DTACS Online Help

Version 1.2.0.5

Contents

1

Welcome to the DTACS Help

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

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

In This Chapter

About This Version of Help

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

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

Help Version and Copyright

DTACS Online Help Version 1.2.0.5 (PC)
June 2010

4036706 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 DTACS 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 DTACS 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 DTA Control System and for no other purposes.

Disclaimer

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

Limitation of Liability

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

Indemnification

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

Other Terms

Cisco reserves the right to change the System at any time without notice. The System is not to be construed as conferring by implication, estoppel, or otherwise any license or right under any copyright or patent, whether or not the use of any information in the System employs an invention claimed in any existing or later issued patent.

The information contained in the System is confidential and proprietary information intended for the use of authorized licensee's of the Cisco DTACS only. If you are not an authorized licensee of the Cisco DTACS, 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

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

OCAP is a trademark of Cable Television Laboratories, Inc.

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

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

Publication Disclaimer

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

This Cisco product contains, in part, certain free software ("Free Software") licensed under GNU General Public License (GPL), which allows you to freely copy, modify and redistribute the Free Software. Please go to

ftp://ftpeng.cisco.com/pub/opensource/scientificatlanta/settop/dta_30

to find additional information regarding the Free Software, including a copy of the GPL and related information. If you have any questions or problems accessing the link, please contact: spvtg-external-opensource-requests@cisco.com.

Additional Support and Resources

The following additional resources are also available to help you:

- ***Technical support*** (see "***Contact Us***" on page 6) from our service engineers or customer service representatives
- ***Printed resources*** (on page 9) 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.

Return Products for Repair

You must obtain a return material authorization (RMA) number before you send products to us for repair or upgrade. To return a product for repair or upgrade, complete the following steps.

1 Obtain the following information about the product that you want to return for repair or upgrade:

- The name and model number (if applicable) of the product and the quantity of returns
- A reason for the return, such as upgrade or failure symptom

- Your company name, contact, telephone number, email address, fax number, repair disposition authority, and any service contract details
- A purchase order number

  Notes:

  – If you are unable to issue a purchase order at the time you request an RMA number, a proforma invoice will be sent to you at the completion of repair. This invoice lists all costs incurred.

  – We must receive a purchase order within 15 days of receipt of proforma.

Important: In-warranty products can accrue costs through damage or misuse, or if no problem is found. Products incurring costs will not be returned to the customer without a valid purchase order.

2 Telephone or fax Factory Services at one of the following numbers to request an RMA number:

- From North America, call:
  – Tel: 1-800-722-2009
  – Fax: 770-236-5477
- From Europe, Middle East, or Africa, call:
  – Tel: 32-56-445-444
  – Fax: 32-56-445-051
- From Latin America, call:
  – Tel: 1-770-236-5662
  – Fax: 1-770-236-5888
- From Asia Pacific, call:
  – Tel: 852-2588-4746
  – Fax: 852-2588-3139

Result: The customer service representative will provide the RMA number and the shipping instructions to you.

Note: RMA numbers are only valid for 60 days. You must contact a customer service representative to revalidate your RMA numbers if the number is older than 60 days. After the RMA number is revalidated, you can return the product.

3 Pack the product in its original container and protective packing material.

Important:

- If the original container and packing material are no longer available, pack the product in a sturdy, corrugated box and cushion it with packing material that is appropriate for the method of shipping.
- You are responsible for delivering the returned goods to us safely and undamaged. Improperly packaged shipments, which may have caused additional damage, may be refused and returned to you at your expense.
- Do not return any power cords or accessories.

4 Write the following information on the outside of the container:

- Your name
- Your complete address
- Your Telephone number
- RMA number
- Problem description (for product failures)

Important: Absence of the RMA number may delay processing your product for repair. Include the RMA number in all correspondence.

5 Ship the product to the address you receive from the customer service representative.

Important: We do not accept freight collect. Be sure to prepay all shipments.

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 6). 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

The topics in this section can help you find information quickly and learn the basics about the DTA Control System (DTACS) and how it can help you manage your DBDS.

Navigation Tips

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

Use any of the following methods to find information you need in the DTACS 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

System

Introduction

This section describes how to configure the DTACS.

In This Chapter

Set up SCP

Before you can set up Simple Content Protection (SCP), you must create a package to hold the encrypted sources on the DNCS. Then you must sync the DTACS database with the DNCS database.

1. On the DNCS, create a package called **SCPnew**.
2. Add sources to the SCPnew package.
3. On the DTACS Admin Console, click **Sys Config**. The DTA Control System Configuration page opens.
4. Click **Sync DB** to sync the database. The SCPnew package will show up on the DTACS UI.
5. Click **Edit** to edit the DTA Control System configuration.

   Note: The checkbox beside SCP enabled should be selected. If it is not, contact Cisco Services to have SCP enabled.
6. In the DNCS Package field, select the **SCPnew** package that you created.
7. Click **Save**. All of the sources in the SCPnew package are available to DTAs for use.

System Configuration

The DTACS system was initially configured during installation. However, there might be times when your site needs to edit the configuration. This section describes how to configure some aspects of the system.

Important: Be very careful when changing your system configuration. You might want to consult with Cisco Services to be sure that the changes you are considering will not adversely affect your network.

System Configuration Settings

Use the following fields when you manage the DTACS system configuration.

Field	Description
Max Number of Virtual Channel Tables (VCT)	The maximum number of VCTs used with a DTA Control System.
Authentication Management Module (AMM)	
Use Universal Controller Location ID	Allows you to override the Location ID so that site announcement messages (site-announce AMMs) can be sent to the DTAs. When you select this option (so that a checkmark appears in the box), all Site Announcement messages from this DTACS are overridden with the Location ID of **0** (zero). This is a special case used for splitting or merging plants. Contact Cisco Services for more information.
Location ID	A unique identifier for a headend associated with a specific DTA Control System. This ID is inserted into Site Announcement broadcast messages and DTA Network Config unicast messages. **Note:** A Location ID of **0** (zero) is a special case used for splitting or merging plants. Contact Cisco Services for more information.
Packet ID (PID) (hex)	A hexadecimal value inserted in the header of each Authorization Management Message (AMM). This value indicates that the message contains AMM data.
Activation Timeout (hours)	The DTACS periodically sends this value to DTAs within AMM messages. This is known as refreshing the timeout value. ■ If a DTA receives timeout values within this specified time period (in hours), the DTA remains activated. ■ If a DTA does not receive timeout values within this time period, the DTA is deactivated. ■ Range of valid values is from 2 to 2880.

Field	Description
Provider Phone Number	The service provider phone number. This field provides a way to contact the headend operator. **Note:** You can use a maximum of 255 alphanumeric characters (excluding the ampersand) in this field.
UTC Offset	The time zone in which the DTA Control System is installed. This value must adhere to these formatting rules: 1 Minutes are expressed in 15-minute increments (for example, 00, 15, 30, 45). 2 The range of valid values is –14:00 to 12:00. 3 Values are formatted as **[–]HH:MM**, where: – [–] is optional and denotes time *behind* UTC – HH denotes hours - You **must** include both hour positions. If your offset is a single-digit hour (such as minus 7 hours), place a zero (0) before the single digit (-07:00). – MM denotes minutes - You **must** include both minute positions, even if both positions are zeros (00). 4 The offset can be positive (ahead of UTC) or negative (behind UTC). **Examples:** ■ An entry of **-05:00** means that your time zone is 5 hours behind UTC. ■ An entry of **02:00** means that your time zone is 2 hours ahead of UTC.
Use Daylight Saving Time (DST)	■ Enabled (checked) indicates that the system uses DST. ■ Disabled (unchecked) indicates that the system does not use DST.
Simple Content Protection (SCP)	
SCP Enabled	■ Enabled (checked) indicates that the system uses SCP. ■ Disabled (unchecked) indicates that the system does not use SCP. **Note:** This field cannot be edited in the DTACS. This field is set at installation.
DNCS Package	The DNCS package that uses SCP.
DTA Messaging Protocol	
Protocol	The type of messaging protocol the system uses. The two valid options are: ■ USP ■ Proprietary **Note:** This field cannot be edited in the DTACS. This field is set at installation.
Note: This screen also displays the last time the DTACS synced its database with the DNCS.	

Configuring the DTACS System

1. Click **Sys Config** in the System section. The DTA Control System Configuration window appears.
2. Click **Edit**. The DTA Control System Configuration window appears with editable fields for text entry and an 'Edit existing DTA System Configuration' message appears.
3. Configure the fields as described in System Configuration Settings.
4. Click **Save**.

Synchronize the DTACS Database

When you make changes in the DNCS that affect the DTACS, you need to synchronize the databases to move those changes to the DTACS database.

Synchronizing the DTACS Database

Follow these instructions to synchronize the DNCS and DTACS databases.

1. Click **Sys Config** in the System section. The DTA Control System Configuration window appears.
2. Click **Sync DB** to synchronize data in the DNCS database with data in the DTACS database. The 'DB Sync request processed successfully' message appears on the DTA Control System Configuration window.
3. Click **Back to Console** or click the **DTACS** link at the top of the window to return to the DTACS main page on any system configuration page.

Synchronization Failure

If you try to synchronize the DTACS database with the DNCS, and the synchronization fails, you need to update the /etc/hosts file on the DTACS server for the DNCS IP address.

Follow these instructions to update the /etc/hosts file.

1. Open an xterm window on the DTACS.
2. Open the **/etc/hosts** file in a UNIX text editor.
3. Locate the line that defines the dncsatm IP address. The line looks similar to the following:

   10.253.0.1 dncsatm
4. Amend the line to include the correct IP address for the dncsatm server.
5. Save and close the /etc/hosts file.

Provisioning GQAMs

The GQAM modulator takes the data it receives and, if necessary, it encrypts the data before modulating it onto an RF carrier for distribution to DTAs.

- The GQAM receives data on a Gigabit Ethernet (GbE) input.
- The GQAM modulator can also send the modified data out to the hubs on up to 16 transport streams.

Note: You do not provision the GQAM from the DTACS itself. GQAMs can only be provisioned from the DNCS. Follow the standard procedure for provisioning a GigE port found in the DNCS online help or in your GQAM documentation.

