly added SAM service unless the ipgServer is stopped and restarted, or until the ipgServer has finished applying collected changes to the IPG files on the Broadcast File System (BFS) server.

You may not want to stop and restart the ipgServer because it updates the system with 7 days worth of IPG data when it restarts, which is a lengthy process.

Additionally, you may not want to wait for the ipgServer to finish applying collected changes to the IPG files on the BFS server because it may take as long as 7 days for the ipgServer to collect and apply all of the changes.

Using the ipgUpdate utility, you can immediately rebuild IPG files on the BFS server. Use the instructions in this chapter to run the ipgUpdate utility.

Confirming That the ipgServer Process is Running

Before you can run the ipgUpdate utility, confirm that the ipgServer process is running on the Application Server. Follow these instructions to check the status of the ipgServer process, and then to start the server, if necessary.

1. Is the AppServer Control window open on the ISDS?
   - If **yes**, go to step 2.
   - If **no**, click **Control** in the AppServer field of the Administrative Console Status window. The AppServer Control window opens.
2. Is the status indicator next to the ipgServer process green?
   - If yes, go to ***Running ipgUpdate*** (on page 467).
   - If **no**, go to step 3.
3. From an xterm window on the Application Server, type **appControl** and press **Enter**. The Applications Control window opens.
4. Type **2** (for Startup/Shutdown Single Element Group) and press **Enter**. The Applications Control window updates to list the servers and processes running on the Application Server.
5. Does the current status (Curr Stt) of the IPG Server group indicate running?

- If **yes**, go to step 10; the IPG Server process is already running.
- If **no**, go to step 6.

6 Type the number associated with **IPG Server** and press **Enter**. The system prompts you to enter the target status for the selected server or process.

7 Type **2** (for running) and press **Enter**. A confirmation message appears.

8 Type **y** (for yes) and press **Enter**. The Applications Control window updates to list the current status of the servers and processes running on the Application Server.

Note: The window may take a few seconds to update.

9 Wait until the **Curr Stt** (current status) of the IPG Server has a status of running.

Note: The Applications Control window updates in real time or you can press **Enter** to force an update.

10 When the IPG Server has a status of running, follow the on-screen instructions to exit from the Applications Control window.

Running ipgUpdate

Note: If you have just restarted the ipgServer process, there is no need to run the ipgUpdate utility. Restarting the ipgServer process automatically rebuilds your IPG data.

1 Open an xterm window on the Application Server.

2 Type **cd /dvs/appserv/bin/tools** and press **Enter**. The /dvs/appserv/bin/tools directory becomes the working directory.

3 Type **ipgUpdate [language] [day-mask]** and press **Enter**.

Notes:

- Do not type the brackets **[ ]** in the command.
- Substitute the 3-letter code for the language in the IPG grid that you support for [language]. Possible choices are:
  - eng for English
  - spa for Spanish
  - fra for French
  - jpn for Japanese
- [day-mask] represents the decimal equivalent of a binary number. Substitute the day-mask that represents the day's IPG files that you want to update for [day-mask]. Possible choices are:
  - 1 for today's IPG files
  - 2 for tomorrow's IPG files
  - 3 for today's and tomorrow's IPG files
  - 7 for today's, tomorrow's, and the following day's IPG files

- We do not recommend updating IPG data for more than 2 days in the future. Data for more than 2 days in the future has a high likelihood of changing on its own. Therefore, any changes to IPG data made by the system operator for 2 days in the future should be picked up naturally by the ipgServer process.

Example: To update the BFS server for tomorrow's IPG files in English, type **ipgUpdate eng 2** and press **Enter**.

4 Wait a few minutes and type **cd /dvs/appFiles/IPG_[language]** and press **Enter**.

Note: Substitute the language of the IPG files you updated in step 3 for [language]. Do not type the brackets in the command.

Example: If you updated IPG files in English, type **cd /dvs/appFiles/IPG_eng** and press **Enter**.

Result: The /dvs/appFiles/IPG_[language] directory becomes the working directory.

5 Type **ls -la IPGgi*** and press **Enter**. The system lists the files in the /dvs/appFiles/IPG_[language] directory that begin with **IPGgi**.

Notes:

- The names of the files are in the form of **IPGgi[dd].dat**.
- The [dd] refers to the date of the month.

Example: IPGgi15.dat refers to IPG files for the 15th of the month.

6 Notice the time and date associated with the IPG files you updated in step 3.

Note: The time and date associated with the IPG files you updated in step 3 should reflect the time and date you executed the command.

Example: If you ran the command in step 3 on the 15th of the month to update IPG files for tomorrow, notice the time and date associated with the IPGgi15.dat file.

7 Does the time and date associated with the IPG files you updated in step 3 reflect the time and date you executed the command?

- If **yes**, the ipgUpdate utility properly updated the BFS server with your IPG files.
- If **no**, call Cisco Services.

Displaying the ipgUpdate Help Window

Follow these instructions to display a window that provides some explanation of the parameters associated with the ipgUpdate utility.

1 Open an xterm window on the Application Server.

2 Type **cd /dvs/appserv/bin/tools** and press **Enter**. The /dvs/appserv/bin/tools directory becomes the working directory.

3 Type **ipgUpdate** and press **Enter**. The ipgUpdate help window opens.

ipgFileDump

The Application Server stores IPG data in binary format. Data stored in binary format is not understandable to the human eye. We created the ipgFileDump utility to convert binary IPG data to text format so that you can examine the data.

Parameters

The ipgFileDump utility requires the following parameters:

- **Language** refers to the native language of the IPG data.
  - eng - English
  - fra - French
  - jpn - Japanese
  - spa - Spanish
- **Filename** refers to files of the type IPGgi[dd].dat. Files of this type contain general information about the IPG data.

  Example: Examples of general information are date, time, SAM service, title, long description, and theme.

  Note: The [dd] parameter refers to the day of the month for which the file contains IPG data.

Using ipgFileDump

Follow these instructions to convert binary IPG data to text format so that you can examine the data.

1. Open an xterm window on the Application Server.
2. Type **cd /dvs/appFiles/IPG_[lang]** and press **Enter**.

   Note: Substitute the language of the IPG files for [lang]. Do not type the brackets **[ ]** in the command.

   Example: For English IPG files, type **cd /dvs/appFiles/IPG_eng** and press **Enter**.

   Result: The /dvs/appFiles/IPG_[lang] directory becomes the working directory.
3. Type **ls IPGgi*** and press **Enter**. The system lists all the IPG general information files in the directory.

   Examples:

   IPGgi04.dat

   IPGgi05.dat

   IPGgi06.dat

   Note: IPGgi04.dat refers to IPG files for the fourth of the month; IPGgi05.dat refers to IPG files for the fifth of the month, etc.
4. Locate the IPG general information file you want to convert to text format.

5 Type **/dvs/appserv/bin/tools/ipgFileDump [lang] [filename] > /tmp/[filename].out** and press **Enter**.

Example: Type **/dvs/appserv/bin/tools/ipgFileDump eng IPGgi04.dat > /tmp/IPGgi04.dat.out** and press **Enter**.

Results:

- The ipgFileDump utility converts the binary IPG data in the IPGgi[dd].dat file to text form.
- The ipgFileDump utility writes the text data to the /tmp/[filename].out file.

Notes:

- We recommend that you store the output from the ipgFileDump utility in the /tmp directory.
- You can append additional files to the command line if you want to convert more than one binary IPG file to text format. To convert more than one binary file to text format, type (all on one line):

  /dvs/appserv/bin/tools/ipgFileDump [lang] [filename1] [filename2] > /tmp/[filename].out

Viewing the ipgFileDump Files

Follow these instructions to view the IPG data in the [filename].out file.

1 Type **cd /tmp** and press **Enter**. The /tmp directory becomes the working directory.

2 Type **more [filename].out** and press **Enter**. The IPG data file opens for viewing using the UNIX more utility.

Example: Using the example developed in Running ipgFileDump, type **more IPGgi04.dat.out** and press **Enter**.

```
Ipg_HeapBlock: nextBlock=0 Ipg_TitleData: compressed,
5 bytes stored in 4 bytes , 1 contiguous blocks, value="Other"
Ipg_HeapBlock: nextBlock=0 Ipg_TitleData: compressed, 11 bytes stored in 9
bytes, 2 contiguous blocks, value="Action/Adv."
Ipg_HeapBlock: nextBlock=0 Ipg_TitleData: compressed, 5 bytes stored in 4
bytes, 1 contiguous blocks, value="Adult"
Ipg_HeapBlock: nextBlock=0 Ipg_TitleData: compressed, 9 bytes stored in 7
bytes, 1 contiguous blocks, value="Biography"
```

Notes:

- Sample output from the ipgFileDump utility is shown in this example.
- Press the Spacebar to page through the file.
- Press the **Ctrl** and **c** keys simultaneously to close the file when you are finished.

CoolTools Utilities

The ISDP Utilities CD includes a collection of utility programs called CoolTools Utilities.

Installation of the CoolTools Utilities occurs automatically when you install the ISDP Utilities. Refer to *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (part number 4031374).

savecore

The savecore utility enables you to save the contents of system memory to a file for later analysis when the ISDS or the Application Server crashes.

Note: The contents of system memory at crash time is commonly referred to as a **core dump**.

ISDS systems run on the Solaris 10 OS or later and therefore do not need to start the savecore utility, it is enabled automatically by default in these operating systems.

Using savecore

The system automatically writes the contents of a core dump to a file on the ISDS or the Application Server. The system writes the contents of the core dump when the system reboots.

Note: The system names the core dump files vmcore.0, vmcore.1, vmcore.2, etc.

Follow these instructions to view the contents of a core dump.

1. Open an xterm window on the ISDS or Application Server, depending upon which server contains the core file you want to examine.
2. Choose one of the following options (do not type the brackets **[ ]** in the command):
   - To examine a core file on the ISDS, type

     cd /export/home/crash/[ISDS name] and press **Enter**.
   - To examine a core file on the Application Server, type

     cd /export/home/crash/[Application Server name] and press **Enter**.

   Result: The directory to which the core dump output was written becomes the working directory.
3. Type **ls -ltr** and press **Enter**. The system lists the files in the current directory according to modification time (most recently written files last).

   Note: The newest file, named similar to **vmcore.#**, contains the contents of system memory from the most recent system crash.
4. Type **strings vmcore.# | more** and press **Enter**. The system opens the core file using the UNIX strings and more utilities.

   Note: Substitute the number associated with the core file you want to examine for #.

   Example: strings vmcore.0 | more
5. Examine the core file to determine why the system crashed.

Notes:

- Press the **Spacebar** to advance through the file.
- Press the **Ctrl** and **c** keys simultaneously to close the core file.

6 Call Cisco Services for help in examining the core file.

IIH

You can use the IIH utility to transmit the following four types of billing transactions to set-tops:

- **dhctInstantHit**—Specified by the **-i** parameter. Refreshes set-tops with their Entitlement Management Messages (EMMs).

  Note: EMMs are encrypted packets of information that the ISDS uses to supply secured service authorizations to set-tops. EMMs enable set-tops to use many digital and interactive broadcast services.

- **resetClientNvm**—Specified by the **-r** parameter. Resets the non-volatile memory (NVM) of a set-top to default values established at the factory.

  Note: The -r parameter is only supported by sites that use the SARA Application Server.

- **bootDhct**—Specified by the **-b** parameter. Reboots a single set-top or a list of set-tops.

- **setPin**—Specified by the -bp and -pp parameters. Resets two possible personal identification numbers (PINs) configured on the set-top:

  - **-bp (blocking PIN)**—The blocking PIN restricts access to specific channels.
  - **-pp (PPV PIN)**—The PPV PIN authenticates the purchase of a pay-per-view (PPV) movie.

These transactions can be transmitted to an individual set-top, a list of set-tops, or a specific model number of set-top. This section contains details of the four types of billing transactions supported by the IIH utility, as well as instructions and examples on using the utility.

Using IIH

The IIH utility can be configured to send four separate billing transactions to set-tops.

Each transaction is identified by the system through specific parameters that are used in conjunction with the IIH utility. See ***IIH*** (on page 472) for information on the parameters used with IIH.

In addition to supporting four billing transactions, the IIH utility can be run to display a help window, as well as a window that displays the current version number of the utility.

The IIH help window is especially useful in that it shows specific examples of how the IIH utility can be used. The remainder of this section provides detailed instructions on running the IIH utility.

Using IIH with a List of Set-Tops

Each of the transactions listed in ***IIH*** (on page 472) can be run using a list of set-tops.

Each set-top in the list is identified by MAC address. You typically prepare the list of set-tops, identified by MAC address, before using the utility by using a text editor, such as vi. Instructions for preparing the list of set-tops are found in ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396).

Note: When the IIH utility processes a list of set-tops, the transaction processes 10 set-tops at a time, by default. The reason 10 set-tops are processed at a time is to avoid monopolizing the bossServer process of the ISDS. If you have an urgent need to process more set-tops than ten at a time, you can override the default value through use of the **-C** parameter.

Displaying the IIH Help Window and Version Number

1. Open an xterm window on the ISDS.
2. Choose one of the following options:
   - To view the help window, type **IIH -?** and press **Enter**.
   - To view the version number, type **IIH -v** and press **Enter**.

Refresh Set-Top EMMs with the dhctInstantHit Transaction

The dhctInstantHit transaction refreshes set-tops with EMMs from the database.

The following procedures provide detailed instructions for sending a dhctInstantHit transaction to an individual set-top, set-tops contained in a list, or set-tops of a specific model type.

Refreshing the EMMs of an Individual Set-Top

Follow these instructions to refresh the EMMs of an individual set-top.

1. Open an xterm window on the ISDS.
2. Type **IIH -i [set-top MAC address]** and press **Enter**. The system refreshes the specified set-top with its EMMs.

   Notes:

   - Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets [ ] in the command.

- The MAC address can be formatted with or without colons (:).

Examples:

IIH -i 00:02:DE:A6:45:92

IIH -i 0002DEA64592

Refreshing the EMMs of a List of Set-Tops

Follow these instructions to refresh the EMMs of a list of set-tops.

1 Open an xterm window on the ISDS.

2 Do you want to force the system to process more than ten set-tops at a time?

- If **yes**, go to step 3.
- If **no**, go to step 4.

3 Type **IIH -i -C[# of set-tops] [text file name]** and press **Enter**. Go to step 5.

Notes:

- Substitute the number of set-tops you want to process at once for [# of set-tops]. Do not type the brackets **[ ]** in the command.
- Substitute the name (including path) of the text file for [text file name]. Do not type the brackets in the command.

  Example: IIH -i -C50 /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

4 Type **IIH -i [text file name]** and press **Enter**.

Note: Substitute the name (including path) of the text file for [text file name]. Do not type the brackets **[ ]** in the command.

Example: IIH -i /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

5 Type **y** and press **Enter**. The system lists the MAC addresses of the set-tops as it sends a dhctInstantHit transaction to each one.

Refreshing the EMMs of Set-Tops with a Specific Model Number

The dhctInstantHit transaction can be configured to refresh the EMMs of a specific model number of set-top. Follow these instructions to refresh the EMMs of set-tops of a specific model number.

1 Open an xterm window on the ISDS.

2 Type **IIH -i -M[model number]** and press **Enter**.

Note: Substitute the model number of DHCT for [model number]. Do not type the brackets **[ ]** in the command.

Example: IIH -i -M2100

Result: A confirmation message similar to the following appears:

```
DHCTs with DHCT Model=[model number] will be Instant-Hit …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

3 Type **y** and press **Enter**. The system sends a dhctInstantHit transaction to each set-top of the specified model number.

Reset Set-Top NVM with the resetClientNvm Transaction

The resetClientNvm transaction resets the non-volatile memory (NVM) of a set-top to default settings established at the factory.

The procedures in this section provide detailed instructions on resetting the NVM of an individual set-top, a list of set-tops, or DHCTs of a specific model number.

Note: The **-r** option, which is used to reset the NVM, is only a valid option at sites that use the SARA Application Server. When the -r option is used at a site that does not use the SARA Application Server, the system displays an error message.

Resetting the NVM of an Individual Set-Top

Follow these instructions to reset the NVM of an individual set-top.

1 Open an xterm window on the ISDS.

2 Type **IIH -r [set-top MAC address]** and press **Enter**. The system resets the NVM of the specified set-top.

Notes:

- Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets [ ] in the command.
- The MAC address can be formatted with or without colons (:).

Examples:

IIH -r 00:02:DE:A6:45:92

IIH -r 0002DEA64592

Resetting the NVM of a List of Set-Tops

Follow these instructions to reset the NVM of a list of set-tops.

1 Open an xterm window on the ISDS.

2 Do you want to force the system to process more than ten set-tops at a time?

- If yes, go to step 3.
- If no, go to step 4.

3 Type **IIH -r -C[# of set-tops] [text file name]** and press **Enter**. Go to step 5.

Notes:

- Substitute the number of set-tops you want to process at once for [# of set-tops]. Do not type the brackets **[ ]** in the command.
- Substitute the name (including path) of the text file for [text file name]. Do not type the brackets in the command.

Example: IIH -r -C50 /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be NVM reset …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

4 Type **IIH -r [text file name]** and press **Enter**.

Note: Substitute the name (including path) of the text file for [text file name]. Do not type the brackets **[ ]** in the command.

Example: IIH -r /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be NVM reset …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

5 Type **y** and press **Enter**. The system lists the MAC addresses of the set-tops as it sends a resetClientNvm transaction to each.

Resetting the NVM of Set-Tops of a Specific Model Number

The resetClientNvm transaction can be configured to reset the NVM of a specific model number of set-top.

Follow these instructions to reset the NVM of set-tops of a specific model number.

1 Open an xterm window on the ISDS.

2 Type **IIH -r -M[model number]** and press **Enter**.

Note: Substitute the model number of set-top for [model number]. Do not type the brackets **[ ]** in the command.

Example: IIH -r -M2100

Result: A confirmation message, similar to the following, appears:

```
saManager is running
DHCTs with DHCT model=[model number] will be NVM-Reset
# MAC addresses will be involved.
Do you want to continue (Y/N)?
```

3 Type **y** and press **Enter**. The system resets the NVM of the specified set-tops.

Reboot a Set-Top with the bootDhct Transaction

The bootDhct transaction reboots a single set-top, a list of set-tops, or set-tops of a specific model number.

Follow the instructions in this section to configure the IIH utility to send a bootDhct transaction.

Rebooting an Individual Set-Top

Follow these instructions to reboot an individual set-top.

1. Open an xterm window on the ISDS.
2. Type **IIH -b [set-top MAC address]** and press **Enter**. The system reboots the specified set-top.

   Notes:

   - Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets **[ ]** in the command.
   - The MAC address can be formatted with or without colons (:).

   Examples:

   IIH -b 00:02:DE:A6:45:92

   IIH -b 0002DEA64592

Rebooting a List of Set-Tops

Follow these instructions to reboot a list of set-tops.

1. Open an xterm window on the ISDS.
2. Do you want to force the system to process more than ten set-tops at a time?
   - If **yes**, go to step 3.
   - If **no**, go to step 4.
3. Type **IIH -b -C[# of set-tops] [text file name]** and press **Enter**. Go to step 5.

   Notes:

   - Substitute the number of set-tops you want to process at once for [# of set-tops]. Do not type the brackets **[ ]** in the command.
   - Substitute the name (including path) of the text file for [text file name]. Do not type the brackets in the command.

   Example: IIH -b -C50 /tmp/iih-in_11.31.02

   Result: A confirmation message, similar to the following, appears:

   ```
   DHCTs listed in file "[filename]" will be Rebooted …
   [#] MAC addresses will be involved.
   Do you want to continue? (Y/N)
   ```

4. Type **IIH -b [text file name]** and press **Enter**.

Note: Substitute the name (including path) of the text file for [text file name]. Do not type the brackets **[ ]** in the command.

Example: IIH -b /tmp/iih-in_11.31.02

Result: A confirmation message, similar to the following, appears:

```
DHCTs listed in file "[filename]" will be Rebooted …
[#] MAC addresses will be involved.
Do you want to continue? (Y/N)
```

5 Type **y** and press **Enter**. The system lists the MAC addresses of the set-tops as it sends a bootDhct transaction to each.

Rebooting Set-Tops of a Specific Model Number

Follow these instructions to reboot set-tops of a specific model number.

1 Open an xterm window on the ISDS.

2 Type **IIH -b -M[model number]** and press **Enter**.

Note: Substitute the model number of set-top for [model number]. Do not type the brackets **[ ]** in the command.

Example: IIH -b -M2100

Result: A confirmation message, similar to the following, appears:

```
saManager is running
DHCTs with DHCT model=[model number] will be Rebooted
# MAC addresses will be involved.
Do you want to continue (Y/N)?
```

3 Type **y** and **press** Enter. The system reboots the specified set-tops.

2way2oos

You sometimes need a way to reclaim IP addresses of set-tops that have been disconnected but never officially changed to "out-of-service" in the database.

A set-top that is no longer in use must have a status of out-of-service in the database for you to use the IP address of the set-top again. Systems that do not reclaim these IP addresses may run out of IP addresses when they try to deploy new set-tops in the homes of subscribers.

We developed the 2way2oos utility to change the status of set-tops to out-of-service in the database. You can prepare a text file that contains a list of MAC addresses of set-tops that you want to change to out-of-service and then use this text file as a parameter when you run the 2way2oos utility.

The instructions in this section provide guidelines for running the 2way2oos utility.

Using 2way2oos

Before running the 2way2oos utility, be sure that you have followed the instructions in Prepare the Text File, and that you have properly created and saved the file of MAC addresses that is to be used as input for the 2way2oos utility.

Be sure of the following important points:

- The file must contain only one MAC address per line.
- The file must be saved in the /dvs/dncs/tmp directory.
- The file must be named 2way2oos.txt.

Note: As a further precaution, you may want to examine the file before running the 2way2oos utility to ensure that the file contains only those MAC addresses of set-tops that are to be marked out-of-service in the database.

Follow these instructions to run the 2way2oos utility.

1 Open an xterm window on the ISDS.

2 Type **2way2oos.ksh** and press **Enter**. A message similar to the following appears:

```
## Total Settops to process
This could take approximately #.### hrs to complete.
Do you want to continue? (y/n)
```

Note: The number of set-tops and the length of time it takes to process them varies depending upon the number of set-tops you have included in your text file.

3 Type **y** and press **Enter**.

Results:

- The Beginning processing MAC addresses message appears.
- The All MACs have been processed message appears when the utility has finished running.

4 You need to stop and restart the HCT Manager process to make the IP addresses available for reuse. Go to ***Stop and Restart the HCT Manager Process*** (on page 479).

Stop and Restart the HCT Manager Process

You need to stop and restart the HCT Manager process on the ISDS to reclaim the IP addresses associated with the set-tops in your text file. The instructions in this section guide you through the steps of stopping and restarting the HCT Manager process.

Note: Stopping and then restarting a process is often referred to as "bouncing" the process.

Bouncing the HCT Manager process consists of the following steps:

1 ***Stopping the HCT Manager Process*** (on page 479).

2 ***Restarting the HCT Manager Process*** (on page 480).

Stopping the HCT Manager Process

1 Open an xterm window on the ISDS.

2 Type **dncsControl** and press **Enter**. The Dncs Control window opens.

3 Type **2** (for Startup / Shutdown Single Element Group) and press **Enter**. The Dncs Control window updates to list the status of all of the processes and servers running on the ISDS.

4 Type the number associated with **DNCS HCT Manager & OSM** and press **Enter**. The Dncs Control window updates to display a message that instructs you to enter the target status for the selected element group, or to type 'E' to display all of the elements in the group.

5 Type **1** (for stopped) and press **Enter**. A confirmation message appears.

6 Type **y** (for yes) and press **Enter**. The Dncs Control window updates to list the status of all the processes and servers running on the ISDS.

7 Wait until the current status (**Curr Stt**) of DNCS HCT Manager & OSM is stopped.

Note: The Dncs Control window updates automatically every few seconds or you can press Enter to force an update.

8 Your next step is to restart the HCT Manager process. Go to ***Restarting the HCT Manager Process*** (on page 480).

Restarting the HCT Manager Process

After stopping the HCT Manager process, follow these instructions to restart the process.

1 Type the number associated with the **DNCS HCT Manager & OSM** processes and press **Enter**. The Dncs Control window updates and displays a message that instructs you to enter the target status for the selected element group or to type E to display all of the elements in the group.

2 Type **2** (for running) and press **Enter**. A confirmation message appears.

3 Type **y** (for yes) and press **Enter**. The Dncs Control window updates to list the status of all the processes and servers running on the ISDS.

4 Wait until the current status (**Curr Stt**) of DNCS HCT Manager & OSM is running.

Note: The Dncs Control window updates automatically every few seconds or you can press **Enter** to force an update.

5 When the current status of the DNCS HCT Manager & OSM processes is running, follow the on-screen instructions to close the Dncs Control window.

mirrState

The Sun Fire V880 and V890 server platforms support disk mirroring. Through disk mirroring, the ISDS stores identical information across sets of hard drives.

System operators and support engineers who perform maintenance operations on a Sun Fire V880 and V890 ISDS may first be required to disable the mirroring functions on the ISDS. Then, after the maintenance operations are complete, the mirroring functions must be re-enabled.

Note: The disabling and re-enabling of the mirroring functions are usually referred to as "detaching" and "re-attaching" the mirrors.

The mirrState utility helps system operators and support engineers detach and re-attach the mirroring functions of the ISDS. Refer to the procedures in this section for information on how to run the mirrState utility.

Using mirrState

Select one of the following options when you run the mirrState utility:

- To disable the disk mirroring functions, go to ***Detaching Mirrored Disks*** (on page 481).
- To re-enable the disk mirroring functions, go to ***Re-Attaching Mirrored Disks*** (on page 481).
- To obtain the version number of the mirrState utility currently loaded onto the DNCS, go to ***Version Number of the mirrState Utility*** (on page 482).

Detaching Mirrored Disks

Follow these instructions to detach the mirrored disks on the ISDS server.

1. Has the output of the ***check_metadevices*** (on page 457) utility revealed any errors associated with the metadevices on your system?
   - If **yes**, correct those errors before proceeding any further.

     Important: The metadevices on your system must be working correctly before you can detach mirrored disks.
   - If **no**, go to step 2.
2. Log on to the xterm window as root user.
3. Type **mirrState.ksh -d** and press **Enter**. The system displays the following message:

   ```
   WARNING!!
   Proceeding beyond this point will DETACH all Controller 2 submirrors.
   Are you certain you want to proceed?
   ```
4. Type **y** and press **Enter**. The system disables the disk mirroring functions on the ISDS.
5. Type **exit** and press **Enter** to log out as root user in the xterm window.
6. Perform your maintenance operations on the ISDS and then go to ***Re-Attaching Mirrored Disks*** (on page 481).

Re-Attaching Mirrored Disks

Follow these instructions to use the mirrState utility to re-attach the mirrored disks.

1. Open an xterm window on the DNCS.
2. Log on to the xterm window as root user.

3 Type **mirrState.ksh -a** and press **Enter**. The system displays the following message:

```
WARNING!!
Proceeding beyond this point will ATTACH all Controller 2 submirrors.
Are you certain you want to proceed?
```

4 Type **y** and press **Enter**. The system re-enables the disk mirroring functions on the ISDS.

5 Type **exit** and press **Enter** to log out as root user in the xterm window.

Version Number of the mirrState Utility

Follow these instructions to obtain the version number of the mirrState utility that is loaded on the ISDS.

1 Open an xterm window on the ISDS.

2 Type **mirrState.ksh -v** and press **Enter**. The system displays the version number of the mirrState utility.

convertIP

The ISDS database stores set-top IP addresses in decimal format, our normal base-10 numbering system. IP addresses, however, are usually displayed in dotted-decimal notation, a format consisting of four 8-bit numbers separated by a dot.

Example: An example of an IP address in dotted-decimal notation is **10.1.64.86**. That very same IP address is stored in the database in decimal format as **167854166**.

The convertIP utility was developed to enable a quick conversion between the two formats. The utility converts an IP address in one format to an IP address in the other format.

Options

The convertIP utility accepts as an argument either a single IP address or the name of a file containing a list of IP addresses.

In general, use the single IP address when you have only one or two IP addresses to convert. When you have many IP addresses to convert, consider creating a text file that contains the IP addresses that you want to convert.

Using convertIP

To run the convertIP utility, choose one of the following options:

- To convert a single IP address, follow the instructions in ***Converting a Single IP Address*** (on page 483).
- To convert IP addresses listed in a file of IP addresses, follow the instructions in ***Converting a File of IP Addresses*** (on page 483).

Converting a Single IP Address

1. Open an xterm window on the ISDS.
2. Type **convertIP** and press **Enter**. The **Enter IP address to convert** message appears.
3. Type the IP address you want to convert and press **Enter**. The convertIP utility converts the IP address and displays both the original value and the converted value on the screen.

   Note: You can type the IP address in either format, decimal or dotted-decimal notation.

   Examples:

   - **Decimal-167854166**
   - **Dotted-decimal notation-10.1.64.86**

Converting a File of IP Addresses

Follow these instructions to use the convertIP utility to convert a file of IP addresses. When the convertIP utility runs, it displays each original and converted IP address on the screen of the ISDS, as well as writes the output to a user-specified file.

Important: You should already have prepared a text file containing IP addresses using the guidelines and directions in Prepare the Text File.

1. Open an xterm window on the ISDS.
2. Type **convertIP -f** and press **Enter**. The **Enter the file name (full path) containing IP addresses to convert** message appears.
3. Type the name of the file you prepared (including the full directory path) and press **Enter**.

   Example: Type **/dvs/dncs/tmp/IP_input_file** and press **Enter**.

   Result: The message **Enter the file name (full path) in which to store the converted IP addresses** appears.
4. Type the name of the file (including the full directory path) in which you want to store the output and press **Enter**.

   Example: Type **/dvs/dncs/tmp/IP_output_file** and press **Enter**.

   Results:

   - The convertIP utility converts the IP addresses and displays both the original value and the converted value on the screen of the ISDS.
   - The convertIP utility displays the number of IP addresses that were converted and suggests that you review the converted IP addresses by examining the output file.

   Example:

```
There are 16 IP addresses in the /dvs/dncs/tmp/IP_input_file file that were
converted. Please review the converted IP addresses in the
/dvs/dncs/tmp/IP_output_file file.
```

getCCdata

The getCCdata utility was developed for the purpose of reporting errors and retrieving data that pertains to CableCARD modules. Examples of the errors reported and the data retrieved include whether the servers that support the CableCARD modules are running and configured correctly, whether the mmi and gfc files are present and configured correctly on the Broadcast File System (BFS) server, and whether CableCARD data is properly represented in the database.

You Need to Know

Output From the getCCdata Utility

When to Run the getCCdata Utility

Run the getCCdata Utility

Follow these instructions to run the getCCdata utility.

1. If necessary, open an xterm window on the ISDS.
2. Type **getCCdata.ksh** and then press **Enter**. The utility runs, generating data to the screen of the ISDS, as well as writing data to two files stored in the /tmp directory of the ISDS.

   Note: On most systems, the utility takes only a minute or two to run.

Sample Output from the getCCdata Utility

The following table lists some sample output from the getCCdata utility. The table includes two columns. The first column includes sample output from the error-reporting portion of the utility; the second column contains the supporting data. There is a one-to-one relationship between the two parts of the output. For each entry in the error part, there is a corresponding entry in the data part.

Note: The first row of the following table includes the actual headings that introduce the the error portion and the data portion of the output generated by the getCCdata utility. As shown in the table, the heading contains the name of the corresponding file, the current version of the getCCdata utility, and the version of software that is running on the ISDS.

Error Report	Data Report
CableCardErrors.out.050510_1424.doc	CableCardData.out.050510_1423.doc
getCCdata.ksh v1.09	getCCdata.ksh v1.09
DNCS Version: 3.5.0.14	DNCS Version: 3.5.0.14

Error Report	Data Report
*****Check 1: CCardServer running:***** ========== Yes	*****Check 1: CCardServer running:***** ========== dncs 25974 587 0 Apr 14 ? 0:18 Logger -g -n /dvs/dncs/tmp/CCardServer dncs 26303 25974 0 Apr 14 ? 21:30 /dvs/dncs/bin/CCardServer
*****Check 2: CCardServer log files:***** ========== Yes: There are multiple CCardServer log files.	*****Check 2: CCardServer log files:***** ========== -rw-r--r-- 1 dncs dncs 2213862 Apr 17 09:58 /dvs/dncs/tmp/CCardServer.000 -rw-r--r-- 1 dncs dncs 2212512 Apr 20 08:12 /dvs/dncs/tmp/CCardServer.001 -rw-r--r-- 1 dncs dncs 2212214 Apr 23 06:22 /dvs/dncs/tmp/CCardServer.002 -rw-r--r-- 1 dncs dncs 2212308 Apr 26 04:33 /dvs/dncs/tmp/CCardServer.003 -rw-r--r-- 1 dncs dncs 2212482 Apr 29 02:46 /dvs/dncs/tmp/CCardServer.004 -rw-r--r-- 1 dncs dncs 2212347 May 2 00:59 /dvs/dncs/tmp/CCardServer.005 -rw-r--r-- 1 dncs dncs 2212411 May 4 23:12 /dvs/dncs/tmp/CCardServer.006 -rw-r--r-- 1 dncs dncs 2212402 May 7 21:25 /dvs/dncs/tmp/CCardServer.007 -rw-r--r-- 1 dncs dncs 2046713 May 10 14:22 /dvs/dncs/tmp/CCardServer.008
****Check 8: loghost in /etc/hosts File***** ========== Yes: There is a single loghost entry in the hosts file.	*****Check 8: loghost in /etc/hosts File***** ========== 192.168.1.1 dncs loghost
****Check 10: Server Defined on BFS:***** ========== Yes	*****Check 10: Server Defined on BFS:***** ========== 41338e6d0000000500002004 | podServer | 1 | 41338e6d0000000700002004 | POD_Data | 1 | 3394330c20a6005e92000001 | POD_Data | -1 | 3394330c8c5d005e92000001 | podServer | -1 |

Error Report	Data Report
*****Check 12: mmi File on BFS:***** ========== Yes	*****Check 12: mmi File on BFS:***** ========== 563|18|2|9|mmi.txt|/DNCS/POD_Data/mmi.txt|12|41338e6d0000000700002004|3390520b366600293f000001|0|70|-1317659392|1115128521|0|1|
****Check 16: Cable Card on Type List:**** ========== Yes	*****Check 16: Cable Card on Type List:***** ========== 10|600|734|Explorer 600 CableCARD Rev 1.0|Scientific-Atlanta|||0|
*****Check 24: Files in podServer:***** ========== Yes	*****Check 24: Files in podServer:***** ========== total 2 -rw-r--r-- 1 dncs dncs 60 Apr 14 12:11 podData
*****Check 29: NOTE:***** ========== The location of the output file is /tmp/CableCardErrors.out.050510_1424.doc	*****Check 29: NOTE:***** ========== The location of the output file is /tmp/CableCardData.out.050510_1423.doc

getEASdata

The Federal Communications Commission established the Emergency Alert System (EAS) in 1994 as a tool for government officials to quickly transmit important emergency information that is targeted to specific geographical areas.

Digital cable system operators need a reliable EAS at their headend to ensure that their subscribers receive national, state, and local warning messages about emergency conditions.

The getEASdata utility ensures the reliability of your EAS. The utility helps you troubleshoot your EAS by reporting EAS-related errors and retrieving data associated with system components that pertain to the EAS. The following list includes some of the EAS-related data retrieved by the getEASdata utility:

- Emergency Alert Controller (EAC) network configuration
- Emergency Alert Receiver (EAR) and Multi-Media Message (MMM) Server processes

  Note: The EAR server monitors and receives EAS-related messages and then passes the messages to the MMM server for formatting and processing.
- Files in the /export/home/easftp directory

- Files converted to audio interchange file format (AIFF) and loaded onto the broadcast file server (BFS) carousel

  Note: Files in AIFF are high-quality sound files.

- EAS timing data

You Need to Know

When to Use getEASdata

Before Using getEASdata

Using getEASdata

The getEASdata utility generates two reports, the EAS Error Report and the EAS Data Report.

- The EAS Error Report highlights errors that the utility discovers in its examination of the EAS configuration.
- The EAS Data Report displays EAS configuration data that the system operator can then examine to identify the source of the error.

We recommend that you generate each report whenever you run the getEASdata utility, even if the EAS Error Report shows no errors. Examining EAS configuration data may be useful in preventing errors before they develop.

1. Open an xterm window on the ISDS.
2. Type **getEASdata.ksh** and press **Enter**. The utility displays a menu instructing you to select 1 to generate an EAS Error Report or to select 2 to generate an EAS Data Report.
3. Type **1** (for Report EAS Errors) and press **Enter**. The utility lists several conditions that must be true before you run the report.

   Note: These conditions are discussed in Before Using getEASdata.
4. Type **y** and press **Enter**. The following message appears:

   ```
   Enter the IP address of a DHCT that should have received the EAS message
   and/or hit return to continue.
   ```
5. Type the **IP address** of a test set-top that did not receive the EAS message, and press **Enter**.

   Note: If you fail to provide an IP address, the utility will still run but it will not provide data in the EAS data on a DHCT section of the EAS Error Report.

   Result: The following message appears:

   ```
   Enter the diagnostic screen the EAS data is on and/or hit return to continue.
   ```
6. Type the number of the set-top diagnostic screen that contains EAS-related data and press **Enter**.

   Note: If you fail to provide the number of the diagnostic screen, the utility will still run but it will not provide data in the EAS data on a DHCT section of the EAS Error Report.

Results:

- The system runs the EAS Error Report and displays the output to the screen of the ISDS.
- The system displays a message that states that the EAS Error Report can also be found in the **/tmp/EASerrors.out.[Date].doc** file.
- The system displays the menu of the getEASdata utility.

7 Type **2** (for Show EAS Data) and press **Enter**. The following message appears:

```
Enter the IP address of a DHCT that should have received the EAS message
and/or hit return to continue.
```

8 Type the **IP address** of a test set-top that did not receive the EAS message, and press **Enter**. The following message appears:

```
Enter the diagnostic screen the EAS data is on and/or hit return to continue.
```

9 Type the number of the set-top diagnostic screen that contains EAS-related data and press **Enter**.

Results:

- The system runs the EAS Data Report and displays the output to the screen of the ISDS.
- The system displays a message that states that the EAS Data Report can also be found in the **/tmp/EASdata.out.[Date].doc** file.

10 The system displays the menu of the getEASdata utility.

11 Type **q** (for quit) and press **Enter**. The getEASdata utility closes.

Examine the getEASdata Reports

This section provides instructions on opening the two reports generated and saved by the getEASdata utility, provides some guidance on examining the data, and shows a few examples of EAS-related errors that you might find.

Opening the getEASdata Utility Reports

Follow these instructions to open the two reports generated and saved by the getEASdata utility.

The instructions direct you to open the reports side-by-side in two xterm windows. By examining the two reports simultaneously, you can better understand the relationship of the reports.

1 Open two xterm windows on the ISDS.

2 Type **cd /tmp** in both of the xterm windows and press **Enter**. The /tmp directory becomes the working directory.

3 In one xterm window, type **ls EASerrors*** and press **Enter**. The system lists all files in the /tmp directory that begin with EASerrors.

Notes:

- The system stores EAS Error Report files in **EASerrors.out.[date].doc** format, where the date is expressed in terms of YYMMDD_HHMM.

- By listing all EAS Error Report files, you can easily identify which one pertains to the most recent report you generated.

4 In the same xterm window, type **more [EAS Error Report name]** and press **Enter**. The selected EAS Error Report opens in the xterm window using the UNIX more utility.

Note: Substitute the name of the EAS Error Report file that you want to open for [EAS Error Report name]. Do not type the brackets **[ ]** in the command.

Example: Type **more EASerrors.out.031008_1541.doc** and press **Enter**.

5 In the other xterm window, type **ls EASdata*** and press **Enter**. The system lists all files in the /tmp directory that begin with EASdata.

Notes:

- The system stores EAS Data Report files in **EASdata.out.[date].doc** format, where the date is expressed in terms of YYMMDD_HHMM.
- By listing all EAS Data Report files, you can easily identify which one pertains to the most recent report you generated.

6 In the xterm window you used in step 5, type **more [EAS Data Report name]** and press **Enter**. The selected EAS Data Report opens in the xterm window.

Note: Substitute the name of the EAS Data Report file that you want to open for [EAS Data Report name]. Do not type the brackets in the command.

Example: Type **more EASdata.out.031008_1542.doc** and press **Enter**.

7 Go to ***Examining the getEASdata Utility Reports*** (on page 489) for help in understanding the reports.

Examining the getEASdata Utility Reports

Refer to these instructions for general guidance in reviewing the two reports generated by the getEASdata utility.

These instructions provide an example of one error that you might find. Refer to ***Sample EAS-Related Errors*** (on page 490) for additional examples.

1 Scroll through the EAS Error Report. As you scroll through the various headings contained in the report, look for errors. Errors are clearly marked in the report by the word Error.

Example: The ***** **eac in /etc/hosts.equiv** ***** heading in the EAS Error Report might include an error message similar to the following:

```
Error: There is no entry for eac in the hosts.equiv file.
```

Note: The eac needs to have one entry in the /etc/hosts.equiv file.

2 After locating an error in the EAS Error Report, look for the corresponding data in the EAS Data Report.

Example: Using the example in step 1, the ***** **eac in /etc/hosts.equiv** ***** heading in the EAS Data Report might show that there is no line in the /etc/hosts/equiv file that contains eac.

3 Troubleshoot each error you find to the best of your ability.

Notes:

- Refer to one of the following documents as you troubleshoot the errors:
  - *Configuring and Troubleshooting the Digital Emergency Alert System* (part number 4004455)
  - *Configuring and Troubleshooting the Digital Emergency Alert System for ISDS Networks User Guide* (part number 4024428)
  - *Distributed EAS on the Regional Control System, Configuration and Troubleshooting Guide* (part number 4002342)
- Call Cisco Services for assistance if you need it.

4 After correcting errors, transmit another EAS message and run the getEASdata utility again.

Sample EAS-Related Errors

Refer to the following list for a discussion of a few additional EAS-related errors:

- The EAS Error Report may include an error under the ***** **VASP data for the MMM Server in the database** ***** heading. The error may be similar to the following:

  ```
  Error: VASP IP
  ```

  Meanwhile, the corresponding ***** **VASP data for the MMM Server in the database** ***** heading in the EAS Data Report may indicate that the asynchronous transfer mode (ATM) address of the ISDS or the Application Server is incorrect.

  Solution: Correct the IP address for the MMM server on the ISDS.

- The EAS Error Report may include the following error under the ***** **Timing Analysis** ***** heading:

  ```
  Error: The message Origination Time and Appserver time are out of sync
  ```

  Under the ***** **EAS messages sent** ***** heading of the EAS Data Report, the data may show that too much time expired between when an EAS message was transmitted and then received.

  Solution: Call Cisco Services. Resolving timing issues requires the help of engineers from Cisco Services.

modDhctCfg

You can use the modDhctCfg utility to transmit the ModifyDhctConfiguration transaction to set-tops. The ModifyDhctConfiguration transaction modifies the status and authorizations of one or more set-top records.

Note: Consult your copy or your billing vendor's copy of the Business Operations Support System (BOSS) Interface Specification document for a complete description of the ModifyDhctConfiguration transaction.

The modDhctCfg utility retrieves authorization and package data from the database, formats it into the ModifyDhctConfiguration transaction, and transmits it to the appropriate set-top(s). The main purpose of the utility is to regenerate and send EMMs to set-tops. The utility essentially refreshes a set-top by sending the last ModifyDhctConfiguration transaction that the ISDS received for the set-tops.

Note: To generate and transmit staging EMMs, use the -s option with the modDhctCfg utility. Instructions for using the -s option, as well as other options supported by the modDhctCfg utility, are provided throughout this section.

Staging Operations and the Billing Interface

When the modDhctCfg utility runs, it tends to compete for system resources with staging operations, as well as with the activities of the billing computer.

If you have to process a large number of set-tops with the modDhctCfg utility, and if time is important, consider temporarily disabling the billing interface and suspending staging operations.

Options

The following table describes the options that are available for use with the modDhctCfg utility. <<*Walt to review this section*.>>

Note: Do not type the brackets **[ ]** in any of the following commands.

Option	Purpose
-?	The **-?** option displays the help window associated with the modDhctCfg utility. **Example: modDhctCfg -?**
-v	The **-v** option displays the version number of the modDhctCfg that is installed on your system. **Example: modDhctCfg -v**
-h	The **-h** option specifies the hostname or IP address of the ISDS when the modDhctCfg utility executes on a remote computer. **Example: modDhct -h172.18.28.176 +dms [set-top MAC address]**
+a -a	Not applicable to ISDS.
-B#	The **-B** option sets the blocking factor for the modDhctCfg transaction. The blocking factor refers to the number of set-top records transmitted at one time in the modDhctCfg transaction. **Note:** The default blocking factor is 10. **Example: modDhctCfg -B50 [file name]**
-c#	Not applicable to ISDS.

+dms -dms	The **+dms** and **-dms** options enable (+) or disable (-) digital packages for the set-top. **Example: modDhctCfg +dms [set-top MAC address]**
+dis -dis	The **+dis** and -dis options are used to enable (+) or disable (-) the decryption of encrypted sessions. **Example: modDhctCfg +dis [set-top MAC address]**
-e#	Not applicable to ISDS.
+f -f	The **+f** and **-f** options determine whether the fast_refresh parameter is set to on (+) or off (-). The ISDS sends EMMs to set-tops that are on the "fast refresh list" automatically; subscribers or installation engineers are not required to telephone the headend when they want a set-top enabled. **Example: modDhctCfg +f [file name]**
-l	The -l option instructs the ISDS to process imported set-top records from another ISDS. This option deletes the secure_micro record from the database and sets to null the ip_address field. To restore this data, the set-tops must reboot. **Example: modDhctCfg -l [file name]**
+i -i	Not applicable to ISDS.
+pXX -pXX	The **+pXX** and **-pXX** options add (+) or remove (-) package XX from a set-top. **Example: modDhctCfg +pHBO [set-top MAC address]**
!pQQQ	The **!pQQQ** option replaces all packages assigned to a set-top with the packages included in file QQQ. **Note:** File QQQ must contain only one package name per line. **Example: modDhctCfg !p[package file name] [set-top MAC address]**
-s	The **-s** option restages set-tops. The secure_micro record in the database is deleted and then re-added. **Example: modDhctCfg -s [file name]**

Using modDhctCfg

The instructions and examples in this section describe how to use the modDhctCfg utility.

This section covers those options that our engineers think you are most likely to use. Refer to ***Options*** (on page 491) for examples showing how to use the various supported options.

Note: The transaction that the utility sends is the same ModifyDhctConfiguration transaction that was sent to the set-top(s) the last time the set-tops received a ModifyDhctConfiguration transaction. The utility simply retrieves the data from the database and re-transmits it.

Sending modDhctCfg to a Single Set-Top

Follow these instructions to send the ModifyDhctConfiguration transaction to a single set-top.

1. Open an xterm window on the ISDS.
2. Type **modDhctCfg [set-top MAC address]** and press **Enter**. The system sends the ModifyDhctConfiguration transaction to the specified set-top.

   Note: Substitute the MAC address of the set-top for [set-top MAC address]. Do not type the brackets **[ ]** in the command.

   Example: modDhctCfg 00:02:DE:4A:11:92

Sending modDhctCfg to a List of Set-Tops

Important:

- The list of set-tops must already exist on the ISDS.
- Follow the guidelines for creating text files when you create the list of set-tops. Refer to ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396) for more information.

Follow these instructions to send the ModifyDhctConfiguration transaction to a list of set-tops.

1. Open an xterm window on the ISDS.
2. Type **modDhctCfg [file name]** and press **Enter**. The system sends the ModifyDhctConfiguration transaction to all the set-tops represented in the file.

   Note: Substitute the name of the file you prepared for [file name]. Do not type the brackets **[ ]** in the command.

   Example: modDhctCfg modDhctCfg-in_11.13.03

Sending modDhctCfg with a Blocking Factor

The blocking factor option specifies now many set-top records the modDhctCfg utility transmits as a block.

When the blocking factor is not specified, the utility uses a default blocking factor of 10. When you urgently need to use the utility to send the ModifyDhctConfiguration transaction to a large number of set-tops, you might want to increase the blocking factor. An increased blocking factor has the effect of increasing the priority of the transactions.

Important:

- Keep in mind that increasing the blocking factor associated with the modDhctCfg utility increases the claim the utility has on system resources. When practical, suspend staging activities and shut down the billing interface before running the modDhctCfg utility with a large blocking factor.
- The list of set-tops must already exist on the ISDS.
- Follow the guidelines for creating text files when you create the list of set-tops. Refer to ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396) for more information.

Follow these instructions to specify the blocking factor used with the modDhctCfg utility.

1 Open an xterm window on the ISDS.

2 Type **modDhctCfg -B# [file name]** and press **Enter**.

Notes:

- Substitute the blocking factor that you want to use for #.
- Substitute the name of the file you prepared for [file name]. Do not type the brackets **[ ]** in the command.

Examples:

- Type **modDhctCfg -B100 modDhctCfg-in_11.13.03** and press **Enter**.

  Result: The system sends the ModifyDhctConfiguration transactions, blocked 100 at a time, to the set-tops represented in the file named in_11.13.03.

- Type **modDhctCfg -B2 modDhctCfg-in_11.13.03** and press **Enter**.

  Result: The system sends the ModifyDhctConfiguration transactions, blocked 2 at a time, to the set-tops represented in the file named in_11.13.03.

  Important: This example (using a small blocking factor) minimizes the claim that the utility has upon system resources. Consider using a small blocking factor while staging operations are ongoing or during periods of high customer service representative (CSR) activity.

HOLD Sending modDhctCfg to Enable or Disable Session-Based Encryption

The **dis** option enables or disables session-based encryption. Follow these instructions to use the modDhctCfg utility with the dis option.

1 Open an xterm window on the ISDS.

2 Choose one of the following options:

- To enable session-based encryption for the specified DHCT, type **modDhctCfg +dis [set-top MAC address]** and press **Enter**.
- To disable session-based encryption for the specified DHCT, type **modDhctCfg -dis [set-top MAC address]** and press **Enter**.

Note: Substitute the MAC address of the appropriate set-top for [set-top MAC address]. Do not type the brackets **[ ]** in the commands.

Sending modDhctCfg to Restage Set-Tops

When used with the modDhctCfg utility, the **-s** option generates staging EMMs.

Important:

- The modDhctCfg utility cannot be used to stage a set-top for the first time. The utility reads information about the set-top from the database to formulate a valid ModifyDhctConfiguration transaction. Set-tops must be staged according to normal staging procedures to populate the database properly.
- The list of set-tops must already exist on the ISDS.
- Follow the guidelines for creating text files when you create the list of set-tops.Refer to ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396) for more information.

Use the following instructions when using the modDhctCfg utility to stage set-tops.

1 Open an xterm window on the ISDS.

2 Type **modDhctCfg -s [file name]** and press **Enter**. The system generates staging EMMs for the set-tops listed in the specified file.

   Note: Substitute the name of the file you prepared for [file name]. Do not type the brackets **[ ]** in the command.

   Example: Type **modDhctCfg -s modDhctCfg-in_11.13.03** and press **Enter**.

preserveLog

The processes that run on the ISDS create log files when they run. These log files contain data, such as the values of parameters at process entry and exit points, that help system operators and engineers troubleshoot the system.

To conserve space, the system places limitations on the number and size of each log file that it stores. When this limit is reached, old log files "roll over" or "roll off" and are replaced with new log files, often before anyone has had an opportunity to examine the old files.

Log files associated with some processes, such as drm and dsm, roll over at an especially quick rate, often as rapidly as every 5 minutes. In addition, whenever a process is stopped and then restarted (known as "bouncing" the process), existing log files are erased.

The preserveLog utility allows the system to save log files for later examination. The preserveLog utility can save log files for processes that run on the ISDS and on the Application Server.

The preserveLog utility can run from the command line of an xterm window on the ISDS. In addition, an entry for the preserveLog utility can be placed in the crontab (cron) file of the ISDS where it can be configured to automatically preserve log files for specific processes.

What Log Files can be Preserved?

The preserveLog utility can save log files for every process that runs on the ISDS. For the Application Server, the preserveLog utility saves "types" of log files.

When the preserveLog utility runs, it begins by creating a unique date directory in the **/export/home/dncs/scripts/saInternalTools/preserveLog/directory** structure on the ISDS.

The utility then creates a directory for each unique log file and copies the specified log files from the /dvs/dncs/tmp directory on the ISDS to this new directory.

For Application Server log files, the utility uses remote procedure calls to transfer the log files from Application Server to the ISDS. Finally, to minimize disk usage, the preserveLog utility uses the gzip utility to compress the log files to be preserved.

Example: The following is an example of what the preserveLog directory structure looks like:

```
/export/home/dncs/scripts/saInternalTools/preserveLog/06_10_08/drm
```

Inside of the drm directory (as noted in this example) are the various compressed log files that pertain to the drm logs.

By default, the utility keeps two days of preserved log files. When the third day's log files are received, the utility deletes log files from the earliest day. You can change the number of days of log files that are preserved by modifying preserveLog file in the /export/home/dncs/scripts/saInternalTools/preserveLog directory. See ***Customize preserveLog*** (on page 497) for additional information.

Confirm Sufficient Storage Space

Before the preserveLog utility runs, the utility confirms that there is sufficient space in the /export/home file system to save the log files.

If the preserveLog utility determines that the **/export/home** file system is at or over 80 percent capacity, the utility displays a message similar to the following:

```
Tue Jun 20 08:39:09 EDT 2006

PROGRAM TERMINATED.  /export/home is at or over 80%!
```

Additionally, the utility transmits a message similar to the following to every open terminal on the system:

```
Broadcast Message from dncs (pts7) on lville Tue Jun 20 08:39:09

/export/home at 80%

PROGRAM TERMINATED!

Please check disk space!
```

You should then proceed to free up space in the /export/home file system.

Customize preserveLog

By default, the preserveLog utility keeps two days of preserved files for each process before deleting old files. You can change the number of days of log files that are preserved by modifying the code for the preserveLog utility.

Important: Before you edit the preserveLog file, note these important points:

- Do not attempt to edit the preserveLog file unless you are a skilled user of the UNIX vi text editing utility. Call Cisco Services for assistance in editing this file if you are unsure of your ability to make the edit yourself.
- We recommend that you use only the UNIX vi text editor to make the edits. A Windows-based utility may inadvertently introduce Windows control characters into the file, often with unpredictable results.

1. Open an xterm window on the ISDS.
2. Type **cd /dvs/dncs/bin** and press **Enter**.
3. Type **vi preserveLog.ksh** and press **Enter**. The preserveLog file opens for editing using the UNIX vi text editor.
4. Locate the following line:

   ```
   if [[ $c -gt 2 ]]
   ```

   Note: The **2** in this line represents the number of days of log files that are to be preserved.
5. Replace the 2 with however many days of log files you want to preserve.

   Examples:

   - To save 3 days of data, the line should look like the following:

     ```
     if [[ $c -gt 3 ]]
     ```
   - To save 4 days of data, the line should look like the following:

     ```
     if [[ $c -gt 4 ]]
     ```
6. Save the file and close the UNIX vi editor.

   Note: Remember to change the command back to the default value of 2 days when you no longer need the customized entry.

Using preserveLog

You can use preserveLog from the command line, or you can run it as a cronjob.

From the Command Line

This section contains instructions and an example for running the preserveLog utility from an xterm window on the ISDS, also known as running the utility "from the command line".

In addition, this section contains a procedure for confirming that the utility actually preserved the log files, as intended.

Running preserveLog From the Command Line

1 Open an xterm window on the ISDS.

2 Type **preserveLog.ksh [logname] [logname] [logname]** and press **Enter**.

Note: Substitute the name of the log file for [logname] for as many log files as you want to preserve. Do not type the brackets **[ ]** in the command.

Example: To preserve log files for the dsm and drm processes on the ISDS, type **preserveLog.ksh dsm drm** and press **Enter**.

Confirming the Preserved Log Files

You can confirm that the preserveLog utility saved the log files for future reference by following these instructions.

The example used in this procedure references the log files associated with the dsm process.

1 Open an xterm window on the ISDS.

2 Type **cd /export/home/dncs/scripts/saInternalTools/preserveLog** and press **Enter**. The specified directory becomes the working directory.

3 Type **ls -la** and press **Enter**. The system displays a list of directories named according to the date on which the preserveLog utility was run. The format of the directories is YY_MM_DD.

Example: The directory for July 5, 2008 is 08_07_05.

4 Select one of the dates revealed in the results of step 3 and type cd [date] and press **Enter**.

5 Type **ls -la** and press **Enter**. The system displays a list of directories named according to the various log files that it has preserved.

6 Select one of the log file directories and type cd [directory] and press **Enter**.

Example: To change directories into the dsm directory, type cd dsm and press **Enter**.

7 Type **ls -la** and press **Enter**. The system displays the name or names of however many compressed log files reside within the directory.

Example: This example shows a series of compressed dsm log files.

```
-rw-r--r--   1 dncs     dncs      178152 Jul  5 14:15 dsm.005.gz
-rw-r--r--   1 dncs     dncs      177441 Jul  5 14:15 dsm.006.gz
-rw-r--r--   1 dncs     dncs      178695 Jul  5 14:15 dsm.007.gz
-rw-r--r--   1 dncs     dncs      179044 Jul  5 14:15 dsm.008.gz
-rw-r--r--   1 dncs     dncs      178703 Jul  5 14:15 dsm.009.gz
-rw-r--r--   1 dncs     dncs      184693 Jul  5 14:15 dsm.010.gz
```

Displaying the preserveLog Help Window and Version Number

Follow these instructions to display the help window and version number of the preserveLog utility.

1 Open an xterm window on the ISDS.

2 Choose one of the following options:

- To display the help window of the preserveLog utility, type **preserveLog.ksh -h** and press **Enter**.
- To display the version number of the preserveLog utility, type **preserveLog.ksh -v** and press **Enter**.

From the crontab File

This section describes how to place an entry for the preserveLog utility into the crontab file of the ISDS, commonly referred to as the "cron" file.

When run from cron, the utility executes automatically at a pre-defined interval, without user intervention.

Tip: The log files for the drm and dsm processes are especially susceptible to "rolling over" before anyone has had an opportunity to review the contents of the files. The log files for these processes are especially suited for having a cron entry for the preserveLog process save their contents.

Important: Do not attempt to edit the crontab file on the ISDS unless you are a skilled user of the UNIX vi text editor and are familiar with how cron entries are structured.

1. Open an xterm window on the ISDS.
2. Type **export EDITOR=v**i and press **Enter**.
3. Type **crontab -e** and press **Enter**. The crontab file opens for editing using the UNIX vi text editor.
4. Append an entry in the crontab file similar to the following example for the preserveLog utility:

   ```
   00,10,20,30,40,50 * * * *
   /dvs/dncs/bin/preserveLog.ksh < logname > < logname >  < logname >  2>&1
   ```

   Example: A cron entry that preserves the log files of the dsm and drm processes every 10 minutes would be structured similarly to:

   ```
   00,10,20,30,40,50 * * * *
   /dvs/dncs/bin/preserveLog.ksh  dsm drm  2>&1
   ```
5. Save the crontab file and close the UNIX vi editor.

Examine the Log Files

Use the gzcat command to examine the compressed log files on an ISDS system. The following instructions guide you through the necessary steps.

Examining the Log Files

1. Open an xterm window on the ISDS.
2. Type **cd /export/home/dncs/scripts/saInternalTools/preserveLog/** and press **Enter**.
3. Type **ls -la** and press **Enter**. The system displays all of the date directories that have been created by the preserveLog utility.

4 Type **cd [date]** and press **Enter**.

Note: Substitute [date] with the actual date associated with the log files you want to view. Do not type the brackets **[ ]** in the command.

5 Type **ls -la** and press **Enter**. The system displays all of the log directories that have been created by the preserveLog utility for the date you entered previously.

6 Type **cd [directory]** and press **Enter**. The selected log file directory becomes the working directory.

7 Type **ls -la** and press **Enter**. The system displays a list of the compressed files in the working directory.

8 To view the contents of a specific log, type **gzcat [filename] | less** and press **Enter**.

Example: Type **gzcat dsm.005.gz | less** and press **Enter**.

Results:

- The selected file opens for review using the gzcat utility.
- The contents of the file are piped to the UNIX less utility.

Tips for Moving Through the Log File

Use the following tips to maneuver through the file piped to the less utility:

- To move a whole page (screen) forward, press either the **Spacebar** or the **f** key.
- To move a whole page (screen) backward, press the **b** key.
- To move a single line forward, press the **j** key.
- To move a single line backward, press the **k** key.
- To exit from the file, press the **q** key.

tellDhctInfo

You can use the tellDhctInfo utility to obtain authorization data about a single set-top or a list of set-tops.

- To obtain information about a single set-top, supply the tellDhctInfo utility with the MAC address or the serial number of the set-top.
- To obtain information about a list of set-tops, supply the tellDhctInfo utility with the name of a file that contains a list of MAC addresses or serial numbers.

Options

Refer to the following table for an explanation of the options available with tellDhctInfo.

Option	Purpose
-?	Displays the help window associated with the tellDhctInfo utility. **Example: tellDhctInfo -?**
-v	Displays the version number of the tellDhctInfo that is installed on your system. **Example: tellDhctInfo -v**
MAC address or serial number	When used in conjunction with the MAC address or serial number of a single set-top, the tellDhctInfo utility provides the authorization data for that set-top. When used in conjunction with a text file containing a list of set-top MAC addresses or serial numbers, the utility provides authorization data for each set-top represented in the text file. **Examples:** ■ **tellDhctInfo [DHCT MAC address]** ■ **tellDhctInfo [DHCT serial number]** ■ **tellDhctInfo [file name]** **Note:** Do not type the brackets **[ ]** in the command.
-b	Formats set-top authorization data into two lines of output. Each line is preceded by the MAC address of the set-top. This format is referred to as "brief" format. **Note:** While suitable for use with the MAC address or serial number of a single set-top, this option is most useful when used with a text file containing a list of set-top MAC addresses or serial numbers. **Example: tellDhctInfo -b [file name]** **Note:** Do not type the brackets **[ ]** in the command.
-d	Lists the subscription packages on the ISDS or assigned to a set-top. **Examples:** ■ **tellDhctInfo -d** ■ **tellDhctInfo -d [DHCT MAC address]** **Note:** Do not type the brackets **[ ]** in the command.
-d2	Lists the packages on the ISDS, as well as the segments within each package. **Example: tellDhctInfo -d2**

-x	Provides set-top authorization data and formats it in such a way that it is suitable for importation into a Microsoft Excel spreadsheet. **Note:** While suitable for use with the MAC address or serial number of a single set-top, this option is most useful when used with a text file containing a list of set-top MAC addresses or serial numbers. **Example: tellDhctInfo -x [file name]** **Note:** Do not type the brackets **[ ]** in the command.

Using tellDhctInfo

This section contains procedures for using the tellDhctInfo utility.

Obtain Authorization and Subscription Data for an Individual Set-Top

The information in this section describes how to use the tellDhctInfo utility to obtain authorization data for an individual set-top.

Obtaining Authorization Data for an Individual Set-Top

1. Open an xterm window on the ISDS.
2. Type **tellDhctInfo [set-top MAC address or serial number]** and press **Enter**. The system displays authorization data for the specified set-top.

   Notes:

   - Substitute the MAC address or serial number of the set-top for [set-top MAC address or serial number].
   - Do not type the brackets **[ ]** in the command.

   Examples:

   tellDhctInfo 00:40:7B:C1:CD:CE

   tellDhctInfo SABFXHXNQ
3. Repeat the procedure for any other set-top for which you want to obtain authorization data.

Obtaining Subscription Data for an Individual Set-Top

Follow this procedure to obtain subscription package authorization data for a set-top, as well as listing all subscription packages available on the ISDS.

1. Open an xterm window on the ISDS.
2. Type **tellDhctInfo -d [set-top MAC address or serial number]** and press **Enter**. The system displays all subscription packages available on the ISDS, as well as subscription package authorization data for the selected set-top.

   Notes:

   - Substitute the MAC address or serial number of the set-top for [set-top MAC address or serial number].

- Do not type the brackets **[ ]** in the command.

Examples:

tellDhctInfo -d 00:40:7B:C1:CD:CE

tellDhctInfo -d SABFXHXNQ

3 Repeat the procedure for any other set-top for which you want to obtain subscription data.

Obtain Authorization Data for a List of Set-Tops

The information in this section describes how to use the tellDhctInfo utility with a text file that contains a list of set-top MAC addresses or serial numbers.

Be sure that you have already created the text file by following the guidelines and instructions in ***Guidelines for Text Files in ISDS Utilities*** (see "***Preparing Text Files for ISDS Utilities***" on page 396).

Tip: When you use a text file that contains a list of set-top MAC addresses or serial numbers, direct the output to another file. Output data tends to scroll so quickly off the screen that it might be unusable. When output is stored in a file, you can reference it at your convenience, as well as search for specific items of data. The instructions in this section make use of an output file.

Obtaining Authorization Data for a List of Set-Tops - Standard Output

1 Open an xterm window on the ISDS.

2 Type **tellDhctInfo [input file name] > [output file name]** and press **Enter**. The utility provides authorization data for each set-top represented in the input file and directs the output to the specified output file.

Notes:

- Substitute the name of the prepared input file for [input file name].
- Substitute the name of the file where you want to store the output for [output file name].
- Do not type the brackets **[ ]** in the command.

Example:

Type **tellDhctInfo /tmp/tellDhct-in_11.13.03 > /tmp/tellDhct-out_11.13.03** and press **Enter**.

3 Use the UNIX **more** utility to review the data in the output file.

Obtaining Authorization Data for a List of Set-Tops - Brief Format Output

1 Open an xterm window on the ISDS.

2 Type **tellDhctInfo -b [input file name] > [output file name]** and press **Enter**. The utility provides authorization data for each set-top represented in the input file and directs the output to the specified output file in "brief" format.

Notes:

- Substitute the name of the prepared input file for [input file name].
- Substitute the name of the file where you want to store the output for [output file name].
- Do not type the brackets **[ ]** in the command.

Example:

Type **tellDhctInfo -b /tmp/tellDhct-in_11.13.03 > /tmp/tellDhct-out_11.13.03** and press **Enter**.

3 Use the UNIX **more** utility to review the data in the output file.

Obtaining Authorization Data for a List of Set-Tops - Spreadsheet Format Output

1 Open an xterm window on the ISDS.

2 Type **tellDhctInfo -x [input file name] > [output file name]** and press **Enter**. The utility provides authorization data for each set-top represented in the input file and directs the output to the specified output file in "brief" format.

Notes:

- Substitute the name of the prepared input file for [input file name].
- Substitute the name of the file where you want to store the output for [output file name].
- Do not type the brackets **[ ]** in the command.

Example:

Type **tellDhctInfo -x /tmp/tellDhct-in_11.13.03 > /tmp/tellDhct-out_11.13.03** and press **Enter**.

3 You can import the output file created in step 2 into a Microsoft Excel spreadsheet.

Obtain ISDS Subscription Package and Segment Data

The information in this section describes how to use the tellDhctInfo utility to obtain a list of ISDS subscription packages, as well as the segments contained within each package.

1 Open an xterm window on the ISDS.

2 Type **tellDhctInfo -d2** and press **Enter**. The system displays a list of subscription packages and segments.

Displaying tellDhctInfo Help

1 Open an xterm window on the ISDS.

2 Type t**ellDhctInfo -? a**nd press **Enter**. The system displays the tellDhctInfo help window.

Displaying tellDhctInfo Version

1 Open an xterm window on the ISDS.

2 Type **tellDhctInfo -v** and press **Enter**. The system displays the tellDhctInfo version number.

mgrep

The UNIX grep program displays each line of text from a file that matches a specified pattern. Sometimes system operators or engineers might benefit if a few lines preceding and/or following the specified pattern are displayed, as well.

We developed the mgrep utility to accomplish this purpose.

Options

The following options are available for the mgrep utility:

- When the pattern for which you are searching consists of multiple words, quotation marks are required around the whole pattern.
- The pattern for which you are searching is case-sensitive.
- The options -M and +N represent the number of lines before and after the pattern that you want the utility to display. If you want to display 5 lines of data before the pattern and 3 lines of data after the pattern, use 5 and 3 for M and N, respectively.
- If you want to display ONLY the fifth line of data before the pattern and/or ONLY the third line of data after the pattern, append o (for only) to the M and/or the N.

  Example: To display only the fifth line of data before the pattern, and only the third line of data after the pattern, use -5o and +3o.

Using mgrep

This section contains procedures for running the mgrep utility.

1 Open an xterm window on the ISDS.

2 Type **cd [required directory]** and press **Enter**. The specified directory becomes the working directory.

  Example: Type **cd /dvs/dncs/tmp** and press **Enter**.

  Notes:

  - The mgrep utility is typically used to search log files. Log files are usually stored in the /dvs/dncs/tmp directory of the ISDS.
  - Do not type the brackets **[ ]** in the command.

3 Type **mgrep [-M[o]] [+N[o]] [-n] [pattern] [filename]** and press **Enter**.

  Example: Type **mgrep -5o +3o "MODIFY DHCT CONFIG" bossServer.017** and press **Enter**.

Note: This example searches for the pattern MODIFY DHCT CONFIG in the file named bossServer.017. In addition to displaying the lines that contain MODIFY DHCT CONFIG, the utility also displays the fifth line before and the third line after the requested pattern.

Sample mgrep Output

This example of sample output uses the following mgrep command:

mgrep -2o +4o "MODIFY DHCT CONFIG" bossServer.017