You Need to Know

Before You Begin

For More Information

For specific information on provisioning GQAMs for the DTACS, refer to the DNCS online help or to the installation and configuration guide for your specific version of the GQAM software.

Daylight Saving Time

From the DST Configuration window, you can create, change, and delete the daylight saving time (DST) rule used by DTAs in your DST zones. Setting up the right DST rule enables the DTAs in your system to automatically adjust to changes in DST observance.

Note: If your site does not observe daylight saving time, there is no need to use a DST rule.

- For additional information on this feature, refer to *Daylight Saving Time Configuration Guide for an RF Network* (part number 749233).

To obtain a copy of this publication, see ***Printed Resources*** (on page 9).

Daylight Saving Time Settings

Use the following fields when you manage the DST in the DTACS.

Important: Do not use an ampersand (**&**) in any text field. Using an ampersand in text fields will cause problems with the user interface.

Field	Description
Daylight Saving Time Zone	The name of the daylight saving time zone currently in use. Typically set up at installation, this field is not editable.
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. When a 0 (zero) is entered in this field, it indicates that the associated DST rule is to be ignored and not applied to the associated DST Zone ID. This field accepts any positive number from 0 to 1439.
Settings in the **Daylight Saving Time Start and End** area of the window define how DST is applied.	
Start: Month	The month the DST rule becomes effective.
Start: Day	The day the DST rule becomes effective.
Start: Day Rank in Month	The day of the month that the DST rule becomes effective. **Example:** The first, second, third, fourth, or last Sunday of the month.
Start: Hour	The hour the DST rule becomes effective.
Start: Minute	The number of minutes after the Start Hour that the DST rule becomes effective.
End: Month	The month the DST rule ends.

Field	Description
End: Day	The day the DST rule ends.
End: Day Rank in Month	The day of the month that the DST rule ends. **Example:** The first, second, third, fourth, or last Sunday of the month.
End: Hour	The hour the DST rule ends.
End: Minute	The number of minutes after the End Hour that the DST rule ends.

Editing the Daylight Saving Time Rule

Follow these instructions to edit the DST rule.

1. Click **DST Config**. The DTACS DST Configuration window opens.
2. Click **Edit**. The Daylight Saving Time Rules window opens with editable fields.
3. Edit the Daylight Saving Time rule as described in DST Settings.
4. Click **Save**.

3

Network Elements

Introduction

The DTA Control System provides a way to provision the following types of network elements:

- MPEG Internet Protocol (IP) streams
- Packet Identifier (PID) routes
- Virtual Channel Tables (VCTs)

In This Chapter

IP Stream Provisioning

Using the IP Stream Provisioning window, you can to configure streams carrying AMMs and SI data.

IP Stream Settings

Use the following fields when you manage IP streams in the DTACS.

Field	Description
Stream Type	Type of IP stream. Valid values are: ■ AMM ■ SI
Destination IP Address	The unique IP address associated with this stream.
Destination IP Port	The network port associated with this stream.
Data Rate (bps)	The data rate (in bits per second) that can be transmitted when using this stream.
Packet ID	The pre-defined packet identifier (PID) associated with the stream data.
Bcast Service Group ID	SI stream only. Select the broadcast service group (BSG) associated with this SI stream.

View IP Streams

Follow these instructions to view the IP streams available in the DTACS.

1 Click **IP Stream Management**. The IP Stream Management window opens.

2 Click the drop-down list in the **Query Streams** section and select the type of stream you want to view:

- All
- SI
- AMM

3 Click **Show**. The IP Streams List window opens, displaying the IP stream types you selected.

Add IP Streams

Follow these steps to add IP streams to the DTACS.

1 Click **IP Stream Management**. The IP Stream Management window opens.

2 Click the drop-down list in the **Add** section and select the type of stream you want to add:
   - SI
   - AMM
3 Click **Add**. The Add Stream window opens with editable fields.
4 Enter information as described in IP Stream Settings.
5 Click **Save**.

Edit IP Streams

Follow these instructions to edit IP streams in the DTACS.

1 Click **IP Stream Management**. The IP Stream Management window opens.
2 Click the drop-down list in the **Query Streams** section and select the type of stream you want to edit:
   - All
   - SI
   - AMM
3 Click **Show**. The IP Streams List window opens, displaying the IP stream types you selected.
4 Check the box next to the IP stream you want to edit, and click **Edit**. The Edit Stream window opens.
5 Edit the fields as described in IP Stream Settings.
6 Click **Save**.

Delete IP Streams

Follow these instructions to delete IP streams from the DTACS.

1 Click **IP Stream Management**. The IP Stream Management window opens.
2 Click the drop-down list in the **Query Streams** section and select the type of stream you want to delete:
   - All
   - SI
   - AMM
3 Click **Show**. The IP Streams List window opens, displaying the IP stream types you selected.
4 Check the box next to the IP stream or streams you want to delete, and click **Delete**. A confirmation window opens.
5 Click **OK**. The IP stream or streams are removed from the DTACS.

PID Route Provisioning

The PID Route Provisioning screen allows you to view and edit PID routes.

View a PID Route

Follow these instructions to view a PID route in the DTACS.

In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.

Note: If multiple pages of query results 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 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 .

Edit a PID Route

Follow these instructions to edit a PID route in the DTACS.

1 In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.

2 Select the PID route you want to edit and click **Edit**.

Notes:

- The MQAM Input ASI input port is the only element of the PID route you can edit.
- If no MQAM sources are present, the Edit button is unavailable.

3 Click **Save**.

User-Defined Sources for PID Routes (PassThru PID Routes)

There might be situations where you need to provision data sources for PID Routes (passthru PIDs) for PSIP, EAS, and other data, instead of using TSRs to pass the data through the entire transport stream.

Using passthru PID routes allows the data to flow through the QAM on carriers that contain DTA-related content. When you provision passthru PID routes for BSGs with active content, the DTACS sets up additional PID routes (AMM, SI/CVT with user-defined PID route sources) on each QAM carrier that contains DTA content.

Note: In earlier releases, service providers needed to use a third-party aggregator to combine EAS and PSIP streams. Beginning with DTACS 1.2, service providers can use the GQAM TSRs to pass the PSIP feeds, and use the PID route to specify the multicast address and source of external EAS source feed.

Before You Begin

PassThru PID Route Source Settings

Use the following fields when you manage passthru PID route sources in the DTACS.

Field	Description
Source Name	Enter the unique name of the source you are adding. This is an alphanumeric field.
Data Rate (bps)	Enter the data rate for the data being carried by the PIDs (in bps). Typically, this data rate is somewhere around 200,000 bps for the combined PSIP and EAS PIDs (100,000 bps for each.)
Destination IP Address	Enter the multicast IP address the QAM should join to get the PIDs, based on the following: ■ If you are using the PID for PSIP, this is the multicast address of the video feed. ■ If you are using the PID for EAS, this is the EAS multicast address.
Destination UDP Port	Enter the destination UDP port for the source (from 1 to 65535). **Note:** This is only required if the Destination IP address is a unicast address, rather than a multicast address.
BSG Name	Select the BSG associated with this source from the drop-down list.
Multicast Source IP Addresses	

Field	Description
1st Source IP Address	Enter the first multicast IP address for the source, if applicable. **Note:** If the destination IP address is multicast, then at least one source IP address must be specified.
2nd Source IP Address	Enter the second multicast IP address for the source, if applicable. Use this IP address if you are using source redundancy.
3rd Source IP Address	Enter the third multicast IP address for the source, if applicable. Use this IP address if you are using source redundancy.

Create a PassThru PID Route

Follow these instructions to add a passthru PID source to a PID route in the DTACS.

1. In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.
2. Click **View/Define Source**. The User Defined Sources for PID Routes window opens.
3. Click **Add**. The Add User Defined PID Route Source window opens.
4. Enter information as described in PassThru PID Route Source Settings.
5. Click **Save**. The DTACS creates the PID routes for the sources you entered.

Add a PassThru PID Definition to a User-Defined Source

Follow these instructions to add a passthru PID definition to a user-defined source in the DTACS.

1. In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.
2. Click **View/Define Source**. The User Defined Sources for PID Routes window opens.
3. Click **Manage Source PIDs**. The PID Definitions for User Defined Sources window opens.
4. Click **Add**. The Add PID Definition for User Defined Source window opens.
5. Select the **Source Name** from the drop-down list.
6. Enter an **Output PID**.
7. Click **Save**. The DTACS creates the PID definition for the source you selected.

Edit a PassThru PID Route Source

Follow these instructions to edit a passthru PID source in the DTACS.

1. In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.
2. Click **View/Define Source**. The User Defined Sources for PID Routes window opens.

3 Select the source you want to edit, and click **Edit**. The Edit User Defined PID Route Source window opens.

4 Edit the information as described in PassThru PID Route Source Settings.

5 Click **Save**. The DTACS creates the PID routes for the sources you entered.

Delete a PassThru PID Definition from a User-Defined Source

Follow these instructions to delete a passthru PID from a user-defined source.

1 In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.

2 Click **View/Define Sources**. The User Defined Sources for PID Routes window opens.

3 Click **Manage Source PIDs**. The PID Definitions for User Defined Sources window opens.

4 Select the PID definition you want to delete, and click **Delete**. A confirmation window opens.

5 Click **OK**. The PID definition is removed from the user-defined source and from the DTACS.

Delete a PassThru PID Route Source

Follow these instructions to delete a passthru PID source from the DTACS.

1 In the Network Elements section, click **PID Route Provisioning**. The PID Route Provisioning window opens, listing the PID routes available to the DTACS.

2 Click **View/Define Source**. The User Defined Sources for PID Routes window opens.

3 Select the source you want to delete, and click **Delete**. A confirmation window opens.

4 Click **OK**. The PID route source is removed from the DTACS.

VCT Provisioning

The VCT Provisioning screen allows you to manage Virtual Channel Tables (VCTs). The DTAs use the VCT ID to retrieve their associated SI data among other sets of data that might be available.

You can use the DTACS to view, add, edit, and delete VCTs.

VCT Settings

Use the following fields when you manage VCTs in the DTACS.

Field	Description
VCT Name	The name of the new VCT.
VCT ID	The ID of the new VCT. **Notes:** ■ The VCT ID is a hexadecimal number. ■ You cannot edit this field. To change the VCT ID, you must delete the VCT and re-create it with a new ID.
Package Set Name	If you are creating a package set, enter the name of the package set here. For more information, see ***Package Sets*** (on page 30).
Available Packages	Packages available in the DTACS for the VCT. Select a package in the Available Packages list and click **Add** to add that package to the Selected Packages list.
Selected Packages	Packages assigned to this VCT. Select a package in the Selected Packages list and click **Remove** to remove that package from the Selected Packages list.

View a VCT

Follow these instructions to view a VCT in the DTACS.

In the Network Elements section of the main page, click **VCT Provisioning**. The VCT Provisioning window opens, listing all the VCTs available in the DTACS.

Note: If multiple pages of query results 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 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 .

Add a VCT

Follow these instructions to add a VCT to the DTACS.

1. In the Network Elements section of the main page, click **VCT Provisioning**. The VCT Provisioning window opens, listing all the VCTs available in the DTACS.
2. Click **Add**. The Add VCT window opens.
3. Enter information as described in VCT Settings.
4. If you need to add package sets to the VCT, see ***Add a Package Set to a VCT*** (on page 30).
5. Click **Save**.

VCT and Channels in the DTACS

In the VCT, sources are listed in order by their ID.

If two sources are assigned to the same channel number over the span of multiple channel maps, the source with the lower-numbered Source ID is kept in the VCT and the remaining source is rejected.

Example: When source 60015 (with a Source ID of 936) and source 60017 (with a Source ID of 937) are assigned to channel 500 on two different DNCS channel maps, the DTACS will select source 60015 for channel 500 of the DTA.

Package Sets

Package sets are unique groups of packages available to specific VCTs. You can have as many as 10 package sets for each VCT in your system.

This section describes how to add package sets to a VCT and remove package sets from a VCT.

Add a Package Set to a VCT

1. Click **VCT Provisioning**. The VCT Provisioning window opens.
2. Select the VCT to which you want to add the package set.
3. Click **Edit**. The Edit VCT window opens.
4. Type a name for the package set in **Package Set Name**.
5. Select a package that this package set will contain in the Available Packages list and click **Add** to move the package to the Selected Packages list.

   Note: Hold the **Alt** key while clicking the packages to select multiple packages.
6. Click **Add** to add this package set to the VCT.
7. Click **Save** to save the changes to the VCT.

Remove a Package Set from a VCT

1. Click **VCT Provisioning**. The VCT Provisioning window opens.
2. Select the VCT that contains the package set you want to remove.
3. Click **Edit**. The Edit VCT window opens.
4. Select the package set you want to remove.
5. Click **Delete**. The package set is removed from the VCT.

Edit a VCT

Follow these instructions to edit a VCT in the DTACS.

1. In the Network Elements section of the main page, click **VCT Provisioning**. The VCT Provisioning window opens, listing all the VCTs available in the DTACS.
2. Select the VCT you want to edit and click **Edit**. The Edit VCT window opens.
3. Edit the fields as described in VCT Settings.

   Note: The VCT ID field is not editable.
4. If you need to add or remove package sets from the VCT, refer to one of the following topics:
   - ***Add a Package Set to a VCT*** (on page 30)
   - ***Remove a Package Set from a VCT*** (on page 30)
5. Click **Save**.

Delete a VCT

Follow these instructions to delete a VCT from the DTACS.

Note: You cannot delete a VCT if any DTA is associated with the VCT. You must delete the association before you can delete the VCT.

1. In the Network Elements section of the main page, click **VCT Provisioning**. The VCT Provisioning window opens, listing all the VCTs available in the DTACs.
2. Select the VCT you want to delete and click **Delete**. A confirmation window opens.
3. Click **OK**. The VCT is removed from the DTACS.

BSG Provisioning

The BSG Provisioning screen allows you to manage broadcast service groups (BSGs). A BSG is a group of QAM channels that service a subset of the DTA device population. A single QAM channel can be associated with a single BSG. All QAM channels within a BSG illuminate a single RF plant.

Note: BSG provisioning is also known as *QAM localization*.

You can use the DTACS to view, add, edit, and delete BSGs.

BSG Overview

Some sites do not have a single homogeneous RF downstream plant frequency plan. Consequently, sites with multiple frequency plans require a separate, unique set of SI data flows for each unique RF plan.

These RF plans are called downstream plant regions (DPR). These DPRs are referred to as a logical construct within the DTACS called broadcast service groups (BSGs). To support a video network with multiple DPRs, several constraints must be addressed.

- **Billing System:** The billing system associates a rate code with a specific service package. The service package is passed to the DTACS, which uses the package to define a set of services (channel lineups) for DTA client devices. However, service packages and their associated channel lineup information as defined on the billing system are not aware of any anomalies that may exist in the plant that affect delivery of those services. Therefore, locating the DTA client devices within the video network for the purpose of supplying it with a valid set of services is necessary.
- **VCT ID:** A video network with several different frequency plans (DPRs) needs to reuse the same VCT ID (authorization code) for each of these DPRs. However, the channel maps associated with a redundant VCT ID (which is used by more than one DPR) may have differing content.
- **QAMs:** For DTA client devices to located services on QAMs, all QAM carriers within a DPR must be associated with a single BSG. This means that no QAM RF channels are shared between two different BSGs. ("BSG straddle" is when a QAM carrier illuminates two BSGs. This is strictly forbidden.) All QAMs involved in delivering content to DTA client devices are assumed to be localized at the edge of the network.

BSG Settings

Use the following fields when you manage BSGs in the DTACS.

Field	Description
BSG Name	The name of the new BSG.
BSG ID	The ID of the new BSG. **Note:** This field is only editable when adding a new BSG. To change the ID of an existing BSG, you must delete the BSG then add it again with the new BSG ID.
Hub ID	Hub associated with the new BSG. **Note:** The Hub ID of **0** (zero) is the hub of the default channel map.
Available Ports	RF ports available in the DTACS for the BSG. Select an RF port in the Available Ports list and click **Add** to add that port to the Selected Ports list.
Selected Ports	RF ports assigned to this BSG. Select an RF port in the Selected Ports list and click **Remove** to remove that port from the Selected Ports list.

View BSGs

In the Network Elements section of the main page, click **BSG Provisioning**. The BSG Provisioning window opens, listing all the BSGs available in the DTACS.

Note: If multiple pages of query results 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 results.

  To use the Page control:

  – Enter the page number in the space provided and click  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  .

Add a BSG

Follow these instructions to add a BSG to the DTACS.

1. In the Network Elements section of the main page, click **BSG Provisioning**. The BSG Provisioning window opens, listing all the BSGs available in the DTACS.
2. Click **Add**. The Add BSG window opens.
3. Enter information as described in BSG Settings.
4. Click **Save**.
5. Your next step is to associate sources with the BSG. Go to ***Associate Sources With a BSG*** (on page 34).

Associate Sources With a BSG

1. Click **BSG Provisioning**. The BSG Provisioning window opens, listing all the BSGs available in the DTACS.
2. Select the BSG you are adding sources to (so that a checkmark appears in the box) and click **Associated Sources**. The Associate Sources window opens.
3. Select the VCT associated with this BSG in the VCT Name drop-down menu.
4. Select a source in the Available Sources list and click **Add** to add that source to the Selected Sources list.
5. Click **Save**.
6. Your next step is to provision a new SI IP stream associated with the BSG. Go to Setting Up IP Streams.

Edit a BSG

Note: The only fields that you can edit in an existing BSG are the BSG Name, Hub ID, and the Ports assigned to the BSG. To edit any of the other fields, you must delete the BSG and add it to the DTACS again.

1. Click **BSG Provisioning**. The BSG Provisioning window opens.
2. Select the BSG you you want to edit (so that a checkmark appears in the box) and click **Edit**. The Edit BSG window opens.
3. Edit the fields as described in BSG Settings.

   Note: The following fields are not editable:

   - BSG ID

- IP Address
- Port Number

4 Click **Save**.

Edit the Sources Associated With a BSG

1 Click **BSG Provisioning**. The BSG Provisioning window opens.

2 Select the BSG you want to edit (so that a checkmark appears in the box) and click **Associated Sources**. The Associate Sources window opens.

3 Edit the sources as required by following these instructions:

- **To add a source to the BSG,** select a source in the Available Sources list and click **Add** to add that source to the Selected Sources list.
- **To remove a source from the BSG,** select a source in the Selected Sources list and click **Remove** to remove that source from the Selected Sources list.

4 Click **Save**.

Remove Sources from a BSG

1 Click **BSG Provisioning**. The BSG Provisioning window opens.

2 Select the BSG you are removing sources from (so that a checkmark appears in the box) and click **Associated Sources**. The Associate Sources window opens.

3 Select a source in the Selected Sources list and click **Remove** to remove that source from the Selected Sources list.

4 Click **Save**.

Delete a BSG

1 Click **BSG Provisioning**. The BSG Provisioning window opens.

2 Select the BSG you want to delete (so that a checkmark appears in the box) and click **Delete**. A confirmation window opens.

3 Click **OK**. The BSG is removed from the DTACS.

4

Home Elements

Introduction

The Home Element Provisioning section of the DTACS main page allows you to manage Digital Terminal Adapters (DTAs) and Code Version Tables (CVTs).

This section describes how to provision home elements, including DTAs and CVTs.

In This Chapter

DTA Management

DTA devices support the conversion of analog basic and extended basic services into digital channels.

DTA Settings

Use the following fields when you manage DTAs in the DTACS.

Field	Description
Unit Address	The MAC address of the DTA you are adding.
VCT ID	Virtual channel table associated with this DTA.
Activation State	Indicates whether the DTA is active (on) or not (off).

View a DTA

Follow these instructions to view a DTA in the DTACS.

1. In the Home Element section on the DTACS main page, click **DTA Management**. The DTA Management window opens.
2. In the **DTA Filter**, enter a valid value (for the field in the By Field list box).
3. Click **Show**. The View DTA Entry List window opens.