```
--------------------------------------------------
$ mgrep -2o +4o "MODIFY DHCT CONFIG" bossServer.017
   7:Mar 16 08:12:01.221 BossTransManager.C(1668):
   9-MODIFY DHCT CONFIG
  13:DhctMacAddr=00:11:E6:4F:42:7E
---
  22:Mar 16 08:12:01.236 BossTransManager.C(1668):
  24-MODIFY DHCT CONFIG
  28:DhctMacAddr=00:11:E6:4F:F7:84
```

Display mgrep Help

1. Open an xterm window on the ISDS.
2. Type **mgrep** and press **Enter**. The system displays the Help window for the mgrep utility.

del-hct-cd

The del-hct-cd utility was developed so that system operators can delete a set-top or a list of set-tops from the ISDS database.

System operators typically delete set-tops from the database when it is uneconomical to repair a set-top or if a set-top is moved from one system to another.

Using del-hct-cd

When you install the ISDS Utilities onto your system, you install a program that the system uses to purge your database of records pertaining to RMA set-tops. You can run the del-hct-cd utility in any of the following modes:

- **Information mode** - Implemented with the **-i** switch, counts and lists the set-tops found on the RMA CD and reports on their database status.

  Note: No deletions from the database occur when the del-hct-cd utility is run in Information mode.

- **Default mode** - Deletes from the Informix database those set-tops contained on the RMA CD that have a status of out-of-service in the Informix database.
- **Delete All mode** - Implemented with the **-a** switch; deletes all set-tops,

regardless of status, that are found on the RMA CD and contained in the Informix database.

Run in Information Mode First

You should run the del-hct-cd utility in Information mode first to learn how many set-tops contained on the RMA CD are listed as in-service and out-of-service in the ISDS database.

Then, based upon this information, you should decide whether to delete from the database all set-tops listed on the RMA CD, or to delete from the database only out-of-service set-tops.

Running del-hct-cd

Follow these instructions to run the del-hct-cd utility on your ISDS.

Note: See ***Process RMA Set-Tops from a File*** (on page 508) for instructions on how to run the del-hct-cd utility if an RMA CD is not available.

1. Open an xterm window on the ISDS.
2. Insert the CD containing the RMA set-top information into the CD drive of the ISDS.

   Notes:

   - Keep the CD in the CD drive of the ISDS throughout this procedure.
   - The script detects when you do not have the RMA CD in the CD drive of the ISDS and displays an error message.
   - On some systems, a File Manager window may open. You can close it.
3. In the open xterm window, type **del-hct-cd.sh -i** and press **Enter**. The script counts the set-tops found on the RMA CD and displays a message that inquires whether the database should be checked for the presence of these set-tops.
4. Type **y** (for yes) and press **Enter**. The script lists the set-tops found on the CD and displays their database status.

   Notes:

   - An RMA EMM CD may contain several hundred set-tops. To create a log file of the set-tops on the RMA CD, type **del-hct-cd.sh -i | tee hct.log** and press **Enter**.
   - The script does not delete any set-tops from the database when run in Information Mode.
   - The following list expands the acronyms used in the script:
     - IS_2W represents "in service, two-way" set-tops.
     - OOS represents "out-of-service" set-tops.
5. Continue with your normal batch install procedure. The Batch Install Progress window appears.

6 Use the Batch Install Progress window to determine whether you want to delete and install all set-tops listed on the RMA CD, or only those marked out-of-service.

7 Choose one of the following options on the Batch Install Progress window:

- To delete and re-install out-of-service RMA set-tops from the database, select **Overwrite Existing DHCTs (Out of Service only)**.
- To delete and re-install all RMA set-tops, select **Overwrite Existing DHCTs (All)**.

> **CAUTION:**
>
> **We strongly recommend that you exercise extreme caution before selecting Overwrite Existing DHCTs (All). Deleting all RMA set-tops removes from the database those set-tops that may already have been repaired and placed in subscriber's homes. These set-tops will be inoperable after you delete them from the database.**

Note: If you select No overwrites, the system loads the EMMs without deleting or overwriting existing information in the database.

8 Click **Continue**. The system deletes from the database those RMA set-tops you selected.

9 Type **exit** and press **Enter** to close the xterm window.

Process RMA Set-Tops from a File

Sites where the staging area is remotely located from the ISDS may find it difficult to supply the ISDS operator with the RMA CD so that the ISDS operator can execute the del-hct-cd utility in conjunction with RMA set-tops.

To support these sites, we have included an option in the del-hct-cd.sh script, implemented by the **-p** switch, that enables the script to read from a file rather than from the RMA CD.

Important: System operators and network administrators who currently use the -p switch when processing RMA set-tops already have a thorough understanding of the directory structure of the RMA CD because they must model the directory structure of their ISDS to reflect that of the CD. Other than a brief mention, this section provides no instructions on analyzing the directory structure of the RMA CD, nor on modeling the directory structure of the ISDS to reflect that of the CD. Any site that is interested in using the -p switch to process RMA set-tops from a file rather than from the CD should contact Cisco Services for guidance.

Guidelines for Processing RMA Set-Tops from a File

On the RMA CD, the individual set-top definition files that are used when processing RMA set-tops are stored in the …/dncs/dhcts directory. To use the -p switch, you must have a similar directory structure in place on your ISDS.

Examples:

/export/home/ftp/dncs/dhcts

/tmp/ftp/dncs/dhcts

In the examples above, you can duplicate the entire CD directory structure and contents at /export/home/ftp or /tmp/ftp on the ISDS.

Note: Even though the entire directory structure is copied to the DNCS, the del-hct-cd.sh script, when used with the -p switch, only accesses the dncs/dhcts subdirectory.

- To run the del-hct-cd utility using the -p and -a switches, type **del-hct-cd.sh -a -p/[directory path name]** and press **Enter**.

  Example: Type **del-hct-cd.sh -a -p/export/home/ftp/dncs/dhcts** and press **Enter**.

- To run the del-hct-cd utility using the -p switch to delete only out-of-service set-tops, type
  del-hct-cd.sh -p/[directory path name] and press **Enter**.

  Example: Type **del-hct-cd.sh -p/export/home/ftp/dncs/dhcts** and press **Enter**.

  Note: If you want to use the -p switch in conjunction with the del-hct-cd.sh script, call Cisco Services for assistance.

Database Backup and Restore

The Informix database contains all headend configuration information, as well as data needed to provision and authorize set-tops. In the event of a power failure, for instance, you might need to restore the database. Only through regular daily backups of your database can you ensure the integrity and persistence of your system data.

For more information and specific instructions for backing up and restoring the Informix database, refer to *Backing Up and Restoring the Informix Database* (part number 740236).

Backup Recommendations

This section provides recommendations for how often you should back up the data of your ISDS. By performing regular backups, you are assured that your valuable data will not be lost should you ever experience a failure of a major component of your ISDS system.

You can back up your data to either 4-mm data tapes or 8-mm data tapes, depending upon the type of tape drive installed in your ISDS. Use the information in this section for tape selection and tape cleaning recommendations.

System Backup Frequency

You can ensure the integrity of your data only by adhering to a regular schedule of database and file system backups.

The recommendations in this section provide some guidance regarding how often system backups should occur. Adjust these recommendations, if necessary, according to the size of the system and the frequency with which the data changes.

Full System Backup

A full system backup refers to a backup of the file systems and the database.

You should perform a complete system backup at least once a month and before making any substantial modification to the system.

In addition, you should perform a complete system backup just prior to upgrading to new system software, as well as right after the upgrade. The backup just prior to the upgrade will be used in case the system must be rolled back to the previous release in the event that the upgrade is unsuccessful.

Important: Clearly label the backup tapes and remove them from the working area so that they cannot be accidentally restored to the new release. New and old backups are not compatible.

File System Backup

You should perform a complete backup of the ISDS and Application Server file systems once a week.

Important: You can back up the file system of the ISDS without first shutting down the system components. However, our engineers highly recommend that you schedule your file system backups for periods of lowest system activity.

Informix Database Backup

The Informix database contains all headend configuration information, as well as data needed to provision and authorize Digital Home Communication Terminals (DHCTs).

You should perform a complete backup of the Informix database once a day. In addition, You should perform a complete backup of the database immediately before and after a channel lineup change or a major system configuration change.

Consider the following recommendations when you backup your database.

- We strongly recommend that you backup your database once each day, preferably early in the morning or late at night, when system activity is usually at a minimum.
- Avoid backing up your database while you are performing any of the following system tasks:
  - Running the Interactive Program Guide (IPG) Collector
  - Loading an Entitlement Management Message (EMM) DVD
  - Staging Set-Tops
- To back up the Informix database, you must have a tape drive connected to or included in your system. Some platforms contain internal tape drives; others must use external tape drives.
- You do not have to shut down the ISDS or the Download Server to back up your Informix database. All system components can be running while you back up the database.
- It can take up to 30 minutes to back up a typical database with approximately 100,000 set-tops. Larger systems may take longer.

Key Files Backup

The key files need to be backed up only as part of a system upgrade.

Restore Recommendations

You need the tapes from your most recent database backup in order to restore the Informix database.

Tape Considerations

Consider the following recommendations concerning your tape drives and the tapes that you use for the database backup.

- Use seven tapes (or sets of tapes) for the database backup, one for each day of the week.

  Important: The tapes that you use to back up your Informix database wear out over time. Be sure to replace your tapes at least once a year.

- You can back up your Informix database to either a 4-mm or an 8-mm data tape. The type of tape you choose depends upon the type of tape drive installed on your ISDS. An 8-mm tape is too big for a 4-mm tape drive; a 4-mm tape is too small for an 8-mm tape drive. Ask the person who handles your account if you are not sure which type of tape is appropriate for your system.

- You can purchase 4-mm tapes or 8-mm tapes in various lengths. While all tapes wear out over time, a longer tape is likely to wear out quicker than a shorter tape because the strength of a tape is inversely proportional to the length of the tape. Use the following guidelines when you purchase tapes to back up your Informix database:

  - 4-mm tapes: Do not exceed 150 meters
  - 8-mm tapes: Do not exceed 160 meters

- Depending on the size of your database, you may need more than one tape to do a complete backup. If you need more than one tape to back up your database, the backup script will prompt you to remove the existing tape and to insert a new tape at the appropriate time.

- The script used by the ISDS to back up the Informix database uses the following default tape drive configuration:

  - Tape size: 5859375 KB
  - Block size: 16
  - Device name: /dev/rmt/0h

- This tape drive configuration is in use on a majority of systems. Occasionally, the tape drive on a system may be configured with a different device name, such as /dev/rmt/1h.

  Note: The 'h' that appears at the end of device name /dev/rmt/0h or /dev/rmt/1h indicates that the system is to use a high density format when writing to the tape.

Cleaning Your Tape Drive

Under normal conditions, most tape and tape drive manufacturers recommend that you clean your tape drive after about 30 hours of use. Use only a cleaning cartridge and kit designed for use with your tape drive. Discard your cleaning cartridge after using it for the number of cleaning cycles specified in the cleaning kit documentation.

Backing Up and Restoring the Informix Database

The Informix database contains all headend configuration information, as well as data needed to provision and authorize DHCTs. We recommend that you back up your Informix database once a day.

Some large systems require more than one tape when backing up the database. The backup script prompts you to insert another tape at the appropriate time if your backup requires an additional tape.

Use seven tapes (or seven sets of tapes), one for each day of the week, when you back up your database.

Note: You do not have to shut down the ISDS in order to back up your Informix database. All system components can be running while you back up the database.

Tape Drive Configuration

Use this procedure if you need to determine the device name of the tape drive used by your system.

Notes:

- You will only have to complete this procedure once. The device name of your tape drive will not change unless you specifically change the tape drive configuration.
- Do not have a tape in the tape drive when you complete this procedure.

1. Open an xterm window as root user.
2. Make sure that no tape is currently in your tape drive.
3. Type the following UNIX routine.

   Important: Type the routine just as shown by pressing **Enter** at the end of each line.

   ```
   for drive in 0 1 2 3 4 5 6 7
   do
   mt  -f  /dev/rmt/$drive status
   done
   ```

   Result: The system checks the status of eight (0-7) possible tape drive configurations and displays the results.

4 Examine the results and use the following observations to determine the device name of your tape drive.
   - If no tape drives are detected in /dev/rmt/0 through /dev/rmt/7, the results show No such file or directory. Therefore, you can conclude that the system did not detect any tape drives. You should investigate why a tape drive was not detected.
   - If a tape drive is detected in /dev/rmt/0, for example, the system should accurately note that no tape is loaded in /dev/rmt/0. Therefore, you can conclude that the device name of the tape drive on the system queried in step 3 is /dev/rmt/0.
   - If /dev/rmt/1 is the device name of your tape drive, then no tape loaded or drive offline would appear next to /dev/rmt/1.
5 Record the device name of your tape drive.

   Note: You might need to refer to this device name when you back up or restore the database.
6 Type **exit** and press **Enter** to close the xterm window.

Database Backup Script Options

The script that backs up the file system is called **backupDatabase**. You can run the backupDatabase script with the following options:

- *-b* — block size. Specifies the blocksize that should be used, in Kilobytes.
- *-l* — Local-tape-drive. Specifies tape drive to use on local host computer. (for example — /dev/rmt/0h)
- *-v* — verbose. Verbose output.
- *-s* — tape size. Specifies the tape size that should be used, in Kilobytes.
- *-t* — tape label. Backup tape label. This must be a unique string with no spaces.
- *-h* — help. Provides a brief description of the valid options.

Back Up the Database

In this procedure, you will back up the Informix database. The system release DVD should still be in the DVD drive of the ISDS.

Use this procedure to back up the ISDS database.

Notes:

- The ISDS can be running while you back up the Informix database.
- It may take up to 30 minutes to back up a typical database with approximately 100,000 set-top boxes.

1 If necessary, open an xterm window on the ISDS.
2 Complete the following steps to log on to the xterm window as **root** user.

a Type **su -** and press **Enter**. The password prompt appears.

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

3 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.

4 After waiting at least 1 minute, did **/cdrom/cdrom** appear in the output of the command executed in step 3?

- If **yes**, go to step 5.
- If **no**, follow these instructions.
  - a Type **/etc/init.d/volmgt stop** and then press **Enter**.
  - b Type **/etc/init.d/volmgt start** and then press **Enter**.
  - c Repeat step 3.

5 Label your backup tape with the following information:

ISDS Database Backup [Day of the Week]

[Site Name]

[Software Version]

System Release DVD x.x.x

[Tape #]

Notes:

- Customize the label with the day of the week, site name, and software version for the site you are backing up.
- If your database backup requires more than one tape, be sure to note the tape number on the label.

6 Insert the tape into the tape drive of the ISDS and wait until the green light stops flashing.

7 Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

Important: Be sure to type the dot, followed by a space, prior to typing /dvs.

8 Choose one of the following options.

- If you are using the standard tape drive configuration, follow these instructions.
  - a Type **/cdrom/cdrom0/s3/backup_restore/backupDatabase** and then press **Enter**. The system displays the following message:

    Please mount tape 1 on /dev/rmt/0h and then press Return to continue.
  - b Go to step 10.
- If you are using a custom tape drive configuration, go to step 9.

9 If you are using a custom tape drive configuration, type

/cdrom/cdrom0/s3/backup_restore/backupDatabase -b [blocksize] -s [tapesize] and then press **Enter**.

Note: Substitute the blocksize and tapesize that pertain to your system for [blocksize] and [tapesize].

Example:

/cdrom/cdrom0/s3/backup_restore/backupDatabase -b 128 -s 13212058

Result: The system displays the following message:

Please mount tape 1 on /dev/rmt/0h and then press Return to continue.

10 Press **Enter**. The system backs up your Informix database.

Notes:

- The system will prompt you to insert additional tapes if your backup requires more than one tape.
- The message **Successfully completed the database backup** appears when the backup has completed successfully.
- If the database backup was not successful, the system displays an error message. Call Cisco Services at 1-866-787-3866 for assistance in resolving the error message.

11 Type **eject cdrom** and then press **Enter**.

12 Remove the DVD and tape(s) and store them in a safe place.

13 Type **exit** and then press **Enter** to log out the root user.

Restore the Database

This section contains procedures for restoring the database from your backup tapes.

How Many Tapes Are in the Backup?

You may have used more than one backup tape when you backed up the Informix database. Refer to one of the following procedures based on whether you used more than one backup tape:

- If you used *only* one tape to back up the Informix database, refer to the ***Restoring the Informix Database Using One Backup Tape*** (on page 516) procedure to restore the database.
- If you used *more than one* tape to back up the Informix database, refer to the ***Restoring the Informix Database Using More Than One Backup Tape*** (on page 518) procedure to restore the database.

Restoring the Informix Database Using One Backup Tape

Complete the following steps to restore the ISDS and ISDP databases using only one backup tape.

Note: You need the tape from your most recent database backup in order to restore the Informix database.

Important:

- The ISDS and Application Server must be stopped before you restore the database.
- Be sure your tape is write-protected before you use it to restore the database.

1. If necessary, open an xterm window on the ISDS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Have you just restored the ISDS file system?
   - If **yes**, go to step 4.
   - If **no**, go to step 5.
4. Complete the following steps. (You have just restored the ISDS file system.)
   a. Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

      Important: Be sure to type the dot, followed by a space, prior to typing /dvs.
   b. Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**. The system formats the database partitions.
5. Insert the system release DVD into the DVD drive of the ISDS.
6. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the DVD.
7. Insert your most recent copy of the ISDS database backup tape into the tape drive of the ISDS and wait for the green light on the tape drive to stop flashing.
8. Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v** and then press **Enter**.
9. When the **Is there more than 1 tape in this backup? [Y/N]** message appears, type **n** and then press **Enter**. The system displays a message about ensuring that the backup tape is in the drive.
10. Press **Enter**. The system restores the database.
11. When the **Successfully restored the database** message appears, remove the tape and store it in a safe place.
12. Complete the following steps to eject the DVD.
    a. Type **cd /** and then press **Enter**.
    b. Type **/etc/init.d/informix stop** and then press **Enter**. The system stops the Informix oninit processes.
    c. Type **eject cdrom** and then press **Enter**.
    d. Type **/etc/init.d/informix start** and then press **Enter**. The system restarts the Informix oninit processes.