   Note: If multiple pages of query results 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 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  .
- You can also sort the query results by clicking the table column headings (Unit Address, VCT, Activation State).

Add a DTA

Follow these instructions to add a DTA to the DTACS.

1. In the Home Elements section of the window, click **DTA Management**. The DTA Management window opens.
2. Click **Add**. The Add DTA Entry window opens.
3. Complete the fields as described in DTA Settings.
4. Click **Save**.

Edit a DTA

Follow these instructions to edit a DTA in the DTACS.

1. In the Home Element section on the DTACS main page, click **DTA Management**. The DTA Management window opens.
2. In the **DTA Filter**, enter a valid value (for the field in the By Field list box) for the DTA you want to edit.
3. Click **Show**. The View DTA Entry List window opens.
4. Select the DTA you want to edit and click **Edit**. The Edit DTA Entry window opens.
5. Edit the fields as described in DTA Settings.
6. Click **Save**.

Reset the NVM of a DTA

Follow these instructions to reset the non-volatile memory (NVM) of a DTA.

1. In the Home Element section on the DTACS main page, click **DTA Management**. The DTA Management window opens.
2. In the DTA Filter, enter a valid value (for the field in the By Field list box) for the DTA you want to reset.
3. Click **Show**. The View DTA Entry List window opens.
4. Select the DTA or DTAs you want to reset and click **Reset NVM**. A confirmation window opens.

5 Click **OK**. The DTACS resets the NVM of the DTA or DTAs.

Reboot a DTA

Follow these instructions to reboot a DTA using the DTACS.

1 In the Home Element section on the DTACS main page, click **DTA Management**. The DTA Management window opens.

2 In the DTA Filter, enter a valid value (for the field in the By Field list box) for the DTA you want to reboot.

3 Click **Show**. The View DTA Entry List window opens.

4 Select the DTA or DTAs you want to reboot and click **Reboot**. A confirmation window opens.

5 Click **OK**. The DTACS reboots the DTA or DTAs you selected.

Send Instant Hits

You can send an instant hit to a single DTA or to multiple DTAs.

1 In the Home Element section on the DTACS main page, click **DTA Management**. The DTA Management window opens.

2 In the DTA Filter, enter a valid value (for the field in the By Field list box) for the DTA that needs an instant hit.

3 Click **Show**. The View DTA Entry List window opens.

4 Select the DTA or DTAs that need an instant hit and click **Send Instant Hit**. A confirmation window opens.

Note: To select multiple DTAs, either use the **Shift** key or the **Ctrl** key and click multiple DTAs in the list.

5 Click **OK**. The DTACS sends an instant hit to the selected DTA or DTAs.

Delete a DTA

Follow these instructions to delete a DTA from the DTACS.

1 In the Home Element section on the DTACS main page, click **DTA Management**. The DTA Management window opens.

2 In the **DTA Filter**, enter a valid value (for the field in the By Field list box) for the DTA you want to delete.

3 Click **Show**. The View DTA Entry List window opens.

4 Select the DTA or DTAs you want to delete and click **Delete**. A confirmation window opens.

5 Click **OK**. The DTA or DTAs are removed from the DTACS.

CVT Provisioning

The DTACS web-based user interface allows you to provision Code Version Table (CVT) entries. The CVT is a table that contains information about download channels and information to map client release software versions to specific DTA types.

You can use the DTACS to query, add, edit, and delete CVTs.

CVT Settings

Use the following fields when you manage PID rates in the DTACS.

Field	Description
CVT Version 2 (CVT2) File Location	
Load CVT2 Image Metadata to File	The unique name of the CVT entry. This name appears in the File Path column on the CVT Management window.
Image Name	The name of the image file in the /dvs/dtacs/pub directory on the DTACS server.
Vendor ID	The vendor ID of the CVT in AABBCC format.
Hardware Version ID	The hardware vendor ID of the DTA in AABBCCDD format.
Transmission State	Determines whether this CVT is being transmitted. Select one of the following options: ■ Off ■ On
Location Type	Specifies the location of the download code. Select one of the following options: ■ Source ID ■ Frequency, Packet ID, Modulation Type ■ Frequency, MPEG Program Number, Modulation Type
Location Type dependent values	
Source ID	The source of the program.
MPEG Program Number	The MPEG program number that corresponds to this CVT.
Packet ID	The PID that corresponds to this CVT.

Field	Description
Frequency (MHz)	The frequency (in MHz) used to transmit the CVT to the DTAs. Valid values are in 0.25 MHz intervals.
Modulation Type	The type of modulation used for this CVT. Select one of the following options: ■ QAM 64 ■ QAM 256

View CVTs

Follow these instructions to view the Code Version Tables (CVTs) available in the DTACS.

1 In the Home Elements section of the main page, click **CVT Provisioning**. The CVT Entry Management window opens.

2 In the Query CVTs section of the window, select the type of CVT you would like to view and click **Show**. The CVT Entry Management screen changes to list the CVTs available in the DTACS.

Note: If multiple pages of query results 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 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 .

Add a CVT

Follow these instructions to add a CVT to the DTACS.

1. In the Home Elements section of the main page, click **CVT Provisioning**. The CVT Entry Management window opens.
2. Click Add. The Add Code Version Table (CVT) Entry window opens.
3. Enter information as described in CVT Settings.
4. Click **Save**.

Edit a CVT

Follow these instructions to edit a CVT in the DTACS.

1. In the Home Elements section of the main page, click **CVT Provisioning**. The CVT Entry Management window opens.
2. In the Query CVTs section of the window, select the type of CVT you would like to view and click **Show**. The CVT Entry Management screen changes to list the CVTs available in the DTACS.
3. Select the CVT you want to edit and click Edit. The Edit Code Version Table (CVT) Entry window opens.
4. Edit the information as described in CVT Settings.
5. Click **Save**.

Delete a CVT

Follow these instructions to delete a CVT from the DTACS.

1. In the Home Elements section of the main page, click **CVT Provisioning**. The CVT Entry Management window opens.
2. In the Query CVTs section of the window, select the type of CVT you would like to view and click **Show**. The CVT Entry Management screen changes to list the CVTs available in the DTACS.
3. Select the CVT you want to delete and click **Delete**. A confirmation window opens.
4. Click **OK**. The CVT is removed from the DTACS.

5

Common Download

Introduction

The Common Download area of the DTACS allows you to manage the common download carousel and DTA images.

This section describes how to configure the common download feature of the DTACS.

In This Chapter

Configure DTACS for Common Download

This section contains instructions on setting up the common download feature of the DTACS.

The procedure for setting up the common download on the DTACS is as follows:

1. ***Configure the DTACS Source on the DNCS*** (on page 46).
2. ***Configure the DTACS GQAM for Common Download*** (on page 47) or ***Add a DTACS GQAM for Common Download*** (on page 47).
3. ***Add a DTACS Carousel Source Definition to the DNCS*** (on page 48).
4. ***Synchronize the DTACS Database*** (see "***Synchronizing the DTACS Database***" on page 17).
5. ***Create the images Directory on the DTACS*** (on page 50).
6. ***Copy the Image Files to the images Directory*** (on page 50).
7. ***Configure the Common Download Carousel*** (on page 52).
8. Add an Image Association.

Configure the DTACS Source on the DNCS

This section describes how to set up a source on the DNCS for the DTACS carousel (also known as the dataPump).

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. On the DNCS tab, click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click one of the following:
   - For SR 4.4 and earlier, click **File > New**. The Set Up Source window opens.
   - For SR 4.5 and later, click **New**. The New Source window opens.
5. Click in the **Source Name** field and type the name you will use to identify this source. You can use up to 20 alphanumeric characters.

   Note: We recommend that you use a naming scheme that indicates that this source is the DTACS CDL carousel. For example, name the source **DTACS CDL Carousel**.
6. Click in the **Source ID** field and type the number you will use to identify this source. 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.
   - Write down the content source ID. You will need it as you continue to set up the service.

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

8 Do you have a GQAM set up for use with the DTACS common download?

- If **yes**, go to ***Configure the DTACS GQAM for Common Download*** (on page 47).
- If **no**, go to ***Add a DTACS GQAM for Common Download*** (on page 47).

Configure the DTACS GQAM for Common Download

This section contains instructions on how to configure your existing DTACS GQAM for common download.

Important:

- You must make sure that the GQAM has sufficient bandwidth available to modulate the DTA images to the DTAs, typically 1 to 2 Mbps.
- The GQAM that you use or set up must use the GbE connection to communicate to the headend.
- This procedure is for an existing GQAM that can be used for the DTACS common download feature. If you need to add a GQAM for this purpose, use the procedure in ***Add a DTACS GQAM for Common Download*** (on page 47).

Follow these instructions to configure the DTACS GQAM for common download.

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

2 On the DNCS tab, click the **Network Element Provisioning** tab.

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

4 Select the GQAM you are configuring and click one of the following:

- **For SR 4.4 and earlier**, click **File >Open**. The Set Up GQAM window opens.
- **For SR 4.5 and later**, click **Edit**. The Edit GQAM window opens.

5 Select an output port on the GQAM that has sufficient bandwidth available for modulating the DTA images to the DTAs (typically, 1 to 2 Mbps).

6 Write down this port number and frequency for later use.

Add a DTACS GQAM for Common Download

To add a DTACS GQAM for common download, follow the procedures in one of the following documents:

- *DNCS Online Help*

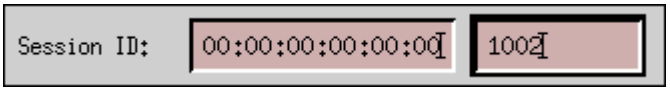
If you already have set up a GQAM for the DTACS, use the procedure in ***Configure the DTACS GQAM for Common Download*** (on page 47).

Add a DTACS Carousel Source Definition to the DNCS

This section contains instructions on how to add a DTACS carousel source definition to the DNCS.

Source Definition Settings

Use the following fields when you manage digital sources and sessions in the DNCS. In SR 4.4 and earlier, be sure to click **Next** to move between session screens.