13. Remove the DVD and store it in a safe place.

14 Type **exit** and then press **Enter** to log out the root user. You can now restart the ISDS and Application Server.

Restoring the Informix Database Using More Than One Backup Tape

Complete the following steps to restore the ISDS and ISDP databases using more than one backup tape.

Note: You need the tapes from your most recent database backup in order to restore the Informix database.

Important:

- The ISDS and Application Server must be stopped before you restore the database.
- Be sure your tapes are write-protected before you use them to restore the database.

1 If necessary, open an xterm window on the ISDS.

2 Complete the following steps to log on to the xterm window as **root** user.

   a Type **su -** and press **Enter**. The password prompt appears.

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

3 Have you just restored the ISDS file system?

   - If **yes**, go to step 4.
   - If **no**, go to step 5.

4 Complete the following steps. (You have just restored the ISDS file system.)

   a Type **. /dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

   Important: Be sure to type the dot, followed by a space, prior to typing /dvs.

   b Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**. The system formats the database partitions.

5 Insert the system release DVD into the DVD drive of the ISDS.

6 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

   Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the DVD.

7 Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v** and then press **Enter**.

8 When the **Is there more than 1 tape in this backup? [Y/N]** message appears, type **y** and then press **Enter**. The system displays a message about ensuring that the last backup tape is in the tape drive**.**

   Note: You are instructed to load the last tape because a configuration file is appended to the final tape in the backup series during the backup procedure.

9 Insert the last tape from your most recent database backup and press **Enter**.

   Results:

- The system examines the configuration file.
- The system displays a message similar to the following:
  Please mount tape 1 on [device name] and press Return to continue.

10 Remove the tape that is currently in the tape drive.

11 Insert the first tape from your most recent database backup and press **Enter**.

Results:

- The system displays archive information from the tape.
- The message **Continue restore? (y/n)** appears.

12 Type **y** and then press **Enter**. The **Do you want to back up the logs? (y/n)** message appears.

13 Type **n** and then press **Enter**.

Results:

- The system begins restoring the database.
- The **Please mount tape 2 on [device name] and press Return to continue** message appears after several minutes.

14 Remove the first tape and insert the second tape from your most recent database backup and then press **Enter**.

Results:

- The restoration of the database continues.
- If there is another tape in the backup series, the system will prompt you to insert the next tape.

15 Repeat step 14 for as many backup tapes that are in the backup series.

16 When the **Restore a level 1 archive? (y/n)** message appears, type **n** and then press **Enter**.

17 When the **Do you want to restore log tapes? (y/n)** message appears, type **n** and then press **Enter**.

18 When the **DNCS Informix partition restore completed and verified** message appears, remove the final tape and store it in a safe place.

19 Complete the following steps to eject the DVD.

a Type **cd /** and then press **Enter**.

b Type **/etc/init.d/informix stop** and then press **Enter**. The system stops the Informix oninit processes.

c Type **eject cdrom** and then press **Enter**.

d Type **/etc/init.d/informix start** and then press **Enter**. The system restarts the Informix oninit processes.

20 Remove the DVD and store it in a safe place.

21 Type **exit** and then press **Enter** to log out the root user. You can now restart the ISDS and Application Server.

Backing Up and Restoring the ISDS

Use the procedures in this section to back up and restore the file system and key files of the ISDS.

Important: You can back up the file system of the ISDS without first shutting down the system components. However, we highly recommend that you schedule your file system backups for periods of lowest system activity.

Back Up the File Systems

The upgrade scripts do not back up the ISDS file systems. Prior to beginning the upgrade, back up the file systems manually. The following procedures provide instructions on backing up the file systems of the ISDS.

Note: The file system backup may require more than one tape.

Failure of File System Backups and the Real-Time, Class Process

Occasionally, the file system backup may fail. If the backup fails, you should check whether there are any real-time, class processes that are running. Current file system backup scripts can handle only the ntpd process that is running as a real-time class process.

Note: The ntpd process is an operating system daemon that sets and maintains system time in synchronization with Internet standard time servers.

If the file system backup fails, system operators should complete the following steps to see if any real-time, class processes are running.

1. From an xterm window, type **ps -efc | grep RT** and then press **Enter**. The system reports whether any real-time, class processes are running on that device.
2. Are any real-time, class processes running (other than the ntpd process)?
   - If **yes** (and the file system backup still failed), call Cisco Services for assistance.
   - If **no**, re-run the procedures to back up the file system. If the backup still fails, call Cisco Services.

Filesystem Backup Script Options

The script that backs up the file system is called **backupFileSystems**. You can run the backupFileSystems script with the following options:

- *-l* — Local-tape-drive. Specifies tape drive to use on local host computer. (for example — /dev/rmt/0h)
- *-v* — verbose. Verbose output.
- *-t* — tape label. Backup tape label. This must be a unique string with no spaces.
- *-h* — help. Provides a brief description of the valid options.

Preparing for the File System Backup

Follow this procedure to prepare for the ISDS file system backup.

1. If necessary, open an xterm window on the ISDS.
2. Complete the following steps to log on to the xterm window as **root** user.
   a. Type **su -** and press **Enter**. The password prompt appears.
   b. Type the root password and press **Enter**.
3. Insert the system release DVD into the DVD drive of the ISDS.
4. Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.
5. After waiting at least 1 minute, did **/cdrom** appear in the output of the command executed in step 4?
   - If **yes**, go to step 6.
   - If **no**, follow these instructions to stop and restart the vold process, which manages the auto-mount functions for the DVD drive.
     a. Type **/etc/init.d/volmgt stop** and then press **Enter**.
     b. Type **/etc/init.d/volmgt start** and then press **Enter**.
     c. Repeat step 4.
6. Label a blank tape with the following information:

   ISDS File System Backup [Date]

   [Site Name]

   [Software Version]

   System Release x.x.x DVD

   Notes:

   - Customize the date, site name, and software version for the site you are backing up.
   - The file system backup may require more than one tape.

Backing Up the File System of the ISDS

Follow these instructions to back up the file system of the ISDS.

Notes:

- If you have correctly followed the directions in this chapter, you should be logged in to an xterm window as root user.
- Expect to spend about an hour backing up the ISDS.

1. Insert the blank tape into the tape drive of the ISDS and wait for the green light to stop flashing.

2 Type **./dvs/dncs/bin/dncsSetup** and then press **Enter**. The system establishes the root user environment.

3 Type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems** and then press **Enter**.

Result:

- The system backs up the ISDS file system.
- If the backup requires more than one tape, the system will prompt for the next tape. Insert a new tape and continue the backup.

  Note: If more than one tape is required, be sure to include the tape number on the label. Label the first tape generated by the backup with the number 1.
- The system displays a message when the backup is complete.

4 When the backup is complete, remove the tape and store in a safe place.

5 Type **exit** and then press **Enter** to log out the root user.

Back Up the Key Files

This section contains information on preparing for and executing a backup of the key files of your ISDS.

Preparing for the Key Files Backup

Complete the following steps to prepare to back up the key files.

1 If necessary, open an xterm window on the ISDS.

2 Complete the following steps to log on to the xterm window as **root** user.

   a Type **su -** and press **Enter**. The password prompt appears.

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

3 Insert the system release DVD into the DVD drive of the ISDS.

4 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of **/cdrom** in the output confirms that the system correctly mounted the DVD.

5 Label a blank tape with the following information:

[ISDS] Key Files Backup [Date]
[Site Name]
[Software Version]
System Release DVD x.x..x

Note: Customize the date, site name, and software version for the site you are backing up.

Using the tar Utility

If you need to back up the key files from a remote computer, you can use the tar utility to create a tape archive instead of using the backupFileSystems script.

Key Files Backup Script Options

The script that backs up the key files is called **backupKeyFiles.** You can run the backupKeyFiles script with the following options:

- *-I*—Key_files_include. Specifies the file that lists all the files that need to be included in the backup
- *-E*—Key_files_exclude. Specifies the file that lists all the files that need to be excluded from the backup
- *-l*—Local-tape-drive. Specifies tape drive to use on local host computer (for example – /dev/rmt/0h)
- *-B*—Backup_Directory. Specifies the backup directory to which the key files should be saved (in tar format)

  Important: The system creates a file named KeyFiles.tar in the specified directory. If you wish to back up ISDS key files at the same time, be sure to specify different directories for each set of key files, or the backups will overwrite each other.
- *-v*—verbose. Verbose output
- *-A*—Alternate Root Directory. Specify the Alternate Root Directory where the key files should be restored. This is useful during a Live Upgrade (System Release DVD upgrades) when you may want to back up key files from one root directory and restore them to another root directory. The Alternate Root Directory must contain the /usr/sbin/tar directory, or the backup script will fail to execute correctly.
- *-h*—help. Provides a brief description of the valid options.

Notes:

- The *–I* and *–E* options are independent of one another; any one of them may be used. If neither the *–I* or *–E* option is specified, then the default Keyfiles.include or Keyfiles.exclude files, which exist in the current directory, are used.
- If either the *–I* or *–E* option is included, the absolute path must be specified.
- The *–l* and *–r* options are mutually exclusive of one another; only one of them can be used.
- The *–B* option cannot be used if either the *–l* or *–r* option is used.
- The backupKeyFiles script currently does not support the *–E* option.

Backing Up the Key Files

Complete the following steps to back up the key files.

Note: You should be logged in to an xterm window as root user.

1. Insert the blank tape into the tape drive of the server you are backing up, and wait for the green light to stop flashing.
2. Type **/cdrom/cdrom0/s3/backup_restore/backupKeyFiles -v** and then press **Enter**. The system backs up the ISDS, Download Server, or LIONN key files and displays a message when the backup is complete.
3. When the backup is complete, eject the tape and store it in a safe place.
4. Type **eject cdrom** and then press **Enter**.
5. Remove the DVD and store it in a safe place.

Restore the File System

This section contains procedures for restoring a previously backed up system.

Preparing to Restore the File System

Complete the following steps to prepare to restore the file system.

Important: You need to know the IP address and the netmask of the ISDS in order to complete this procedure.

1. Open an xterm window on the ISDS.
2. Complete the following steps to log on to the xterm window as **root** user.
   - **a** Type **su -** and press **Enter**. The password prompt appears.
   - **b** Type the root password and press **Enter**.
3. Insert the system release DVD into the DVD drive of the ISDS.
4. Type **shutdown -y -g0 -i0** and then press **Enter** on the ISDS. The system halts all processes on the ISDS, and an **ok** prompt appears.
5. At the ok prompt on the server into which you have inserted the DVD, type **boot cdrom - SAshell** and then press **Enter**. The system boots into the OpenWindows environment.

   Notes:

   - When the system boots into the OpenWindows environment, it searches its non-volatile RAM for configuration information.
   - If the system is unable to locate its configuration information (a rare occurrence), it prompts you for the information it needs through the Solaris Installation menu.
6. In the process of booting, did the Solaris Installation menu appear?
   - If **yes**, go to step 7.
   - If **no** (the system successfully found the configuration information it needed), go to step 8.
7. Complete the following steps on the Solaris Installation menu.
   - **a** At the Solaris Installation menu, select **Continue**.
   - **b** At the Identify This System menu, select **Continue**.

c At the Hostname menu, type the hostname of the ISDS and then select **Continue**.

d At the IP Address menu, type the IP address of the ISDS and then select **Continue**.

e At the Subnets menu, select **Yes** at the System part of subnet question and then select **Continue**.

f At the Netmask menu, type the netmask of the ISDS and then select **Continue** (or just select Continue to accept the default value of 255.255.255.0).

g At the IPv6 menu, choose **No** and then select **Continue**. The Confirm Information window opens that allows you to review all of the configuration information you have just submitted.

h Review the data on the Confirm Information window and correct anything that needs to be changed; then, select **Continue**.

i At the Name Service window, select **None** and then select **Continue**. The Confirm Information window reappears.

j Review the data on the Confirm Information window and correct anything that needs to be changed; then select **Continue**. An xterm window opens.

8 Insert your most recent file system backup tape into the tape drive of the server you are restoring.

9 Type **cd /tmp/cdrom/backup_restore** and then press **Enter**. The /tmp/cdrom/backup_restore directory becomes the working directory.

Prerequisite

You need the tape(s) from your most recent backup of the file system before restoring the file system.

Important: Be sure your tape(s) are write-protected before you use them to restore the system.

Shutdown ISDS Processes

To restore the key files, you must shut down the ISDS processes. See ***Stop ISDS Processes*** (on page 351) for procedures on how to stop the system components and servers.

File System Restore Script Options

The script that restores the ISDS file systems is called **restoreFileSystems**. You can run the restoreFileSystems script with the following options:

- *-l* — Local-tape-drive. Specifies tape drive to use on local host computer (for example -- /dev/rmt/0h)
- *-B* – Backup directory. Specifies the directory that contains the backup from which the file system will be restored. The backup directory must be on an NFS-

mounted filesystem.

- *-v*—verbose. Verbose output
- *-i*—interactive. Runs the restoration script in interactive mode
- *-h*—help. Provides a brief description of the valid options

Note: The *–l*, *–r*, and *-B* options are mutually exclusive of one another; only one of them can be used.

Using the tar Utility

To restore the key files from a remote computer, you can use the tar utility to extract the tape archive instead of using the restoreFileSystems script.

Restoring the File System

Complete the following steps to restore the file system of the ISDS.

1. If necessary, open an xterm window on the ISDS and log in as root user.
2. Type **./restoreFileSystems -v** and then press **Enter**.

   Result:

   - The system restores the ISDS file system.
   - If the backup required more than one tape, the system prompts for the next tape. Insert the next tape and continue the restoration.
   - The system displays a message when the restoration is complete.
3. When the restoration is complete, remove the tape and store it in a safe place.
4. Is the server a SUN T5440?

   - If **yes**, you need to restore the output and input devices. Go to step 5.
   - If **no**, go to step 7.
5. Type **eeprom output-device=screen** and press **Enter**. The output device is set to virtual console.
6. Type **eeprom input-device=keyboard** and press **Enter**. The input device is set to virtual console.

   Note: The monitor and keyboard will be used as the output and input devices after the next reboot.
7. Type **/usr/sbin/shutdown -y -i0 -i6** and then press **Enter**. The ISDS reboots and the Common Desktop Environment (CDE) login window appears.

   Note: The system may reboot a few times as part of the restoration process.
8. Log on to the CDE as **root** user.
9. Follow the ***Restore the Database*** **(on page 516)** procedures to restore the Informix database. After restoring the Informix database, go to step 7 to enable disk mirroring.
10. Type **/cdrom/cdrom0/s3/backup_restore/mirrState -a** and then press **Enter**.

Note: The latest System Release DVD should still be in the drive of the ISDS and you should still be logged in as root user to an xterm window.

The system displays the following message:

WARNING!
Proceeding beyond this point will ATTACH all Controller 2 submirrors.
Are you certain you want to proceed?

11 Type **y** and then press **Enter**. The system enables the disk mirroring functions on the ISDS.

Note: Depending upon your system configuration, it may take up to an hour for all of the data to become mirrored.

12 Type **eject cdrom** and then press **Enter**. The system ejects the DVD.

13 Click the right mouse button on the server you restored and select **Log Out**. The root user logs off and the CDE window returns.

14 Log on to the CDE window as **dncs** user.

Restore the Key Files

This section contains procedures for restoring previously backed up key files.

Prerequisite

You need the tape from your most recent backup of the key files before restoring the key files.

Important: Be sure your tapes are write-protected before you use them to restore the key files.

Key Files Restore Script Options

The script that restores the key files is called **restoreKeyFiles**. You can run the restoreKeyFiles script with the following options:

- *-l*—Local-tape-drive. Specifies tape drive to use on local host computer (e.g. -- /dev/rmt/0h)
- *-v*—verbose. Verbose output
- *-h*—help. Provides a brief description of the valid options

Note: The *–l* and *–r* options are mutually exclusive of one another; only one of them can be used.

Preparing to Restore the Key Files

Complete the following steps to prepare to restore the key files.

1 If necessary, open an xterm window on the ISDS.

2 Complete the following steps to log on to the xterm window as **root** user.

a Type **su -** and press **Enter**. The password prompt appears.

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

3 Insert the latest System Release DVD into the DVD drive of the ISDS.

4 Type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.

5 Insert your most recent key files backup tape into the tape drive of the ISDS, and wait for the green light to stop flashing. Go to ***Restoring the Key Files on the ISDS*** (on page 528).

Restoring the Key Files on the ISDS

Complete the following steps to restore the key files of the ISDS.

1 If necessary, open an xterm window on the ISDS and log in as **root** user.

2 Type **/cdrom/cdrom0/s3/backup_restore/restoreKeyFiles -v** and then press **Enter**. The system restores the key files and displays a message when the restoration is complete.

3 When the restoration is complete, eject the tape and store it in a safe place.

4 Type **eject cdrom** and then press **Enter**.

5 Remove the DVD and store it in a safe place.

6 On the ISDS, type **/usr/sbin/shutdown -y -g0 -i6** and then press **Enter**. The ISDS reboots.

7 Log on to the CDE of the ISDS as a **dncs** administrator.

Power Failure Recovery

If the ISDS fails due to a power failure (or for any other reason), follow these steps to ensure a graceful return to service.

1. Check the database logs for errors. For more information, see ***Check the Database Log for Errors*** (on page 529).
2. Does the database log contain errors?
   - If **yes**, locate your latest database backup tapes and contact Cisco Services.
   - If **no**, restart the ISDS and recheck the log to see if other problems are indicated.
3. Are other problems indicated by the database log?
   - If **yes**, locate your latest database backup tapes and contact Cisco Services.
   - If **no**, your database should work correctly.

Check the Database Log for Errors

Solaris panics are logged in the /var/adm/messages file, and Informix assertion failures are logged in the export/home/informix/online.log. To determine whether you should contact Cisco Services, look for messages in the /export/home/informix/online.log stating that Informix performed work during recovery.

Example: Defragmentation not necessary

The following example indicates that your tables do not need to be defragmented. Messages indicate that no work was needed or performed during the recovery. This example shows what you will see upon startup after a graceful shutdown.