Field	Description
Session ID	**Left Session ID** - The session MAC address. Type 12 zeros (the system inputs the colons for you).
	Right Session ID field - The source ID you used when you added the content source.
	Your final entry will look similar to the following example: 
Specify effective date and time	Allows you to define when subscribers can start viewing content from this source. Leave unselected so that the source becomes available immediately.
Define Session	Define the session programming. Select the **Multicast through a GQAM** option.
Bandwidth (Mbps)	The bandwidth available to this source. Typically, this will be 1 to 2 Mbps, defined by the limits of the DTA or by the bandwidth available on the GQAM.
QAM Name	Select the GQAM you configured for DTACS common download.
Output Carrier	The GQAM output port you defined for the DTACS common download.
Program Number	The MPEG program number (for example, 132).
Source IP Address 1	The IP address of the DTACS interface that the dataPump (DTACS carousel) uses to stream the DTA images.
Source IP Address 2	The second IP address of the DTACS interface that the dataPump (DTACS carousel) uses to stream the DTA images. If not used, leave empty.
Source IP Address 3	The third IP address of the DTACS interface that the dataPump (DTACS carousel) uses to stream the DTA images, if used. If not used, leave empty.
Image Destination Multicast IP Address	The unique (dedicated) multicast IP address that the dataPump (DTACS carousel) uses to send the image stream to. This multicast IP address is the address that the GQAM should join via the headend router to receive the image stream. **Important:** For this field, use a unique IP address; do not use the other DTACS multicast IP addresses (that support PID routes, SI, CVT, or AMM).

UDP Port	A user-selected, available, and non-reserved port number (for example, 2002).

Adding a Source Definition

1. On the DNCS Administrative Console, click the **DNCS** tab.
2. Click the **System Provisioning** tab.
3. Click **Source**. The Source List window opens.
4. Click once on the row containing the service source you need to define and click one of the following:
   - **For SR 4.4 and earlier**, click **File > Source Definitions**. The Source Definition List window opens for the source you selected.
   - **For SR 4.5 and later**, click **Source Definitions**. The Source Definition List window opens for the source you selected.
5. Click one of the following:
   - **For SR 4.4 and earlier**, click **File > New Digital**. The Digital Source Set Up window opens.
   - **For SR 4.5 and later**, click **New Digital**. The New Digital Source window opens.
6. Enter the Session ID for this session.
   - The left part of the Session ID is the session MAC address. Type 12 zeros (the system inputs the colons for you).
   - The right part of the Session ID is the source ID you used when you added the DTACS source.
7. If you need to specify when this source will become active, select **Specify effective date and time** to enter that information. If left unselected (unchecked), the source will become available immediately.
8. Click **Next**. The Define Session window opens.
9. Select the **Multicast through a GQAM** option.
10. Click **Next**. The Multicast Digital Session Definition window opens.
11. Enter the information on this screen as defined in Source Definition Settings.
12. Click **Save**. The source is listed in the Source List and should display as active.

Synchronizing the DTACS Database

Follow these instructions to synchronize the DNCS and DTACS databases.

1. Click **Sys Config** in the System section. The DTA Control System Configuration window appears.

2. Click **Sync DB** to synchronize data in the DNCS database with data in the DTACS database. The 'DB Sync request processed successfully' message appears on the DTA Control System Configuration window.
3. Click **Back to Console** or click the **DTACS** link at the top of the window to return to the DTACS main page on any system configuration page.

Create the images Directory on the DTACS

Your next step is to create the images directory on the DTACS, so you can store the DTA code files (also known as images) on the DTACS.

1. Log into the DTACS as root.
2. Type **cd /dvs/dtacs/dtacsFiles** and press **Enter**. The dtacsFiles directory becomes the working directory.
3. Type **mkdir images** and press **Enter**. The system creates the images directory in the dtacsFiles directory.

Copy the Image Files to the images Directory

Your next step is to copy the image files to the images directory you just created.

1. Obtain the DTA image files as per your site's standard procedure.
2. Copy the image files into the /dvs/dtacs/dtacsFiles/images directory.

Carousel Configuration

This section contains information regarding the configuration of the common download carousel.

Carousel Configuration Settings

Use the following fields when you manage the Common Download carousel in the DTACS.

Field	Description
Image Storage Directory	Defines the download file path where the image is stored on the DTACS (/dvs/dtacs/dtacsFiles/images). You can use up to 128 characters in this field.
Data Rate (bps)	Determines the maximum data rate (in bps) the DTACS can use to distribute the image. **Valid values:** Between 1 and 5,000,000 bps. **Recommended values:** Between 1000000 and 2000000 bps.
Block Size (bytes)	Determines the maximum size of the blocks (in bytes) that the carousel transmits to DTAs. **Valid values:** Between 1024 and 1257 bytes. **Recommended value:** 1024. **Important:** This value must not exceed the system MTU.
Destination IP Address	The unique (dedicated) multicast IP address defined for the dataPump (DTACS carousel) GQAM session.
Destination IP Port	The port number defined for the dataPump (DTACS carousel) GQAM session. **Valid values:** Between 1024 and 65535.
Program Number	The MPEG program number defined for the dataPump (DTACS carousel) GQAM session. **Example: 132**.
Location Type	Specifies the location of the download code. Select one of the following options: ■ Source ID ■ Frequency, Packet ID, Modulation Type
Location Type dependent values	
Source ID	The source ID for the download. This field is active if you selected **Source ID** in the **Location Type** field.

Field	Description
MPEG Program Number	The MPEG program number of the download. This field is active if you selected **Frequency, Packet ID, Modulation Type** in **Location Type** field.
Frequency (MHz)	The frequency of the download. This field is active if you selected **Frequency, Packet ID, Modulation Type** in **Location Type** field. **Maximum value:** 16383.75 MHz.
Modulation Type	The type of modulation standard this download uses. This field is active if you selected **Frequency, Packet ID, Modulation Type** in **Location Type** field. ■ QAM 64 ■ QAM 256

View the Common Download Carousel Configuration

Follow these instructions to view the common download carousel settings in the DTACS.

In the Common Download section of the main page, Click **Carousel Config**. The DTACS Common Download Configuration window opens that lists the configuration of the common download carousel.

Configure the Common Download Carousel

Follow these instructions to configure the common download carousel in the DTACS.

1. In the Common Download section of the main page, Click **Carousel Config**. The DTACS Common Download Configuration window opens.
2. Click **Edit**. The Edit DTACS Common Download Configuration window opens.
3. Edit information as described in Carousel Configuration Settings.
4. Click **Save**.

Image Association

This section contains information on image associations in the DTACS.

Image Association Settings

Use the following fields when you manage image associations in the DTACS.

Field	Description
Image Name	Select the name of the image file you are associating from the drop-down list. **Note:** This is the only field that is editable after the association has been created.)
Vendor ID	Select the distributor of the image file from the drop-down list. **Example:** Cisco is **8762**.
Hardware ID	Select the correct hardware ID for the DTAs that will receive this image. **Example:** For DTA30s, select **1600**.
Download Command	Select **Immediate**. **Note:** This field only displays when you are adding or editing an image association.

Adding an Image Association

Follow these instructions to add an image association to the DTACS.

1. Click **Image Association**. The DTA Image Association Management window opens.
2. Click **Add**. The Add DTA Image Association window opens.
3. Complete the fields on the screen as described in Image Associations Settings.

   Important: With some versions of DTACS software, the software requires a Unit Address, even though a Unit Address is not mandatory. If you see this behavior, follow these instructions to clear this requirement:

   a. In the Unit Address section, check the **Address** box.

   b. Click **Delete Address**.

   c. Click **Save**.
4. Click **Save**. The system saves the information in the DTACS database and displays the DTA Image Association Management window.

   Notes:

- Saving this image association should create a CVT file in the /dvs/dtacs/pub directory on the DTACS. The DTACS sends this CVT information out every minute on the SI IP stream to all the active DTACS PID routes.
- The dataPump (DTACS carousel) session should appear as active on the GQAM output, as seen from the GQAM front panel.
- If you used the Source ID Location Type in the DTACS Carousel configuration, each DTA must have a VCT assigned to it. This VCT must contain the hidden channel (as viewed using the DTA Virtual Channel Map diagnostic screen) that contains the Source, Frequency, and MPEG Program information for the dataPump session.

  If the hidden channel does not appear in the DTA's VCT, then modify any VCT on the DTACS and save it. This forces the DTACS to rebuild the VCT SI data. The hidden channel should then appear on the DTA.

5 Click **Exit** to close the DTA Image Management window.

Edit an Image Association

The only field you can edit in an image association is the Image Name field. To change any other fields, you must delete the image association and add a new one to the DTACS.

Follow these instructions to edit an image association in the DTACS.

1 Click **Image Association**. The DTA Image Association Management window opens.

2 Select the image association you want to edit (check the box in the row of the image association) and click **Edit**. The Edit DTA Image Association window opens.

3 Select a new **Image Name** for the image association from the drop-down list.

4 Click **Save**. The information is saved to the DTACS database and the Edit DTA Image Association window closes.

5 Click **Exit** to close the DTA Image Association Management window.

Delete an Image Association

Follow these instructions to delete an image association from the DTACS.

1 Click **Image Association**. The DTA Image Association Management window opens.

2 Select the image association you want to delete (check the box in the row of the image association) and click **Delete**. A confirmation window opens.

3 Click **OK**. The information is removed from the DTACS database.

4 Click **File > Quit** to close the DTA Image Association Management window.

Vendor and Hardware ID

This section contains information regarding the configuration of the vendor and hardware IDs for DTA images.

Adding a Vendor and Hardware ID

Follow these instructions to add a vendor and hardware ID to the DTACS.

Note: You cannot edit a vendor and hardware ID after you create it. To change the information in a vendor and hardware ID, you must delete the ID and add it to the DTACS again.

1. Click **Vendor and Hardware ID**. The DTA Vendor and Hardware ID Management window opens.
2. Click **Add**. The Add Vendor and Hardware ID window opens.
3. Type the appropriate information in the following fields:
   - **Vendor ID:** Type the hexadecimal number associated with the vendor in the AABB format.
   - **Hardware ID:** Type the hexadecimal number associated with that vendor's hardware ID in the AABB format.
4. Click **Save**. The Add Vendor and Hardware ID window closes and the ID you added displays in the DTA Vendor and Hardware ID Management list.