```
15:16:36  Physical Recovery Started.

15:16:36  Physical Recovery Complete: 0 Pages Restored.

15:16:36  Logical Recovery Started.

15:16:36  20 recovery worker threads will be started.

15:16:39  Logical Recovery Complete.

          0 Committed, 0 Rolled Back, 0 Open, 0 Bad Locks
```

In this case, you should restart the system and verify that there are no other problems, then check the log files once again for errors. If errors are indicated, contact Cisco Services.

Example: Defragmentation is necessary

The following example indicates that you should contact Cisco Services. Messages indicate that 1776 pages were restored, 2995 records were committed, and 14 records were rolled back. This example shows what you will see upon startup after an uncontrolled shutdown.

```
12:09:11  Physical Recovery Started.

12:09:12  Physical Recovery Complete: 1776 Pages Restored.

12:09:12  Logical Recovery Started.

12:09:12  20 recovery worker threads will be started.

12:09:17  Logical Recovery Complete.

          2995 Committed, 14 Rolled Back, 0 Open, 0 Bad Locks
```

In cases like this, you should retrieve the latest copy of your database backup tapes and contact Cisco Services to defragment your tables and rebuild your indexes.

25

Troubleshooting

Introduction

This section contains information on troubleshooting your ISDS, RNCS, and online help. It also contains information on logging for troubleshooting.

In This Chapter

ISDS Troubleshooting

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, see ***ISDS Utilities*** (on page 396) or refer to *DBDS Utilities Version 6.3 Installation Instructions and User Guide* (part number 4031374).

ISDS Process Not Running

After the ISDS is up and running, all of the ISDS processes should have a green working state on the ISDS 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 Cisco Services.

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 Cisco Services.
5. Try to restart the process as follows:
   a. In the ISDS Control window, click once on the process name.
   b. Click **Process > Start Process**.
6. Did the process change to a green working state after a few moments?
   - If **yes**, the process is now running. No further action is necessary.
   - If **no**, contact Cisco Services.

Related Topics

- ***Troubleshoot with Dashboard Indicators*** (on page 344)

Troubleshoot with DashBoard Indicators

Quick Path: ISDS Administrative Console Status > DashBoard area > Launch > Troubleshoot

This section provides troubleshooting assistance for DashBoard indicators that are outside of their target ranges.

DNCS Idle CPU %

When this indicator shows 20% or less for a 15-minute period or more, take the following actions. Otherwise, the system is operating as expected.

Possible Causes	Check and Correct
■ A runaway process or processes ■ Too many processes are running ■ Insufficient CPU resources	Display the DashBoard indicator for **DNCS Process CPU** % and determine the status of this indicator: ■ If the DNCS Process CPU % is less than 50% over a 15-minute period, the system is functioning within normal operating levels and does not require further troubleshooting. ■ If the DNCS Process CPU % is more than 50% consistently over a 15-minute period, use the **prstat** command to identify the ISDS processes that contribute to the high utilization. Then check the ***DNCS Database Process CPU %*** (on page 345). **Note:** Refer to the man page for usage and options for this command.

DNCS Database Process CPU %

When this indicator shows 30% or greater consistently over a 15-minute period or more, contact Cisco Services. In other instances, use the following table to troubleshoot.

Possible Causes	Check and Correct
■ A runaway process or processes ■ Too many processes are running ■ Insufficient CPU resources	Use the **prstat** command to identify the ISDS processes that contribute to the high utilization. **Note:** Refer to the man page for usage and options for this command.

DNCS Process CPU %

When this indicator shows 50% or greater for a 15-minute period or more, take the following actions. If they do not resolve the memory issue, contact Cisco Services.

Possible Causes	Check and Correct
■ A runaway process or processes ■ Too many processes are running ■ Insufficient CPU resources	Use the **prstat** command to identify the ISDS processes that contribute to the high utilization. **Note:** Refer to the man page for usage and options for this command.

Free Memory %

When this indicator shows an upward trend over a period of several days, take the following actions.

Possible Causes	Check and Correct
■ Memory leaking	**1** Use the **prstat** command to identify the process or processes that contribute to the trend by manually recording the data over several days. **Note:** Refer to the man page for usage and options for this command. **2** Check the absolute memory size of the processes. If any single process is using more than 250 Mbyte of memory, contact Cisco Services for assistance.

RNCS Troubleshooting

Even with regular maintenance, you may encounter problems with your RCS. If problems do occur, the following tasks can help you troubleshoot your RCS.

- ***Adjust Logging Levels of a Process*** (on page 546)
- ***Adjust Logging Levels of Libraries*** (on page 546)
- ***ISDS Troubleshooting*** (on page 532)

PCG Troubleshooting

If the PCG device ever becomes corrupted or otherwise inoperable, you must reinstall both the PCG operating system and the PCG software, in that order. See ***PCG*** (on page 46) for more information.

Reports Troubleshooting

This section describes the most common situations that may cause errors with the Report Writer software and provides troubleshooting guidelines and possible solutions. Refer to the following table to review symptoms and possible remedies.

Symptom	Possible Solutions
Cannot find the error files	■ ***Determining if Error Files Exist*** (on page 538) ■ ***Error Files*** (on page 538)
Cannot find the web browser toolbar	■ ***Displaying the Web Browser Toolbar*** (on page 539)
Cannot access Report Writer	■ ***Report Writer Not Installed Properly*** (on page 539) ■ ***Web Server Not Running*** (on page 539) ■ ***Cannot Access Report Writer URL*** (see "***Cannot Access the Report Writer URL***" on page 540)
No data in report	■ ***No Data or Old Data in the Report*** (on page 540) ■ ***Web Browser Unable to Display Data*** (on page 541)
Old data in report	■ ***No Data or Old Data in the Report*** (on page 540)
Browser displays runtime errors when you try to generate a report	■ ***Runtime Errors*** (on page 541)
Web browser does not display data	■ ***No Data or Old Data in the Report*** (on page 540) ■ ***Web Browser Unable to Display Data*** (on page 541)
SNMP Poll reports do not regenerate data	■ ***SNMP Poll Reports Do Not Regenerate Data*** (on page 542)

General Reports Troubleshooting

If errors occur while Report Writer is generating a report, those errors are logged into one or more files, depending on the report type. By examining the contents of these files, it may be possible to determine why Report Writer is not providing the results you expect.

The ISDS creates one or more of the following files if errors occur while ISDS is generating a report. Examine the contents of these files to determine why ISDS is not providing the results you expect.

Report	File
All Reports	/tmp/PPVEvents.err
	/tmp/ZeroCredit.err
	/tmp/CableCard.err
	/tmp/CSSReport.err
	/tmp/Converters.err
	/tmp/DhctPkg.err
	/tmp/DNCSPkg.err
	/tmp/Qams.err
	/tmp/NetCrypt.err
	/tmp/Pcg.err
	/tmp/SDVServers.err
	/tmp/QPSKMods.err
	/tmp/QPSKDemods.err
	/tmp/InServOneWay.err
	/tmp/NRNeverConn.err
	/tmp/NRLostConn.err
	/tmp/SvcGroup.err
	/tmp/DhctsignOnFailed.err
	tmp/PcgSession.err
SNMP Poll Reports	/tmp/NRSNMPPoll.err
	/tmp/ResAppVersion.err
	/tmp/FreeMem.err
	/tmp/Uptime.err
	/tmp/asnmp.err
	/tmp/getdhcts.err

Determining if Error Files Exist

When you successfully generate a report, the files listed in the Error Files table are either non-existent or exist but have been cleared (zero content).

1. To determine if an error file exists, log in to the ISDS server and enter the password.
2. Type **cd /tmp** and press **Enter**.

3 Type **ls -l *.err** and press **Enter**.

Note: The "l" in **-l** is a lowercase letter L.

4 Type **cat [filename].err** and press **Enter**. The [filename] represents one of the error file names listed in ***Error Files*** (on page 538). If the file contains errors, its contents will appear on the screen.

Displaying the Web Browser Toolbar

If the web browser Navigation Toolbar is not displayed (Back, Forward, etc.), click **View > Toolbars > Navigation Toolbar**. The Navigation Toolbar appears.

Report Writer Not Installed Properly

If Report Writer is not functioning as expected, verify that the Report Writer software is installed on the ISDS server and that the installation status is "completely installed."

1 Log in to the ISDS as **dncs** user.

2 Open an xterm window on the ISDS.

3 Type **pkginfo -l SAIrptwrt** and press **Enter.** The Report Writer installation status and version number appear on the screen:

```
STATUS: completely installed
VERSION: [product version]
```

4 Does the STATUS field indicate completely installed?

- If **yes**, the Report Writer software installation is complete.
- If **no**, you must uninstall then reinstall the Report Writer software. Refer to *Report Writer Version 4.3 for DNCS and ISDS User Guide* (part number 4021181) for these procedures.

Web Server Not Running

To run ISDS, the Apache HTTP Server must be running on the ISDS server.

1 Log in to the ISDS server as **root.**

2 Type **ps -ef | grep httpd** and press **Enter.**

3 Does the information on your screen look similar to the following example:
root 458 1 0 08:36:10 ? 0:00 ./httpd

- If **yes**, the Apache HTTP Server is running.
- If **no**, type **/etc/rc2.d/S99http** and press **Enter** to start the Apache HTTP Server.

Cannot Access the Report Writer URL

If you are unable to access the ISDS website from your browser, verify that you are typing the correct URL.

1. From the ISDS Admin window select the **ISDS** tab.
2. From the **Utilities** tab, click **Reports.**
3. Select **Report Manager**. A prompt for the user ID and password appears on the screen.
4. Does the Prompt window open?
   - If **yes**, your browser successfully accessed Report Writer.
   - If **no**, type **http://[ip_address]:8045** and press **Enter**. In this command, [ip_address] represents the ISDS server IP address.
5. Did you successfully access the website?
   - If **yes**, click **Report Manager**.
   - If **no**, repeat this procedure.
6. Does the Prompt window open?
   - If **yes**, your browser successfully accessed Report Writer.
   - If **no**, see ***Report Writer Not Installed Properly*** (on page 539) to verify that the correct version of the Report Writer software is installed on your ISDS.

No Data or Old Data in the Report

No Data in Report

Occasionally, after you run a report, the resulting web page displays only the name of the report, a timestamp, and the Run Report button. If you believe that the report should contain data, use the following procedure to determine if ISDS is connecting to the ISDS database.

1. Log in to the ISDS server and enter the password.
2. Open an xterm window on the ISDS.
3. Type **cd /tmp** and press **Enter.**
4. Type **ls *.err** and press **Enter**.

   Note: The "l" in **ls** is a lowercase letter L.
5. Type **cat [report_name].err** and press **Enter**. Replace [report_name] with the name of the report you are requesting. Do not type the brackets **[ ]** in the command.
6. Locate the **[report_name] / open Db( ) error: + an error msg.Exiting** line in the list. The [report_name] represents the name of the requested report.
7. Does the **ERROR: failed to connect!** message appear on your screen?

- If **yes**, Report Writer could not connect to the ISDS database; this is the reason that the reports do not contain data.
- If **no**, Report Writer is connected to the ISDS database, and there is no data to report or some other error has occurred.

Old Data in Report

If a report contains old data, click **Run Report** to refresh the report with current data.

Runtime Errors

Runtime errors generated by ISDS are displayed in the browser. The display includes the name of the file that contains the errors, along with the error messages.

To exit the error display, click the browser **Back** button.

Important: We recommend that you get assistance from your system administrator to resolve runtime errors.

Web Browser Unable to Display Data

Some reports generate a large amount of data. Due to its limitations, your browser may not be able to display very large reports.

To view the data files of reports that have large amounts of data, use a text editor. You can find the data files for each report generated by Report Writer in the **/dvs/RepWriter/current/webspace/reports** directory.

The following tables list the data files generated for each type of report.

Database Reports	File Generated
PPV Events	PPVEvents.html.dat
Zero Credit	ZeroCredit.html.dat
CableCARD Report	CableCard.html.dat
Channels, Sources and Sessions Report	CSSReport.html.dat
DHCT Report	Converters.html.dat
DHCT Packages Report	DhctPkg.html.dat
ISDS Packages Report	DNCSPkg.html.dat
Service Group Report	SvcGroup.html.dat
QAMS Report	Qams.html.dat
PCG Report	Pcg.html.dat

Database Reports	File Generated
NetCrypt Report	NetCrypt.html.dat
SDV Servers Report	SDV Servers.html.dat
QPSK Modems	QPSKMods.html.dat
QPSK Demods	QPSKDemods.html.dat
In Service One-Way	InServOneWay.html.dat
Non-Responding DHCTs — Never Connected	NRNeverConn.html.dat
Non-Responding DHCTs — Lost Connection	NRLostConn.html.dat
DHCT Sign-on Failed Report	DhctSignOnFailed.html.dat
PCG Sessions Report	PcgSession.html.dat

SNMP Poll Reports	File Generated
Non Responding DHCTs — SNMP Poll	NRSNMPPoll.html.dat
OS/App Version	ResAppVersion.html.dat
Memory	FreeMem.html.dat
DHCT Uptime	Uptime.html.dat

System Reports	File Generated
No file generated	

SNMP Poll Reports Do Not Regenerate Data

Occasionally, the ISDS software assumes that the SNMP Poll Reports are in the process of running, when in fact they are not. This situation can occur if you exit your browser while the SNMP Poll Reports are running.

Important: The SNMP Poll Reports can take a significant amount of time to complete, depending on the number of set-tops in the system. While the SNMP Poll Reports are being generated, do not exit your browser. Exiting the web browser while the reports are being generated can cause errors in the ISDS software that will require some manual clean-up steps. We also recommend that you do not click any buttons on your browser until the SNMP Poll Reports are completely generated.

Notes:

- While the reports are being generated, the following message appears on the screen: **Running [report name]. Please wait**. In this message, [report name] represents the name of the SNMP Poll report being generated.

- Concurrently, a table appears on the screen, and as each SNMP Poll report is generated its status is updated from working to complete.

Regenerating SNMP Poll Report Data

If the SNMP Poll Reports do not appear to be regenerating data, complete the following steps to correct the situation.

1. Exit your web browser.
2. From an xterm window on the ISDS, type **su root** and press **Enter**.
3. Enter the root password and press **Enter**.
4. Type **cd /dvs/RepWriter/current/webspace/gen** and press **Enter**.
5. Type **ls** and press **Enter**.
   Note: The "l" in **ls** is a lowercase letter L.
6. Does the file **snmprunning** appear on the screen?
   - If **yes**, type **rm snmprunning** and press **Enter** to delete the file.
   - If **no**, then the failure of SNMP Poll Reports to regenerate is not the problem. Review other sections in this chapter and try another resolution.
7. Type **cp snmp.html.refresh snmp.html** and press **Enter**.
8. Type **exit** and press **Enter**.

   CAUTION:

   Before running Report Writer, exit all instances of your web browser associated with your UNIX user ID. When you try to run Report Writer with more than one instance of your web browser associated with your UNIX user ID, a message appears on the screen stating that your browser has detected a lock file. Do not continue. If you attempt to continue, Report Writer may exhibit unpredictable behavior.
9. Launch your web browser, and run the SNMP Poll Reports.

   Important: Do not attempt to use the web browser until the SNMP Poll Reports are complete.

Online Help Troubleshooting

Occasionally, you may encounter problems while using ISDS Online Help.

Here are some troubleshooting tips you can use that may resolve the problem.

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 that the page is completely loaded into the browser before attempting to print the page.

Help Page Does Not Display Properly

Occasionally, a Help page may not load completely. To resolve this problem, complete these steps.

1. Click **View > Reload** on your browser toolbar.
2. Did the page reload properly?
   - If **yes**, you are finished with this procedure.
   - If **no**, go to step 3.
3. Close the Help completely, and then re-open the Help from the ISDS.
4. Did the page reload properly?
   - If **yes**, you are finished with this procedure.
   - If **no**, go to step 5.
5. Contact your network system administrator.

Logging

Quick Path: ISDS Administrative Console > ISDS tab > Utilities tab > Logging

From the Logging Summary window, you can select the type of information the ISDS records about critical processes (and their libraries). When the ISDS 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.

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 ISDS log in /var/log/dncsLog and view the data that the ISDS has recorded. Or you can open the log for an individual process in /dvs/dncs/tmp/[name of process.*].

If you are using our RCS solution, you can capture logging information about the processes and libraries for each site in your system.

Logging Levels

By selecting a level of logging for a specific site, you can control the type of information that the ISDS will record about processes running at a site.

The default level is the **Error** level, but you can choose any of the following logging levels for any process shown as well for any of its libraries.

- **Emergency** - At this level, the ISDS records issues that require immediate attention and may result in a major malfunction of ISDS applications.
- **Alert** - At this level, the ISDS 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 ISDS records information about ISDS problems, such as a process core or a database failure.
- **Error Conditions (the default logging level)** - At this level, the ISDS records operational problems, such as hardware is offline or a code error.
- **Warning** - At this level, the ISDS records information about potential problems that you should know about.
- **Notice** - At this level, the ISDS records information about normal, but significant events.

- **Information** - At this level, the ISDS records informational messages.
- **Debug** - At this level, the ISDS records information that may help in debugging a problem.

Adjust Logging Levels of a Process

Quick Path - With RCS: ISDS Administrative Console > ISDS tab > Utilities tab > Logging > [Select a Site] > [Select Levels] > Save

Quick Path - Without RCS: ISDS Administrative Console > ISDS tab > Utilities tab > Logging > [Select Levels] > Save

Follow these instructions to select logging levels for processes running on the ISDS (or RNCS if you are using our RCS Solution.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Utilities** tab.
3. Click **Logging**. The Logging Summary for Host window opens and displays the processes of the ISDS host as the default. If you are using our RCS solution and want to display the processes for a site other than the central ISDS site, go to step 4. Otherwise, go to step 5.
4. Click the **Logging Summary for Host** arrow and select the site whose processes you want to log. The system updates the list of processes and displays the processes running at the site you selected.
5. 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.
6. Click **Save**. The system displays a message to let you know the save was completed.
7. Click **OK**.
8. Click **Exit** to close the Logging Summary window and view the logging data in /var/log/dncs/log. Or you can look at data for an individual process in /dvs/dncs/tmp/[name of process.*].

Adjust Logging Levels of Libraries

Quick Path - With RCS: ISDS Administrative Console > ISDS tab > Utilities tab > Logging > [Select a Site] > [Select Process] > Display Libraries

Quick Path - Without RCS: ISDS Administrative Console > ISDS tab > Utilities tab > Logging > [Select Process] > Display Libraries

Follow these instructions to select logging levels for the libraries of specific processes.

1. On the ISDS Administrative Console, click the **ISDS** tab.
2. Click the **Utilities** tab.

3 Click **Logging**. The Logging Summary for Host window opens and displays the processes of the ISDS host as the default. If you are using our RCS solution and want to display the processes for a site other than the central, ISDS site, go to step 4. Otherwise, go to step 5.

4 Click the **Logging Summary for Host** arrow and select the site whose processes you want to log. The system updates the list of processes and displays the processes running at the site you selected.

5 Click **Select** next to the process whose libraries you want to log.

6 Click **Display Libraries**. The Libraries for the process you selected in the previous step are listed beneath the Logging Summary list.

7 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.

8 Click **Save**. The system displays a message to let you know the save was completed.

9 Click **OK**.

10 Click **Exit** to close the Logging Summary window. You can now open an xterm window and view the logging data in /var/log/dncs/log. Or you can look at data for an individual process in /dvs/dncs/tmp/[name of process.*].

26

ISDS Security

Introduction

The integrity, availability, and confidentiality of system operational data depend on system administrators who implement policies and procedures for system security and users who take system security seriously.

An intruder only needs knowledge of a few passwords to cause damage to a local system or network.

To help you maintain secure passwords, this section provides instructions for changing passwords for both system administrators and regular ISDS users.

Outside access to the ISDS presents issues for system security. Therefore, this section also provides instructions for system administrators for limiting access to the ISDS by outside vendors and other individuals.

In This Chapter

Passwords

This section provides guidelines on ensuring secure passwords, on ensuring strong passwords, and instructions on changing user passwords.

Valid Passwords

The following guidelines must be met to create and use valid passwords in the ISDS.

- Blank (null) passwords are not valid in the ISDS.
- Passwords must contain at least 8 characters.
- Passwords must be a combination of letters, numbers, and at least one special character.
- Passwords that are all one character (for example, 1111111 or aaaaaaa) are not valid.
- Passwords expire after a certain number of days. This number is configurable and can vary from site to site. The default is 13 weeks. After that period, your password is voided and you must have an administrator reset your password.

  Note: This applies to **ALL** accounts, including root and the dncs role.
- The system administrator account (root) can change the password to any account.

Secure Passwords

System administrators can implement system requirements to ensure passwords are secure.

This section provides guidelines for ensuring passwords are secure.

To maintain secure passwords, follow the guidelines in this list of best password practices:

- Assign a unique password that is not assigned to multiple users.
- Use strong passwords; see ***Strong Passwords*** (on page 552) for more information.
- Assign different and unique passwords for all systems that the user accesses.

  Note: This limits knowledge of any compromised passwords.
- Collect and authenticate all passwords at the operating system level, or system-core level, not within applications.
- Suspend user IDs after three invalid attempts.

- Assign a one-time password to users who forget passwords. Prompt users to change this one-time password upon login.
- Force privileged or high-security users who have system privileges to change their passwords every 60 days or less, unless extended authentication methods are used.
- Change privileged or high-security user passwords immediately if a password has been compromised.
- Change non-expiring and high-security passwords immediately when an employee who has access to these passwords leaves the company.
- Prompt the user to immediately change passwords when he or she logs in to a system for first-time use.

  Note: Immediately changing passwords ensures that only the user knows the password.
- Change all factory-default passwords immediately (during initial system set up) of all equipment received from vendors.
- Review vendor documentation to ensure that all passwords are identified and changed.
- Stress password confidentiality all the time.
- Use unique passwords on different systems or use extended access authentication if you are an administrator with exceptional system privileges.
- Establish a secondary or backup-supervisor user.
- Keep the secondary or backup-supervisor user in a sealed envelope that is locked in a secured place.

  Note: The name of the account should be an ordinary user name so its presence will not be obvious.
- Use access control lists. Do not assign passwords to files or tables.
- Use mediums other than email to issue passwords and user names. If you must use email, send two separate email messages. The examples below are of separate user name and password email messages:
  - First email: Your new UNIX user name will be xxxx, but the password will be sent to you in a separate email message.
  - Second email: Your password is xxxx. This is a one-time only password. Please change it upon login and always be sure to use strong passwords and keep them confidential!
- Deny the use of passwords that are similar to the current password.
- Deny the use of passwords that are similar to the user name.

- Provide a password history file that consists of a minimum of five previous passwords.
- Incorporate provisions that prevent interception of passwords (encrypted or plain text) into system, security, and network architecture.
- Create a denied, or restricted, list of passwords.

  Note: Words in this list cannot be used as passwords. For example, days of the week, months, sports teams, division, and company names.

Strong Passwords

Users unwisely believe they play a minor role in system security and that the majority of security responsibility relies on the system administrator.

System security is everyone's responsibility.

Both system administrators and users need to use strong passwords. A strong password contains two unrelated words and a special character or number, such as red$code or n1ttf@gm. In contrast, a weak password is often logical and easy to remember, and therefore, easy to guess.

Follow these guidelines to create strong passwords.

- **Do not** give a password to anyone, unless a supervisor approves the request. Document the request and approval.
- **Do not** wait for software to prompt you for a password change.
- **Do not** create a password that consists of numerals only.
- **Do not** use a personal Social Security Number or telephone number.
- **Do not** use a login ID in a backward, forward, or scrambled letter combination for a password.
- **Do not** include anagrams of dictionary words. An anagram is a word or phrase formed by rearranging the letters of another word or phrase. For example, "lives" is an anagram for "Elvis."
- **Do not** select an exact word or phrase from any dictionary, for example, a standard, technical, specialized, professional, foreign, or slang dictionary.
- **Do not** use a common first and last name, a company name, or product name, for example, John Doe, IBM, or HP.
- **Do not** use verb conjugations, such as see, saw, or seen.
- **Do not** use cultural icons, such as Batman, Superman, or Goofy.
- **Do not** use alphabetical sequences, such as abcde.
- **Do not** create a password that is one alphabetical character, such as mmmmm.

- **Do not** use academic degrees for a password, such as Ph.D. or M.S.
- **Do not** use job-related abbreviations or acronyms, such as MHz, LAN, or H2O.
- **Do not** use a street name, child's name, or car model that can be personally related to you.
- **Do not** make passwords logically sequential, such as January, February, or March.
- **Do not** print a password.
- **Do not** store passwords in readable form, such as log-in scripts, programs, software macros, unless encrypted or restricted access is guaranteed.
- **Do not** leave passwords in an unsecured location.

Change Passwords

In addition to using strong passwords, change passwords regularly to protect the integrity of your system. The lead system administrator should change the root password on a regular basis. Administrators should require users to change their own passwords regularly.

Users who log in to the ISDS as "root" have access to all areas of the system. Typically, the lead system administrator has root access and can change the root password as needed. Most users do not need root access.

The root password is shared among a select group of administrators or super users. In contrast, normal ISDS users have unique passwords. When you add a user to the ISDS, set the system to prompt the user for a new password upon the first login.

When users attempt to log in the first time, the system prompts the user to enter a new password. In this way, only the user knows his or her password.

If a user's password is compromised, the user can change the password quickly at any time. Alternately, the administrator can reset a user's password by following the procedure in Changing the User's Password.

The following procedures explain how administrators can change the password for a user to change their own password.

Important: The procedure in this section also applies to the Application Server.

Note: This topic applies to all systems.

1. Open an xterm window on the system.
2. At the login prompt, type **passwd** and press **Enter**. The system will prompt you for your existing password.
3. Enter your **existing password** and press **Enter**. The system will prompt you for your new password.

4. Enter your **new password** and press **Enter**. The system prompts you to re-enter your new password.
5. Type your **new password** again and press **Enter**. The system compares your two password entries. If they match, the **password successfully changed** message appears. If they do not match, you must re-enter the new password.
6. Type **exit** and press **Enter** to close the xterm window.
7. Log out of the system.
8. Log into the system with your new password.

Monitor the expiration period of critical Solaris accounts weekly. The following users must be checked, along with any custom accounts that are considered critical to the successful operation of the system:.

ISDS Accounts

- root
- dncs
- dncsSSH
- pcgrequest
- pcgscp
- Informix
- easftp
- dncsftp

Note: The dncsSSH, pcgrequest, pcgscp, and Informix accounts are not login accounts that expire, unless a system administrator has changed the expiration dates on these accounts. We do not recommend modifying or setting passwords for these accounts.

RNCS Accounts (if applicable)

- root
- dncs
- dncsSSH
- pcgrequest
- Informix
- easftp

Note: The dncsSSH, pcgrequest, and Informix accounts are not login accounts that expire, unless a system administrator has changed the expiration dates on these accounts. We do not recommend modifying or setting passwords for these accounts.

Download Server Accounts (if applicable)

- root

Checking the Password Expiration for Critical Accounts

Follow these instructions to check the password expiration for critical Solaris accounts.

1. Login to the system as root.
2. In an xterm window on the system (ISDS, RNCS, or Download Server), type **logins -x** and press **Enter**. The system displays the password status for all of the user accounts on the system.

   Example result:

   ```
   root    0    root    0    Super-User
                /
                /sbin/sh
                PS 071309 -1 91 14
   ```

   The password aging information is contained in the last line of each entry. From this example:

   PS 071309 -1 91 14

   - The first value (**PS**) is the current status of the password:
     - **PS** – Account has a functioning password.
     - **NL** – Account is a no login account.
     - **LK** – Account is locked, e.g. Password has expired.
     - **NP** – Account does not have a password. It is possible that there are few accounts with NL (for example, the Informix account); however, you cannot login as these users using NULL as the password.
   - The second value (**071309**) is the date when the password was last changed (July 13, 2009).
   - The next value (**-1**) is the number of days that must pass before the password can be changed. A value of -1 means this functionality is disabled.
   - The next value (**91**) is the number of days the password is valid. A value of -1 means this functionality is disabled.

- The last value (**14**) is the number of days a password expiration warning will be displayed upon login before the password expiration date. A value of -1 means this functionality is disabled.

If the password for any critical account will expire soon, you must change the password, ***extend the password expiration date*** (see "***Extending the Password Expiration Date***" on page 556), or ***disable password expiration*** (see "***Disabling the Password Expiration Date***" on page 556).

Important: Disabling password expiration simplifies password management, but doing so increases your security risks.

Extending the Password Expiration Date

Note: The new password expiration date must be communicated to the customer.

1. Login to the ISDS as root.
2. In an xterm window, type **passwd –r files –x [days] [username]** and press **Enter**.

   Note: The **[days]** parameter is the total number of days from when the user set their password to when that password expires. If your normal expiration period is 30 days, and you want to extend that period for two more weeks, you would add 14 days to the existing [days] parameter for a total of 44 days.

   Example: Type **passwd –r files –x 44 jonesx** and press **Enter**.

Disabling the Password Expiration Date

Note: The account holder must agree that password aging will be disabled at the expense of security. We do not recommend disabling the password expiration period.

1. Login to the ISDS as root.
2. In an xterm window, type **passwd –r files –x –1 [username]** and press **Enter**.

   Example: Type **passwd –r files –x –1 jonesx** and press **Enter** to disable the password expiration date for account jonesx.

27

ISDS Reference Guide

Introduction

The ISDS Reference Guide is a companion document to the ISDS Online Help. This reference guide provides additional information to explain certain background concepts.

In This Chapter

What is the ISDS Solution?

The IPTV Service Delivery Platform (ISDP) solution is a high-performance, open-architecture network that is capable of delivering a wide-range of advanced video applications using the Internet Protocol (IP) as the common communication method.

Unlike other delivery methods, IP streaming enables service providers to evolve their networks over time to enable the full, connected experience of many services to many screens.

For information on the basic approaches service providers can take in configuring the ISDP solution, refer to the *ISDP System Overview with Focus on the ISDP Server and ISDP Client* (part number 4017607).

What is an ISDS?

An IPTV Services Delivery System (ISDS) is a UNIX workstation that is typically installed in a headend or, occasionally, a hub, and is connected to a service-delivery system.

The ISDS provides information about each element in a service-delivery system and allows elements to communicate with each other. By communicating with these elements, the ISDS allows operators to provide subscribers with many types of digital services.

Network Overview

This section provides an overview of how you can use the ISDS Administrative Console to view the network status and manage the network.

View Network Status

The ISDS Administrative Console Status window helps you determine the status of the ISDS and of the Application Server.

ISDS Status

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

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

In addition, if you click the **Control** button in the ISDS section, the ISDS Control window opens, which allows you to monitor all of the major ISDS processes.

Application Server Status

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

- **Running** — the Application Server software package is present and in operation
- **Inactive** — the Application Server software package is present, but not in operation
- **Not Responding** — the Application Server does not respond when the ISDS tries to communicate with it
- **Not Installed** — a Application Server host is defined in the host table, but the Application Server software package is not present; this usually indicates that you are not using our Application Server, but the application server of another vendor
- **Blank** — no Application Server host is defined in the host table, and the Application Server software package is not present; usually indicates that you are not using our Application Server, but the application server of another vendor

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

WARNING:

Do NOT attempt to start or stop an AppServer process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.

The Application 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**) — Generates the files containing the global, hub-specific, and staging configuration values and places the files on the broadcast server.
- **IPGServer - language supported (Interactive Program Guide Server)** — Generates the IPG files for each language supported, and places the files on the Broadcast File Server. The languages available are English, French, Spanish, and Japanese.

  Note: Each language that is supported has its own application. For example, if English is supported, the application would be listed as **IPGServer- eng**.
- **ppvfileserver (Pay-per-view File Server)** — Generates PPV files 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.
- **vcServer (Virtual Channel Server)** — Places the files for all configured virtual channels on the Broadcast File Server.
- **bfsRouter (Broadcast File Server Router)** — For a Regional Control System (RCS), routes BFS Application Program Interface (API) calls from the SARA Server, such as IPG, PPV, or VCS, to the BFS on the ISDS at the central RCS site. The BFS Server on the central RCS site is site-aware. The BFS router converts any non-site BFS calls to site-specific calls and passes them along to the BFS server. This includes calls from Application Server processes, such as IPG, PPV, VCS, and any other third-party applications using the BFS API.

For more information on the SARA Server, refer to the *SARA Application Server 3.4.1 User Guide* (part number 4012159). See Printed Resources for information on obtaining documentation.

Manage the Network

This section describes some of the tools you can use to manage the ISDP network.

DNCS Administrative Console Window

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

ISDS Tab

The **ISDS** tab on the Administrative Console provides access to certain functions that ISDS software directly controls.

System Provisioning Sub-Tab

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

The **System Provisioning** sub-tab on the ISDS tab is divided into several functional sections.

Service Provisioning

Quick Path: Administrative Console > ISDS 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
IP Source Definitions	■ Add, modify, provision, or delete IP multicast sources

System Management

Quick Path: Administrative Console > ISDS 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 network as described in the following table.

This button...	...allows you to perform these tasks
Sys Config	■ Set up DHCT session signalling parameters ■ Set up Network session signalling parameters ■ Set up SDV parameters ■ Set up ISDS Service Delivery Server parameters ■ Set up system-wide Bandwidth Management parameters
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 *ISDP Set-Top Staging Guide* (part number 4021173). See Printed Resources for information on obtaining documentation.
User Access	■ Add, modify, or delete users with differing levels of access to the ISDS. **Note:** For assistance in using this feature, refer to *Guidelines for System Security Passwords* (part number 738188). See Printed Resources for information on obtaining documentation.
IP VOD	■ Establish communications between the ISDS and the VOD server.
DST	■ Set up daylight saving time (DST) rules that can be used by DHCTs in different time zones. Setting up the correct DST rules enables the set-tops in your system to automatically adjust to changes in DST observance.
Bandwidth Mgmt	■ Establish bandwidth management business rules.

EAS Message

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

The **EAS message** section of the System Provisioning sub-tab allows you to manage the EAS (Emergency Alert System).

WARNING:

Do not modify any of the Emergency Alert System settings in the ISDS unless you are specifically instructed to do so by the Federal Communications Commission (FCC), National Weather Service, local weather authority, or us. Otherwise, you could cause the EAS to perform improperly or not at all.

Note: For more information about the Emergency Alert System, see ***Manage a Digital Emergency Alert System*** (on page 283).

Network Element Provisioning Sub-Tab

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

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

This button...	...allows you to perform these tasks
Headend	Add, ***modify*** (see "***Modify a Headend***" on page 19), or ***delete*** (see "***Delete a Headend***" on page 20) a headend
Cluster	Add, modify, or delete a node set and its associated hub
MPEG Source	Add, modify, or delete an MPEG source
GbE Transport	***GbE Elements*** (on page 60)
Hub	■ ***Add*** (see "***Add a Hub***" on page 22), ***modify*** (see "***Modify a Hub***" on page 23), or ***delete*** (see "***Delete a Hub***" on page 24) a hub ■ Define the time zone where a hub is located ■ If daylight saving time is observed at this hub, define the DST Zone ID
Localization	***Localization Codes*** (on page 29)
VASP	Add, modify, or delete a VASP
DCM	***Digital Content Manager (DCM)*** (on page 61)
VQE	***VQE*** (on page 34)

Home Element Provisioning Sub-Tab

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

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

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.
Reports	Run various reports to see how the system is functioning. For more information, see the . **Note:** To obtain this guide, see ***Printed Resources*** (on page 8).
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.
Logging	Access the Logging utility to fine-tune log levels for processes and their libraries.
Session List	Control sessions and resources within the network.
xterm	***Open an xterm window*** (on page 565) to perform troubleshooting activities.

Open an xterm Window

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

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

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

DHCT Provisioning

The **DHCT Provisioning** area has five buttons that allow you to work with the set-tops in your system as described in the following table. You may find the *Downloading New Client Application Platform Installation Instructions* (part number 4003052) useful for more information on using this part of the ISDS. See Printed Resources for information on obtaining documentation.