Deleting a Vendor and Hardware ID

Follow these instructions to delete a vendor and hardware ID from the DTACS.

Note: You cannot edit a vendor and hardware ID after you create it. To change the information in a vendor and hardware ID, you must delete the ID and add it to the DTACS again.

1. Click **Vendor and Hardware ID**. The DTA Vendor and Hardware ID Management window opens.
2. Select the line that contains the ID that you want to delete (so that a checkmark appears in the box).
3. Click **Delete**. A confirmation window opens.
4. Click **OK**. The ID is removed from the DTACS database.

6

System Monitoring

Introduction

To maintain a healthy system, you need to periodically monitor the DTACS.

This section provides information that allows you to monitor the DTACS.

In This Chapter

The Admin Console

You can monitor and change the status of DTACS processes from the Administrative Console. The console allows you to view the overall status of DTACS. You can also choose to view or change the status of the ***DTACS processes*** (on page 59).

DTACS Processes

This section describes the processes running on the DTACS and contains instructions on how to start and stop those processes.

Monitoring DTACS Processes

You can monitor all of the major DTACS processes by opening the Process Status window from the DTACS Admin Console. The Process Status window provides a list of all the major processes on the DTACS workstation, along with the ***working state*** (see "***Working States of DTACS Processes***" on page 61) of each.

Description of DTACS Processes and Dependencies

The following table describes the processes and their dependencies listed on the DTACS Control window.

Important: Every DTACS process depends on the logManager and the eventManager processes for debug log management and event distribution.

Process	Description	Dependencies
ammDistributor	Transmits 'refresh' AMMs to the DTAs.	■ dtacsIpStreamer - AMMs are submitted as 'send once' messages. Stopping ammDistributor will stop the transmission of refresh messages. ■ ammdistributor_datarate - Environment variable that controls the bandwidth of the AMM stream. Values between 20 - 80 are valid. **Note:** The fewer DTAs in your system, the more often the ammDistributor will send the refresh messages.
dataPump	The dataPump transmits encoded DTA images for the download carousel.	ocdlManager - Manages this process depending on the image download configuration.
dtacsBossProxy	Implements the backend processing of BOSS transactions not supported by the DTACS.	No additional dependencies.
dtacsBossServer	Provides the BOSS interface to the DTACS.	■ dtaManager - For DTA-related BOSS transactions. ■ dtacsBossProxy - For unsupported BOSS transactions.

Process	Description	Dependencies
dtacsCvtMgr	Provides a web services (SOAP) interface to manage the CD2-CVT file and the transmission of CD2-CVT. Also provides the ability to provision locally generated CVTs on the DTACS.	dtacsIpStreamer - CVTs are submitted as 'repeat send' messages. Stopping dtacsCvtMgr will not stop the transmission of CVTs previously submitted to the dtacsIpStreamer.
dtacsIpStreamer	Transmits data supplied by other DTACS processes as MPEG elementary streams to specified IP addresses (multicast or unicast).	No additional dependencies.
dtacsNeMgr	Provisions and maintains network element configuration for PID routes, DTA CAT insertion, and SCP MPK insertion.	■ dtacsIpStreamer - IP stream update events. ■ dtacsUIServer - Configuration update events. ■ dtacsSiManager - Source update events.
dtacsSiManager	Generates SI and Channel Map data for transmission.	dtacsIpStreamer - SI data is submitted as 'repeat send' messages. Stopping dtacsSiManager will not stop the transmission of SI data previously submitted to dtacsIpStreamer.
dtacsUIServer	Provides the mechanism for displaying the user interface for the DTACS.	Depends on the following processes for UI-related data: ■ dtacsBossServer ■ dtacsCvtMgr ■ dtacsIpStreamer ■ dtacsNeMgr ■ dtacsSiMgr ■ dtaManager ■ ocdlManager

Process	Description	Dependencies
dtaManager	Provisions and manages DTA devices.	dtacsIpStreamer - AMMs are submitted as 'send once' messages. Stopping dtaManager will stop the transmission of DTA AMM updates triggered from the DTA Mgt UI and Billing System activity.
eventManager	An internal support process that provides a generalized mechanism for event notifications.	No additional dependencies.
logManager	An internal support process for managing debug logging levels of DTACS processes.	No additional dependencies.
ocdlManager	OCAP Common Download Manager. Manages carousel setup and images the OCAP CDL.	dtacsCvtMgr - For insertion of CVT.
scpManager	Initializes and monitors the SCP key server and generates SCP AMMs.	No additional dependencies.

Working States of DTACS Processes

A colored square indicates the working state of a particular process as described in the following list:

- Green — The process as a whole is running, although a subprocess may be paused.
- Yellow — The process has not finished starting up or shutting down, or is waiting on a subprocess to finish starting up or shutting down.
- Red — The process has stopped or did not start.

After the DTACS 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. Contact Cisco Services if a process continually remains in a red or yellow state.

WARNING: Do **NOT** attempt to start or stop a DTACS process manually unless a Cisco Services representative specifically tells you to do so. Otherwise, you could disrupt service to your subscribers.

Starting and Stopping Services

This section contains instructions on how to start and stop services on the DTACS.

Starting Services

Follow these instructions to start a service.

1. From the DTACS main window, click the **Admin Console** tab.
2. Click one of the following, depending on how you want to display the services:
   - **Show** - displays the services in the same window as the DTACS.
   - **Pop-out** - displays the services in a separate window from the DTACS.

   Results: The Process Status window displays.
3. Select the service you want to start and click **Start**. After a few moments, the color of the status indicator will turn green.

Stopping Services

Follow these instructions to stop a service.

1. From the DTACS main window, click the **Admin Console** tab.
2. Click one of the following, depending on how you want to display the services:
   - **Show** - displays the services in the same window as the DTACS.
   - **Pop-out** - displays the services in a separate window from the DTACS.

   Results: The Process Status window displays.
3. Select the service you want to stop and click **Stop**. After a few moments, the color of the status indicator will turn red.

Process Status Update Response Time

When you start or stop a DTACS service, the DTACS server should respond within about 5 seconds. If the server takes longer than about 5 seconds to respond that a service has started or stopped, you can change the process status update response time.

The process status update response time is controlled by the UI_POLL_INTERVAL parameter in the dtacsInitd.cfg file.

Changing the Process Status Update Response Time

Follow these instructions to change the process status update response time.

1. Log into the DTACS server as dtacs user.
2. Open an xterm window on the DTACS server.
3. Type **cd /dvs/dtacs/etc/** and press **Enter** to make the /etc directory the working directory.
4. Open the **dtacsInitd.cfg** file in a text editor.
5. Locate the **UI_POLL_INTERVAL** line. The parameter value listed in this line is listed in milliseconds (ms).

   Example: If the line shows UI_POLL_INTERVAL=20000, then the polling interval is set to 20 seconds.
6. Change the parameter value to one that better reflects your workflow.

   Important: We recommend that you set this parameter to a value that is not less than **4000** (4 seconds) for the best results.
7. Save and close the dtacsInitd.cfg file.
8. In the xterm window, type **dtacsKill dtacsInitd** and press **Enter** to stop the dtacsInitd process.
9. Once the dtacsInitd process has stopped, type **dtacsStart** and press **Enter** to start all processes again.
10. To ensure that your DTACS session uses the latest value, close and re-open your DTACS browser session.

7

Emergency Alert System

Introduction

This section describes the workings of the Emergency Alert System (EAS) in the DTACS network.

In This Chapter

EAS With the DTACS

The DNCS generates in-band EAS messages on every QAM that carries at least one unencrypted service.

EAS messages are received by an EAS receiver, which sends all EAS messages directly to the DNCS. The DNCS receives the EAS messages and forwards them to the out-of-band modulators, for the benefit of legacy devices.

The DNCS also forwards the EAS messages to each enabled QAM for the benefit of clear QAM tuners. The QAMs multiplex the EAS messages into the in-band transport stream. The DTA uses the in-band EAS facility of the DNCS.

The DNCS enables in-band EAS based on the "Default Host" channel map. Any QAM that carries one or more clear services, as listed in the "Default Host" channel map, also carries in-band EAS messages.

Note: The Default Host channel map is different from the "Default" channel map. The Default Host channel map must be enabled for EAS to work with the DTACS.

8

Configure the Network Time Protocol

Introduction

This chapter explains how to synchronize the Network Time Protocol (NTP) on the DTACS Server with the timer on the DNCS.

In This Chapter

Configuring the NTP

Configuring the NTP Server

Complete the following steps to sync the NTP server on the DTACS Server with the time server on the DNCS server.

1 Open an xterm window.

2 Type **pgrep -lf ntp** and press **Enter** to verify that xntpd is not running before you continue.

- If xntpd *is* running, a message like the following will appear: `1136 /usr/local/xntpd/ntpd -c /etc/inet/ntp.conf -p /etc/ntp.pid -l /var/adm/log/ntp`
- If xntpd is *not* running, nothing will appear after you enter the command.

3 As root user, type **/usr/local/xntpd/ntpdate -d <IP of NTP Server>** and press **Enter** to verify network connectivity to the NTP server.

Example:

```
# /usr/local/xntpd/ntpdate -d 10.253.0.1
```

Notes:

- Use the DNCS as the NTP server. This keeps the DTACS time in sync with the DNCS. The DNCS should already be configured to use an NTP server.
- You may have multiple NTP servers.

Results: The system should respond with both transmit and receive packets followed by time information sent from the NTP server. If the final line of the output states "no server suitable for synchronization found," then either a problem exists with the NTP server or a network issue is preventing a connection. Verify the IP address with your Network Administrator and attempt the command listed above again. If you are still unable to resolve this problem, contact Cisco Services for assistance.

4 Type **su -** and press **Enter** to change to root.

5 Use the vi editor to add the NTP server IP's to the /etc/hosts file. Add the IP and hostname of each NTP server. For example:

```
10.253.0.1      dncsatm
```

Notes:

- There should already be a dncsatm entry in the /etc/hosts file.
- You can also include additional NTP server entries in the /etc/hosts file.

6 Type **cd /etc/inet** and press **Enter** to change to the /etc/inet directory. The /etc/inet directory becomes the working directory.

7 Type **cp ntp.conf ntp.conf.bak** and press **Enter** to make a copy of the existing ntp.conf file.

8 Use the vi editor to edit the ntp.conf file so that the first lines contain an entry for each NTP server that you choose to use.

Example:

```
server dncsatm mode 10 prefer
server 127.127.1.0 #local clock will engage if GPS fails
fudge dncsatm stratum 13
driftfile /etc/ntp.drift
```

Note: Simply replace the IP address with the NTP server name defined in the /etc/hosts file.

9 Type **:wq!** to save these changes and exit the vi editor.

10 Type **/etc/init.d/xntpd stop** and press **Enter** to stop the ntpd process.

11 Type **/etc/init.d/xntpd start** and press **Enter** to re-start the ntpd process.

12 Type **pgrep -fl ntp** and press **Enter** to verify the ntpd process is running.

Example:

```
29840 /usr/local/xntpd/ntpd -c /etc/inet/ntp.conf -p /etc/ntp.pid -l
/var/adm/log/ntp
```

13 Type **ntpq** and press **Enter** to display the ntpq prompt.

14 Type **peers** and press **Enter** to verify the DNCS is the clock being used.

Example:

```
     remote           refid      st t when poll reach   delay   offset    disp
==============================================================================
 LOCAL(0)        LOCAL(0)         5 l   21   64  377     0.00    0.000    0.94
*dncsatm         10.90.176.136    4 u   28   64  377     1.46  -15.339    0.94
```

Notes:

- The appearance and content of the results will vary according to your System release version.
- The asterisk (*) in front of the dncsatm (as shown in the above example) indicates that the DTACS is using the DCNS ATM as a reference clock and that the DTACS server is synchronized to the DNCS.
- Important: If the asterisk (*) is in front of LOCAL, then the DTACS is not synchronized to the DNCS. It is synchronized with the hardware clock on the server. This situation must be corrected immediately.

15 At the ntpq> prompt, type **lass** and press **Enter**.

Results: A result similar to the following examples appear on the screen.

Example:

```
ind assID status  conf reach auth condition  last_event cnt
===========================================================
  1 27724  9014   yes   yes  none    insane   reachable  1
  2 27725  9614   yes   yes  none  sys.peer   reachable  1
```

Note: The device numbers listed in the first column of the following output correspond with the devices listed in the ntpq> peers output from the example in step 13.

16 Use the date command on the DNCS and DTACS servers to verify the time on both servers.

DNCS Example:

Mon Nov 23 15:36:46 EST 2009

DTACS Example:

Mon Nov 23 15:31:15 EST 2009

Note: In this example above, the DTACS time is 5min 31sec behind the DNCS. NTP will automatically synchronize the servers once the time difference is less than two minutes.

17 If you need to synchronize the servers, type **date hhmm.ss** (where hhmm.ss is the target time on the DNCS) and press **Enter** to reset the DTACS time. The DTACS time is reset to match the DNCS.

Example: # date 1536.46

9

DTACS Security

Introduction

This section contains information about security used on the DTACS Server. This includes information about user accounts, password expiration rules, and role-based access control.

In This Chapter

Operating System Defaults

- **Operating System:** Solaris 10
- **Security Features:**
  - **Secure by Default** - OS is installed with minimal network services
  - **Networking**
    - SSH is the only network listening service installed by default for remote access; others are set to off or configured for only local machine access
    - X11 forwarding is also enabled for remote UI access using SSH
  - **Restricted Network Resources** - Authorized users have access to all network resources, but the system itself has very little exposure to the network, making unauthorized access very difficult
  - **System Monitoring** - Basic Security Module (BSM) provides monitoring of system events for logging and auditing

Operating system defaults are set up during system installation.

Important: We recommend that you do **not** change the system defaults to retain the highest level of system security. Cisco Systems, Inc. is not responsible for any damage that might occur to your DNCS or DBDS if you choose to change the system defaults.

Role-Based Access Control

Prior to the implementation of the Security Enhancements on the DNCS, the dtacs user account was the only account required to accomplish almost any task associated with the DNCS system. These tasks include access to the DNCS GUI suite, the DNCS database, the DNCS file system, diagnostic scripts, logging, and the command line.

Like DNCS, we have implemented role-based access control as part of the DTACS operating system. This access control allows system administrators to assign specific administrative control of parts of the system to users.

You can give users permissions to run certain commands or access to certain files. You can also prevent users from running commands or accessing files. Role-based access control allows increased flexibility in the assignment of permissions on the system.

The following table lists the three most important roles and account types available on the DTACS and a description of their permission levels.

Role	Files		Commands	Database		
	Read	Write	Execute	Read	Write	Alter
Root	Y	Y	Y	Y	Y	Y
DTACS Role	Y	Y	Y	Y	Y	N
DTACS Admin Account	Y	N	N	N	N	N

This section is a more detailed description of the roles and accounts available on the DTACS Server.

root User

The root user is the system administrator account and has all privileges and rights.

- Login access to the system using the root user is limited to direct local access, such as from the local console.
- You can switch to the root user from another account that is logged in locally or remotely.
- You must use the root user to create all customer-specific login accounts.
- The root user has permission to switch to the dtacs role.
- The root user is the database administrator.

dtacs Role

The dtacs role is the DTACS application administrator and user.

- You should perform all DTACS application activities (including starting and stopping the DTACS applications, DTACS GUI access, DTACS application file management, DTACS diagnostic script execution, and DTACS log configuration) using the dtacs role.
- You must use the dtacs role to start the Administrative Console.
- Access to the dtacs role is limited to the root user and DTACS Administrator accounts. These are the only accounts with permission to switch to the dtacs role.
- You cannot login directly to the DTACS using "dtacs" and the dtacs role password.

DTACS Administrator

DTACS Administrator accounts are the only system accounts (other than root) that have permission to switch to the dtacs role.

- These accounts are created when needed by the DTACS system administrator using the create_users script.
- These accounts can be used on the DTACS only to view logs and other application files.

System Access

- Can log into the DTACS Server operating system (Solaris)
- Can read but cannot write DTACS Server files
- Cannot execute DTACS Server applications
- Can switch to the dtacs role

DTACS Operator

DTACS Operator accounts can be used on the DTACS only to view logs and other application files.

- These accounts are created when needed by the DTACS system administrator using the create_users script.
- These accounts do not have permission to switch to the dtacs role.

System Access

- Can log into the DTACS Server operating system (Solaris)
- Can read but cannot write DTACS Server files

- Cannot execute DTACS Server applications
- Cannot switch to the dtacs role

Regular Users

Regular User accounts do not have permission to view DTACS logs or other application files.

- These accounts are created when needed by the DTACS system administrator using the create_users script.
- These accounts do not have permission to switch to the dtacs role.

System Access

- Can log into the DTACS Server operating system (Solaris)
- Cannot read or write DTACS Server files
- Cannot execute DTACS Server applications
- Cannot switch to the dtacs role

User Accounts

This section describes how to create and delete user accounts.

Creating a User Account

1. Open an xterm window on the DTACS Server.
2. Log into the DTACS Server as root.
3. Type **cd /dvs/dtacs/etc** and press **Enter**.
4. Type **create_users** and press **Enter**.
5. Select one of the following user types:
   - Add Regular User
   - Add Operator
   - Add Administrator

   Notes:
   - See User Account Defaults for more information on the user types.
   - Users who require access to the DTACS interface should be granted Administrator privileges; otherwise, their functionality is severely limited.
6. Type the name of the new user account and press **Enter**.

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

   Result: The **Do you wish to continue adding this user (Y/N)?** message appears.
7. Type **y** (for yes) and press **Enter**.
8. Type the **password** for the user and press **Enter**.
9. Re-type the **password** for the user and press **Enter**. The create_users program exits.

Deleting a User Account

Important: Even when you delete a user, the user name still exists in the password history file. We do **not** recommend that you edit this file. If you delete a user, then add the same user again, that user's old password history remains in effect. Thus, the new account will not be able to change the password to any of the previous 5 passwords used by the old account.

Use this procedure to delete users that were added using the create_users script.

1. Log into the DTACS Server as root.

2 Review the user files in the user's home directory and move any files that should be retained to another directory, outside the user's home directory.

3 In an xterm window, type **userdel -r [username]** and press **Enter**. The system deletes the user's home directory.

Note: Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

4 Type **projdel user.[username]** and press **Enter**. The system removes the user from the /etc/project file.

Note: Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

5 Is the user you are deleting a Regular User?

- If **yes**, type **groupdel [username]** and press **Enter**. The system deletes the group associated with that user.

  Note: Substitute the user's name for [username]. Do not type the brackets **[ ]** in the command.

- If **no**, you are finished with this procedure.

Database Access

The following permissions are set up by default on the DTACS database:

root user: DBA, connect, resources

dtacs role: Connect and only insert, delete, select, and update on tables

dtacsSSH: Connect and select on tables only

public: No access

1 Open an xterm window on the DTACS Server.

2 Log into the DTACS Server as dtacs user.

3 Type **listdbusers** and press **Enter**. A list similar to the following displays:

```
Privileges for tbl_based_ses_data :
User         Select             Update             Insert  Delete  Index
Alter
dtacs          All                All                Yes     Yes     No
No
dtacsSSH       All                None               No      No      No
No


Privileges for ted :
User         Select             Update             Insert  Delete  Index
Alter
dtacs          All                All                Yes     Yes     No
No
dtacsSSH       All                None               No      No      No
No
```

```
Privileges for transport_defaults :
User         Select             Update             Insert  Delete  Index
Alter
dtacs          All                All                Yes     Yes     No
No
dtacsSSH       All                None               No      No      No
No

Privileges for ts_downstream :
User         Select             Update             Insert  Delete  Index
Alter
dtacs          All                All                Yes     Yes     No
No
dtacsSSH       All                None               No      No      No
No
```

Note: The list has been shortened for purposes of illustration.

Who Am I?