Important: Except for testing purposes, you should set up (stage) the set-tops in your system as described in the *ISDP Set-Top Staging Guide* (part number 4021173). See Printed Resources for information on obtaining documentation.

This button...	...allows you to perform these tasks
Type	■ View a list of the set-top types contained in your ISDS database, along with the revision level and OUI for each. ■ Add, modify, or delete a set-top type. ■ Download specific operating systems to the set-tops in your network.
DHCT	■ Add, modify, or delete an individual set-top. ■ Send service or system information to an individual set-top within a few minutes. ■ Enable an individual set-top to display secure PPV and VOD services. ■ Authorize a set-top module for service. **Note:** Your billing system normally authorizes the set-tops in your system for all services. Although you can authorize set-tops for services directly from the ISDS, your billing system performs this task more quickly and efficiently. Except for testing purposes as described here, you should coordinate the authorization of set-tops for services with your billing system vendor.
Boot Page	This feature is reserved for future use.
OS	■ View the names of files that currently reside on the BFS.

Image **Note:** Although this button is in the DHCT Provisioning area, you can use this button to download software to set-tops.	■ Load the set-top resource file (set-top.res) into the ISDS database. ■ View a list of the current set of image files on your system. ■ Load new image files onto the BFS, or remove old image files that are no longer used. ■ Create test groups of set-tops. ■ Set up and download client software to set-tops on your system.

■ ***Application Interface Modules Tab*** (on page 567)

Application Interface Modules Tab

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

This button...	...allows you to perform these tasks
BFS Admin	■ Add, modify, or delete BFS servers, sources, and hosts. For assistance, see Manage a Third Party Application.
BFS Client	■ Add, modify, or delete new servers, directories, files, and links to the BFS that allow set-tops to access application information.
CSM Service	■ ***Add*** (see "***Add CSM Services***" on page 73), modify, or delete Channel Service Manager (CSM) services that associate a specific service with an application that defines the medium to be used for that service.
Channel Maps	■ Add, modify, or delete channel maps. ■ ***Add services*** (see "***Add a Service to a Channel Map***" on page 110) to specific channel slots on specific channel maps. ■ Assign specific channel maps to specific hubs.

Server Applications Tab

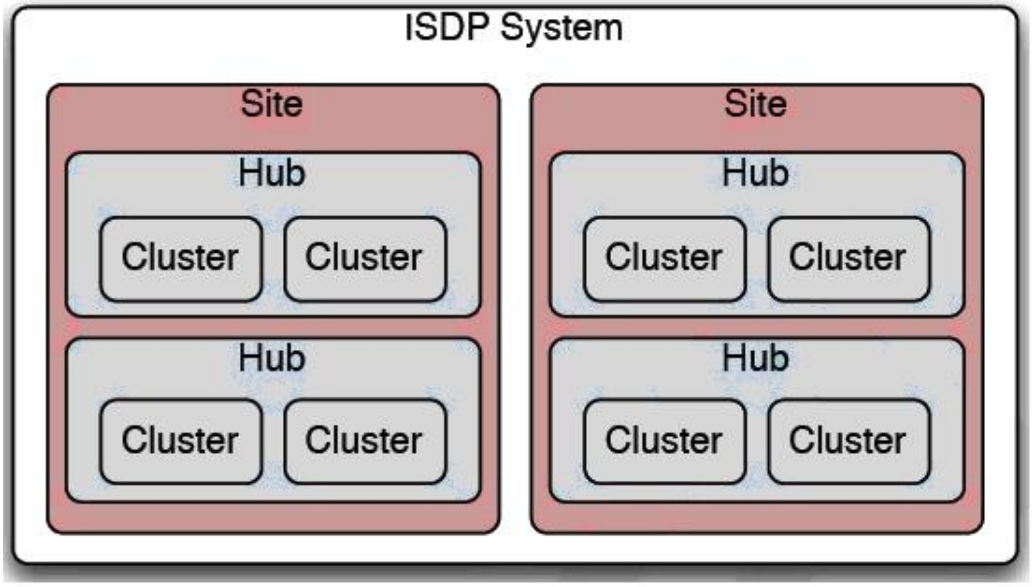
The **Server Applications** tab on the Administrative Console provides access to applications that reside on the Application Server so that you can configure services associated with applications. The options that appear on this tab vary depending on the applications available on your system. The following illustration provides some examples of options you might see on this tab. Refer to the *SARA Application Server 3.4.1 User's Guide* (part number 4012159) for more information. See Printed Resources for information on obtaining documentation.

Flows

The ISDS provides information about the system to set-tops using a set of IP multicast flows. This section describes each flow and how the ISDS processes them.

The flows in the system are arranged in a hierarchy. The system is divided into sites, hubs, and clusters as shown in the diagram below.

The lowest level in the hierarchy, the cluster, is a collection of IP subnets. Each set-top is assigned to a cluster, each cluster to a hub, and each hub to a site by the operator in the ISDS. Since there is only one system-wide flow, a well-known multicast address is used (224.0.23.42). The remaining flows use dynamic IP addresses. The set-tops acquire the IP addresses of the site, hub, and cluster flows during the registration process (in the UNConfigConfirm message).



System Multicast Flow

The system-wide flow contains IP names or address of the various video application servers in the system and a code verification table (CVT) that tells the set-tops in the system when to upgrade their code. All set-tops join the system-wide flow during the boot process. The system-wide flow resides at a well-known IP multicast address. The IP names or addresses are provided on the system-wide flow using DSM-CC UNConfigIndicator messages.

Site Flow

The site flow provides the layout of sites and determines at which sites the various hubs are located.

Hub Flow

The hub flow provides the system information (SI) table which contains service parameters for each service in the system.

Cluster Flow

The cluster flow provides a way for the ISDS to send messages to one or more set-tops.

The cluster flow is special in that it is the only permanently joined multicast flow in the system. All other flows in the system are joined as required.

The cluster flow allows the ISDS to provide change notification for all other flows. When there is new information in one of the other system multicast flows, a change notification is sent on the cluster flow.

The set-top then joins the flow that contains new information and waits for the update. Once the set-top obtains the updated information, it leaves the other flow. The change notifications are provided on the cluster flow using DSM-CC UNPassThru messages.

BFS Flow

The BFS flow is the primary interface (means of communication) between the Application Server and the set-tops that are connected to the network.

Glossary

10BASE-T

An IEEE standard (802.3) for operating 10 Mbps Ethernet networks (LANs) using two pairs of twisted-pair cabling: one pair for transmitting data and the other for receiving data.

1394

A high-speed two-way connection that allows easy transfer of digital video.

55-1

See SCTE55-1.

ac-3

Digital audio compression – 3 (Dolby Labs)

access point

An interface between the wireless network and a wired network. Access points combined with Ethernet support the creation of multiple radio cells that enable roaming.

analog

A format in which information is transmitted by modulating a continuous transmission signal, such as amplifying the strength of a signal or varying its frequency.

APDU

Application Protocol Data Unit. A common structure to send application data between the M-Card module and the host.

API

Application Program Interface. A set of protocols, routines, and tools for building software applications. An interface that enables programs to communicate with each other.

Application Server

A server used to execute the application programs, which provide an interface for downloading application data to the set-tops and CableCARD modules. The AppServer works in conjunction with the ISDS and the two servers share a common database.

AppServer

See Application Server.

authentication

A method in which the network requires a user to identify themselves by entering a user name and password.

authorization

The process of granting or denying access to specific resources.

authorized service domain

In the authorized service domain (ASD), content is secured using the mechanisms available through the operator's conditional access system.

The authorized service domain (ASD) physically translates into a collection of one or more trusted devices where content may be securely stored and moved within the domain (typically the subscriber's home).

The distinction between the authorized service domain and other forms of copy protection (for example, DTCP) is that the content remains under operator control at all times with ASD. The control points within the domain are the M-Cards supplied by the operator. Consider the authorized service domain as the operator's digital rights management (DRM) system and an extension of the operator's conditional access (CA) system.

bandwidth

The maximum data carrying capacity of a transmission link. For networks, bandwidth is usually expressed in bits per second (bps).

BER

Bit error rate. Ratio of received bits that contain errors.

BFS

Broadcast File System. The primary interface (means of communication) between the AppServer and the DHCTs that are connected to the network.

bind

A DNCS function that matches the CableCARD module's ID to its host's ID to ensure that the host device conforms to the copy-protection rules defined by the Copy Control Information (CCI). You must bind a CableCARD module to its host before the host can receive high-value copy-protected services.

bit rate

The number of bits of information that can be transmitted over a channel in a given second (usually expressed in bits per second [bps]).

blended image

A screen image on the host device that displays the current channel video, along with the diagnostic screen.

boot

The loading of the operating system (OS) and application programs into the main memory or random access memory (RAM) of the system.

Bootloader

A factory program installed into the DHCTs to ensure reliable upgrades.

BOSS

Business Operations Support System. Open Network Computing RPC protocol for sending requests and responses. It is used by the Billing System to interface to the DNCS and is one of the DNCS/ISDS interfaces for communication with SMS hosts. All BOSS requests are processed by the BOSS server and routed to the proper DNCS/ISDS component.

BOSS Server

Provides a mechanism for the routing of a BOSS requests to and from the appropriate DNCS/ISDS component and the BOSS client that initiated the request. Also provides a mechanism for the routing of a BASS request to and from the appropriate Application Server and the BASS client that initiated the request.

bounce

Stop and restart a network element or process. For example, to *bounce* the osm process means to stop and restart the process.

bps

Bits per second.

brick mode

A state in which the DHCT is not authorized to receive services. Provided by a package which stops all functions of the DHCT, including the ability for it to turn on. Also called *service disconnect*.

bridge

Device that connects and passes packets between two network segments that use the same communications protocol.

broadband

A characteristic of a network that indicates that a wide band of frequencies is available. A large amount of information can be carried by multiplexing and transmitting on many different frequencies simultaneously. Sometimes used more narrowly to describe cable modem service or DSL (digital subscriber line) service from a telephone company.

broadcast address

A unique address reserved for sending a message to all receiving stations.

broadcast flag

A technology that sends a message to copying devices not to allow unauthorized copying or distribution via networking devices such as connected Digital Video Recorders.

broadcast server

A server that delivers interactive content and broadcast data feeds. It uses Internet Protocol (IP) to encode and deliver data over networks that support IP Multicast.

CA

See Conditional Access.

CableCARD

A device that plugs into a digital cable-ready TV or DHCT and allows the receipt of encrypted services.

carousel

Transports data modules and application server processes from the BFS server to the DHCT. For each new application server process that registers with the BFS, a new data carousel is created and the ID information is updated in the BFS directory structure. *Also known as* Data Carousel or Data Pump.

CAS

Conditional access system. The PowerKEY® CAS is a flexible, secure Digital Rights Management (DRM) system for supporting digital and analog services. The system offers software encryption and decryption and uses secret key, public key, and private key data to secure the digital signal.

CCI (Copy Control Information)

Copy Control Information defines a program's level of copy protection. There are currently three copy protection levels defined: *copy freely*, *copy once*, and *copy never (copy once* and *copy never* are known as *high-value copy protection*). The CCI is set for the program by the program originator.

The DNCS/ISDS sends the CCI information to the DHCT or CableCARD module in an Entitlement Control Message (ECM) that lets the DHCT or CableCARD module know whether the program is high-value or not.

CDL

Common Download.

Certification Revocation List

See CRL.

Channel Map

A set of channels that specific subscribers are authorized to receive through their DHCTs.

channel map ID

See VCT ID.

Channel Mapping

Placing an available television channel signal to appear at any desired channel marking on a customer's HCT.

Clear Channel

A service that is delivered to subscribers unscrambled or unencrypted.

cluster

A logical element that represents a collection of set-tops.

The cluster to which a set-top is assigned determines the channel map and system information (SI) that the set-top receives. Each cluster corresponds to a single multicast carousel that carries all of the cluster-specific data for that cluster.

Comment out

To add a # (pound sign) to the beginning of a line in a UNIX file. UNIX Servers ignore any lines within a file that begins with a #.

conditional access

An encryption/decryption process, which provides access to the broadcaster's services and ensures secure purchase transactions for interactive services.

Copy protection

A system for preventing the unauthorized reproduction of copyrighted media through setting the copy protection levels for a program or service. There are three types of copy protection settings:

- Copy freely
- Copy once (high-value)
- Copy never (high-value)

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.

CPE

customer premise equipment. Network devices (PCs, set-top boxes) that are located at a customer site and connect to a cable modem (CM) or other access network.

CRL

Certification Revocation List. A list of host devices that are not authorized to duplicate copy-protected content.

CVT

Code Version Table. A method for staging set-tops. The CVT is a table that contains information about download channels and information to map client release software versions to specific set-top types.

The Broadcast File Server (BFS) broadcasts this information once per second on the quadrature phase shift keying (QPSK) frequency. If a set-top does not have valid client release software installed, the set-top searches QPSK frequencies for software download information. When the set-top finds this information, it can begin to download valid client release software.

data bus

The bus (connections between and within the CPU, memory, and peripherals) that is used to

carry data to and from a processing unit or storage device.

data carousel

See carousel.

data pump

See carousel.

data rate

An amount of information that can be transferred per a unit of time, for example bits per second (bps).

DCM

digital content manager. An MPEG processing device that is capable of supporting extremely high numbers of video stream processing.

decryption

The process of decoding encrypted data into its original and understandable language.

DHCT

Digital Home Communications Terminal. Our digital set-top that is two-way capable for interactive services. *See also* Explorer.

download server

A secondary server to push device images to network devices, such as set-tops and CableCARD modules.

DSG

DOCSIS set-top gateway.

DTV

Digital Television. A telecommunication system for broadcasting and receiving video and audio by means of digital signals.

DVR

digital video recorder. A device that records television programs without the use of videotape and saves them to a hard drive located inside the recorder. The programs can then be deleted, saved to a tape, or left on the hard drive. A DVR allows you to pause live broadcast for interruption, such as creating your own instant replays. *Also known* as PVR.

EA

Entitlement Agent. Data structures transmitted within messages having cryptographic protection that authorize reception of service to a DHCT.

EAC

Emergency Alert Controller. A workstation that receives and formats the Emergency Alert Message (EAM), then sends it by FTP to the Digital Network Control System (DNCS) over an Ethernet connection.

EAM

Emergency Alert Message. A message sent by the Federal Communications Commission (FCC), the National Weather Service, or local authorities to cable service providers who broadcast these messages to cable television subscribers. These messages include regular tests of the Emergency Alert System, as well as messages that warn of dangerous conditions such as thunderstorms, floods, tornadoes, hurricanes, and earthquakes.

EARS

Emergency Alert Receiver Server. A server that monitors a designated port to receive EAMs. When the EARS receives an EAM, it places the audio portion of the EAM in the /export/home/easftp directory and sends the EAM to the MMMServer.

EAS

Emergency Alert System. A warning system that is activated at the headend and broadcasts emergency messages to subscribers.

EAT

Emergency Action Termination. An event code that ends transmission of EAMs to subscribers. Used when your system does not use CableCARD modules.

ECM

Entitlement Control Message. System-wide information that “unlocks” an encrypted service by transmitting control words. Each ECM is unique for each service. An ECM enables cryptographic partitioning so that different Entitlement Agents (EAs) can selectively grant access to their own services.

EMM

Entitlement Management Message. Contains information for a specific DHCT that enables it to access secure services.

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.

encryption

The process of converting plain text into a coded signal for security.

EOM

End of Message. An event code that ends transmission of EAMs to subscribers. Used when your system uses CableCARD modules.

Explorer®

Our registered trademark name for the Digital Home Communications Terminal (DHCT). Also known as a set-top box.

FECM

Future entitlement control messages.

firewall

Router or access server, or several routers or access servers, designated as a buffer between any connected public networks and a private network.

flash memory (ROM)

Nonvolatile storage that can be electrically erased and reprogrammed so that software images can be stored, booted, and rewritten as necessary.

flash ROM

A rewritable ROM that does not lose its information when the power turns off.

flows

The ISDS provides information about the ISDP system to set-tops using a set of IP multicast flows. The flows in the system are arranged in a hierarchy.

The lowest level in the hierarchy, the cluster, is a collection of IP subnets. Each set-top is assigned to a cluster, each cluster to a hub, and each hub to a site by the operator in the ISDS.

The set-tops acquire the IP addresses of the site, hub, and cluster flows during the registration process (in the UNConfigConfirm message).

force tuning

The set-top service is changed without the user's control. Force Tuning may be initiated and suspended by EAS messages.

frequency

The number of times an electromagnetic wave repeats an identical unit of time, usually one second. One Hertz (Hz) is equal to one cycle per second.

FTP

File Transfer Protocol. A method used to exchange files between computers on a network or the Internet using the TCP/IP protocol.

gain

The extent to which an analog amplifier boosts the strength of a signal.

gateway

A network component that acts as an entrance to another network.

headend

The location of the network elements that processes the signal by receiving and preparing the source signals and making them ready for the transport network. *See also* network elements.

hello packet

Multicast packet that is used by routers for neighbor discovery and recovery.

high-value copy-protected service

A copy-protected service that has a copy protection setting of either *copy once* or *copy never*.

horizontal resolution

The number of vertical lines (or pixels) that can be resolved from one side on an image to the other side.

hub

A hub is a logical element identified by a multicast IP address which set-tops join to acquire system information (SI). In the network topology, a hub belongs to a headend. A cluster belongs to a hub.

IEE-802.3

An IEEE specification for SCMA/CD based Ethernet networks.

IEEE

Institute of Electrical and Electronics Engineers. Professional organization whose activities include the development of communications and network standards. IEEE LAN standards

are the predominant LAN standards today.

IEEE 1394

A high speed digital interface that is used to transmit digital audio/video data. Also known as Firewire.

IEEE 802.11

A family of IEEE specifications for setting wireless LAN standards. Specified for 1 and 2 Megabits per second (Mbps) wireless Local Area Networks (LANs).

IEEE-802.11b

An IEEE specification for 5.5 or 11 Megabits per second (Mbps) wireless Local Area Networks (LANs).

IEEE-802.x

The set of specifications for local area networks (LAN) from the Institute of Electrical and Electronics Engineers (IEEE).

Internet Protocol

The standard protocol within TCP/IP that defines the basic unit of information passed across an Internet connection by breaking down data messages into packets, routing and transporting the packets over network connections, then reassembling the packets at their destination.

interstitial

Programming that appears on PPV channels between events, such as general programming or an advertisement.

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.

IP multicast

Routing technique that allows IP traffic to be propagated from one source to a number of destinations or from many sources to many destinations. Rather than sending one packet to each destination, one packet is sent to a multicast group identified by a single IP destination

group address.

LAN

Local Area Network. High-speed, low-error data network covering a relatively small geographic area that connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area.

LED

light-emitting diode. Semiconductor device that converts electrical energy into light. Status lights on hardware devices are typically LEDs.

Logger

A utility on the Application Server that manages the size, name, and placement of the log files in the /dvs/appserv/tmp directory.

MAC address

Media Access Control address. A unique physical address embedded into a network device. Similar to a serial number.

macroblocking

Blocking, freezing, or tiling of a picture due to signal interference or signal strength and level issues.

memory

Data storage used by computers or other digital electronic devices or systems to hold programs and data while they are temporarily in use.

MIB

Management Information Base (SNMP data structure).

microprocessor

A central processing unit (CPU) implemented on a single chip that performs the bulk of the processing and controls the parts of a system.

MMM Server

Multi-Media Message Server. Relays the EAM TXT file to the PassThru process and converts the WAV file to AIFF format. It then places the AIFF file on the bfsServer.

MPEG

Moving Picture Experts Group. An international video compression standards-setting group

working under the supervision of the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). MPEG's mission is to develop standards for compressed full-motion video, still image, audio and other associated information.

MPEG-1

A bit stream standard for compressed video and audio optimized to fit into a bandwidth of 1.5 Mbps.

MPEG-2

Intended for higher quality video-on-demand applications and runs at data rates between 4 and 9 Mbps.

MPEG-4

A low-bit-rate compression algorithm intended for 64-kbps connections.

MTBF

mean time between failure.

multicast

Single packets copied by the network and sent to a specific subset of network addresses. These addresses are specified in the destination address.

multicast address

Single address that refers to multiple network devices.

multicast group

Dynamically determined group of IP hosts identified by a single IP multicast address.

NAT

Network address translation. The translation of an Internet Protocol (IP) address used within one network to a different IP address known within another network.

NVM

non-volatile memory. Memory that holds its content when the device it is associated with is turned off.

PAL

Phase alternation line. TV system used in most of Europe in which the color carrier phase definition changes in alternate scan lines. Utilizes an 8 MHz-wide modulated sign.

PCG

PowerKEY CAS gateway.

PID

packet/program identifier. A number assigned to MPEG transport packets to identify the contents of the data and the information stream to which they belong. The 13-bit PID number is assigned in the MPEG-2 transport packet headers. All packets from the same stream have the same PID number.

PIN

personal identification number. A password used for identification.

PIP

Picture-in-Picture. Allows you to watch more than one TV program (channel) at the same time on television sets or other devices. With PIP feature of TV, one program will be displayed on the entire TV screen, and another program or programs will be displayed in individual smaller squares on the screen.

POD Module

Point-of-Deployment module. Approximately the size of a credit card and inserts into a host device (either a DHCT or cable-ready television) to provide conditional access to secure digital content. *See also* CableCARD, M-CARD.

POST

Power on self test. Set of hardware diagnostics that runs on a hardware device when that device is powered up.

PowerKEY® Conditional Access system

Our registered trademark name for the hardware and software encryption and decryption of digital signal. Uses secret key, public key, and private key data to secure the digital signal.

PowerTV®

Our registered trademark name for the operating system software and integrated circuits created for high-speed processing and presentation of interactive graphics and audio for the DHCT.

PPV

pay-per-view. Service for which subscribers are charged a user fee for individual program events. *See also* IPPV.

PPV Barker

A screen that the DHCT displays to advertise an event or let a subscriber order a PPV event.

PPV window

A period of time during which a PPV action occurs. The period of time that a window is present often determines when the PPV service displays a specific type of advertisement or purchase option.

provision

The process of preparing a device or service so that the DNCS/ISDS recognizes the device, which allows the device to operate properly.

PVR

See DVR.

QAM

quadrature amplitude modulation. A frequency modulation technique primarily used for program audio and video. QAM supports data rates from 27 Mbps to 36 Mbps.

QPSK

Quadrature Phase-Shift Keying. Digital modulation scheme that send data by modulating the phase of a reference signal (the carrier wave).

QPSK modulator/demodulator

The QPSK modulator works with the QPSK demodulator and the DHCT to provide forward signaling and a reverse communications path for interactive video and data services. The QPSK modulator and demodulator convert digital bit streams to RF format and RF signals to digital bits, respectively.

Radio Frequency

Logical grouping of information that includes a header containing control information and (usually) user data.

RAM

Random access memory. Volatile memory that can be read and written by a microprocessor.

revoked

Condition in which a host device cannot be authorized to copy copy-protected services.

RJ-45

Registered jack-45. A serial connector used to hook up computers to local area networks (LANs).

RMA

Return material authorization.

RMT

Required Monthly Test. The FCC requires operators of cable television stations to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

router

A device that routes data through a packet-switched network, such as the Internet, from one LAN or WAN to another, or from a LAN to the Internet.

RPPV

reservation pay-per-view. Requires the subscriber to use the telephone to reserve a PPV event.

RWT

Required Weekly Test. The FCC requires operators of cable television stations to conduct weekly and monthly tests of their EAS. These tests ensure the reliability of the EAS equipment so that subscribers will receive national, state, and local warning messages about emergency situations.

SAM

Service Application Manager. Associates a specific service with an application that defines the medium to be used for that service, such as the World Wide Web. The SAM maintains the application in a specific directory to be used when needed by the DHCTs.

S-CARD

Single-Stream CableCARD. *See also* CableCARD, M-CARD, POD Module.

SCTE 55-1

A standard initiated by the Society of Cable Telecommunications Engineers that defines out-of-band communications in a video network.

SDTV

Standard definition TV. Digital television format that includes 480-line resolution in both

interlaced (480i) and progressively scanned (480p) formats.

Service Disconnect feature

The process of disabling a DHCT so that it cannot be used to view cable services. Also known as *Brick mode*.

shared key authentication

A type of authentication that assumes each station has received a secret shared key through a secure channel independent from an 802.11 network. Stations authenticate through shared knowledge of the secret key. Use of Shared Key authentication requires implementation of the 802.11 Wireless Equivalent Privacy algorithm.

SI

system information. A standard set of tables providing the data necessary for a navigation device to discover and access services.

signal level

The signal power or intensity at a specified point and with respect to a specified reference level.

SIL

Signaling interface level.

SNMP

Simple Network Management Protocol. A network management protocol used almost exclusively in TCP/IP networks. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SONET

Synchronous Optical Network. An optical fiber network capable of transmitting ATM data packets over long distances. This data remains in a digital state and can be repeated indefinitely.

subnet mask

32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.

subscriber

A household or business that legally receives and pays for cable and/or pay television service for its own use.

S-Video

A video connection that carries the brightness and color portions of a video signal in separate streams for improved color accuracy and reduced distortion.

tar

Short for *tape archive*, a UNIX utility that combines a group of files into a single file with a *.tar* extension.

TCP/IP

Transmission Control Protocol/Internet Protocol. An Internet working protocol that provides reliable data transport using connection-oriented techniques.

TED

Transaction Encryption Device. Provides Conditional Access control for the PowerKEY software within the DNCS and works directly with the DNCS/ISDS to maintain security throughout the network.

TED FX

A TED that provides faster transactions. See TED.

timestamp

The current time, recorded on the network at the headend, in which an event occurs.

Tracing

The process of tracking the flow of data messages between the Application Server and other network elements.

transport network

Provides the communication link enabling audio, video, and data to be transported from the headend to the hub. It involves a network of switching and transmission equipment and can include AM fiber and SONET technologies.

transport stream

A data communications signal that is formatted in accordance with the protocol defined in the MPEG-2 specification ISO IEC 13818. An MPEG transport stream can carry voice, video, or data information. The MPEG data transmission protocol transports real-time data.

two-way operation

Operation in which transmission is made in two directions (from the headend to the subscriber and from the subscriber to the headend).

UN-Config

User-to-network configuration. A message sent from the DNCS that configures the DHCT.

unicast

Message sent to a single network destination.

unicast address

Address specifying a single network device.

UNIX

An operating system that is less computer/server-specific than other operating systems. UNIX is widely used in the telecommunications industry and by the Internet.

upstream

The transmission path from the subscriber to the headend.

USB

universal serial bus. A port on a PC or other device that provides connection to peripherals, such as CD-ROM drives, printers, modems, and keyboards.

VASP

Value-added service provider.

VCT ID

Virtual channel table identifier. Each set-top is assigned a virtual channel table identifier (VCT ID) during the set-top provisioning process. A set-top uses its VCT ID to retrieve its associated SI data among other sets of data that might be available on its hub. For this reason, you might hear the terms VCT ID and Channel Map ID used interchangeably.

Note: The ISDS keeps an association of Hub/QPSK/VCT ID. If a VCT ID no longer applies to a Hub, the ISDS stops sending SI or VCT data associated with that VCT ID to that Hub.

vertical resolution

The number of horizontal lines (or pixels) that can be resolved from the top of an image to the bottom.

VOD

video-on-demand. The ability of a subscriber to select a program event and watch it within moments of selection. VOD allows pausing and rewinding of the event.

VOD back office

A set of servers that manage asset publication and asset metadata, subscriber rentals, NPT (normal play time, or the time to resume playing a movie that was stopped); create and publish the VOD catalog which contains categories and subcategories of offerings, such as Movies on Demand (MOD) and Subscription VOD (SVOD).

VOD navigation server

A front-end server that interfaces to the set-top VOD navigation client and allows the subscriber to navigate the VOD catalog by category (for example, drama, comedy, etc.) and select an offering (MOD or SVOD) to purchase, view, or preview. In addition, the navigation server may return the list of active rentals as requested by the subscriber.

VOD search engine server

A server that responds with a list of asset URLs that meet the search criteria specified by the search client residing on the set-top. The search is based on the conditional access system used by the set-top.

VOD SRM

VOD session resource manager. A server that processes requests for VOD session setup or teardown and checks entitlements and credit limits with the Billing System/Operations Support System (OSS)/Backoffice Support System (BSS).

VOD storage/streaming

Aggregates, stores, and distributes VOD content for set-tops.

VoIP

Voice-over-Internet-Protocol. These services are a provision of voice telephony through the use of packet-switched networks running Internet Protocol (IP) networks rather than traditional circuit switching.

VQE

Visual quality experience. A real-time error repair and quick-channel change system for system providers delivering broadcast data over DSL in an ISDP.

WAN

Wide Area Network. A network that interconnects geographically distributed computers or local area networks.

Index

K

L

M

N

O

P

T

U

V

W

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

678.277.1000
www.cisco.com

June 2010 Printed in United States of America Part Number 4038462 Rev A