To determine who is logged into a session, you can type one of the following from the DTACS Server command line and press **Enter**:

- **id**
- **/usr/ucb/whoami**

Note: If you add /usr/ucb to your default path, you only need to type whoami and press **Enter**.

Result: The system returns the user ID of the user currently logged into the session.

Session Security

The DTACS Server will close a user session that has been idle for a configurable period of time. After a session is closed, users must log back into the system.

- Session locking default time: 30 minutes (1800 seconds)
- Recovery: User logs in again

Notes:

- The session locking time does not affect the root user.
- Session locking also affects SSH, xterms, consoles on the CDE, and shells launched during a session.

Change the Session Timeout Default for a User

Follow these instructions to change the session timeout default for a user.

1. Open an xterm window on the DTACS Server.
2. Type **cd /export/home/[user account]** and press **Enter**.
3. Open the **.profile** file in a UNIX text editor.
4. Add the following line to the .profile file:

   export TIMEOUT=[seconds]

   Notes:

   - Do not type the brackets **[ ]** in the command.
   - Enter the time as a number of seconds.

     Examples:

     – To enter a session locking time of **5 minutes**, change the field to **export TIMEOUT=300**

     – To enter a session locking time of **15 minutes**, change the field to **export TIMEOUT=900**

   - We recommend that you keep the session locking time to as short a time as possible. This helps prevent unauthorized use of your system.
5. Save the .profile file and close the text editor.
6. In the xterm window, type **. ./.profile** and press **Enter**. The system will use the updated .profile file.

Note: Be sure to type a space between the first two periods.

Override Session Limitations

Follow these instructions to override the session limitations for a user.

1. Log into the DTACS as root.
2. Type the following command and press **Enter**:

   projmod -K 'project.max-tasks=(priv,x,deny)' user.[username]

   Note: The **x** in (priv,x,deny) is the number of active sessions the user is allowed to have open at a time.
3. Substitute the user name for **[username]**. Do not type the brackets **[ ]** in the command.

Password Management

Regardless of password management rules enforced by a system, users must still be encouraged to choose difficult to guess passwords. Proper system management of passwords is important but the primary responsibility for strong passwords ultimately rests with the user.

Password Guidelines

Users must select a very strong password. Strong passwords have the following general characteristics:

- Contain 8 or more characters
- Contain at least 2 alphanumeric characters and at least one numeric or special character
- Do **not** consist of only one character type (**aaaaaaa** or **11111111**)
- Do **not** contain any aspects of a date
- Are **not** proper names
- Are **not** telephone numbers or similar numeric groups
- Are **not** user IDs, user names, group IDs, or other system identifiers
- Do **not** contain more than two (2) consecutive occurrences of the same character
- Are **not** consecutive keyboard patterns (for example, **qwerty**)

System Password Retention

The system sets the following restrictions on re-using passwords:

- The system retains the last 5 passwords each user uses.
- The system does not allow you to re-use any of the last 5 passwords each user has used.

Change User Account Passwords

We recommend that you change the default passwords for the root and for the dtacs role at a minimum to increase the security level on the DTACS. Our recommendations for other account passwords are as follows:

- **informix account:** Changing the informix account password is not necessary since this account is locked by default.

- **dtacsSSH account:** Changing the dtacsSSH account password is not necessary since this user is not directly used by an operator, and the default password is either not known or documented.
- **easftp and dtacsftp accounts:** These account passwords should be done only in coordination with the administrator of the EAS and the VOD systems.

A user account password can be changed by the user or by the system administrator.

Changing Your Own Password

Note: You can change your own account password. Only administrators can change other users' account passwords.

1. Open an xterm window on the DTACS Server.
2. At the login prompt, type **passwd -r files** 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 DTACS Server.
8. Login to the DTACS Server with your new password.

Changing Another User's Password

Note: Only administrators can change other users' account passwords.

1. Open an xterm window on the DTACS Server.
2. Log into the DTACS Server as root.
3. Type **passwd -r files [username]** and press **Enter**.

   Example: Type **passwd -r files jonesx** and press **Enter**.
4. Type the new password for the user and press **Enter**.
5. Type the **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. Have the user log out of the DTACS Server.
8. Have the user login to the DTACS Server with the new password. If you used the **-f** option, the user must enter the one-time password you created. Then, the system prompts the user to create a new password.

Changing the Root Password

Note: Only administrators can change other users' account passwords.

1. Open an xterm window on the DTACS Server.
2. Log into the DTACS Server as root.
3. Type **passwd -r files root** and press **Enter**.
4. Type the new password for the root user and press **Enter**.
5. Type the new password again and press **Enter**. The system changes the root password.

Password Expiration Period

By default, the system requires that all user accounts change their passwords after 13 weeks. The system also displays a warning 2 weeks before the deadline. After that time, if the user has not changed their account password, the user account is locked.

Important: This expiration period is applicable to **all** users, including root, dtacsSSH, informix, dtacsftp, easftp, any custom accounts, and the dtacs role.

- Default number of weeks a password is valid: 13
- Default time period from password expiration the user receives a warning message to change passwords: 2
- Recovery: Administrator must reset the user account by changing the password

You can change or disable the password expiration period applied when adding new users or changing passwords, and change or disable an individual user's password expiration period.

You can change the password expiration period applied when creating new users or changing passwords.

Important:

- New users added to the DTACS after the password expiration period has changed automatically inherit the new password expiration period.
- Existing users' individual expiration periods remain in force until the user's password is changed (either by an administrator or by the user).
- Unless the system password expiration period is disabled, all user accounts will inherit the system password expiration period each time they change their passwords, even if the user's expiration period has been disabled.
- If you set the value of MAXWEEKS to -1, you disable password expiration.

Changing the System Password Expiration Period

Use this procedure to change the password expiration period for the entire system.

1. Open an xterm window on the DTACS Server.
2. Log into the DTACS Server as root.
3. Type **cd /etc/default** and press **Enter**.
4. Open the **passwd** file in a UNIX text editor.
5. Locate the following line in the passwd file:

   export MAXWEEKS=13
6. Change the expiration period to the number of weeks that you prefer.

   Note: We recommend that you keep the expiration period as short as possible. This helps prevent unauthorized use of your system.
7. Locate the following line in the passwd file:

   export WARNWEEKS=2
8. Change the warning period to the number of weeks that you prefer.
9. Save the passwd file and close the text editor.
10. Type **exit** and press **Enter** to close the xterm window.

Important:

- New users added to the DTACS after the password expiration period has changed automatically inherit the new password expiration period.
- Existing users' individual expiration periods remain in force until the user's password is changed (either by an administrator or by the user).
- Unless the system password expiration period is disabled, all user accounts will inherit the system password expiration period each time they change their passwords, even if the user's expiration period has been disabled.
- If you set the value of MAXWEEKS to -1, you disable password expiration.

Changing a User's Password Expiration Period

1. Open an xterm window on the DTACS.
2. Log into the DTACS Server as root.
3. Type **passwd -r files -x –1 [account name]** and press **Enter**.

   Notes:

   - Type the username for **[account name]**.
   - Do not type the brackets **[ ]** in the command.
4. Verify the expiration period by typing **passwd -s [username]** and press **Enter**.

   Example: Type **passwd –r files –s dtacs** and press **Enter**. The system displays a message similar to the following:

   ```
   dtacs     PS
   ```

```
user      pw_status      date          MIN     MAX     WARN
```

Note: Only PS should be listed after the account name for an account with a disabled expiration period. If numbers appear after the PS, repeat step 4.

5 Type **exit** and press **Enter** to close the xterm window.

Important: Unless the system password expiration period is disabled, all user accounts will inherit the system password expiration period each time they change their passwords, even if the user's expiration period has been disabled.

10

Troubleshooting

Introduction

This section contains information about procedures you can use to troubleshoot issues on the DTACS Server.

In This Chapter

Correcting Java Errors in Firefox

You may have to stop the tomcat process and clear the Firefox cache if you experience java errors:

Example:

```
"An error occurred in http://localhost:8045:/dtacs/dta/dta.js:136  tform.uid
has no properties."
```

You must perform the following tasks to correct this java error:

- Exit out of the DTACS WUI
- Change to the root userid
- Stop the tomcat process
- Remove all files from the Firefox cache directory
- Restart the tomcat process
- Stop using the root userid
- Start the DTACS WUI

Stopping the Tomcat Process

Follow these steps to stop the Tomcat process on the DTACS Server:

1. Select **File > Exit** on the DTACS WUI.
2. Type **su - root** to change to the root userid.
3. Type the password for the root user at the password prompt.
4. Type **/export/home/informix/bin/formatDbSpace.sh** and then press **Enter**. The system formats the database partitions.
5. Type **cd /etc/rc2.d** to change to the /etc/rc2.d directory.
6. Type **./S98tomcat stop** to stop the tomcat process.

Removing Files from the webui Directory

Follow these steps to remove files from the webui work directory on the DTACS Server:

1. Type **cd /dvs/dtacs/webui/work** at the root prompt to change to the webui work directory.

> **CAUTION:**
>
> **Verify that you are in the correct directory (/dvs/dtacs/webui/work/) before you type the next command.**
>
> **When you type the next command you will delete all files in the directory.**

2 Type **pwd** at the prompt to verify that you are in the webui work directory. The directory name appears at the system prompt.

3 Type **rm -rf*** at the root prompt to remove all files from the webui work directory.

Starting the Tomcat Process

1 Type **cd /etc/rc2.d** to change to the /etc/rc2.d directory.

2 Type **./S98tomcat start** to start the tomcat process.

3 Type **exit** to stop using the root userid. The system prompt displays.

Clearing the Firefox Cache

1 Type **cd /export/home/dtacs/.mozilla/** at the root prompt to change to the mozilla directory.

2 Type **ls** at the prompt to verity that the firefox directory exists.

3 Type **cd firefox** to change to the firefox directory

4 Type **ls** to view all files in the firefox directory. Note the name of the ******.default directory.

Note: The asterisks (*******) are place holders for the first part of the .default filename.

5 Type **cd *******.default** to change to the default directory.

6 Type **ls** to view the contents of the default directory. Verify that the Cache directory exists.

7 Type **cd Cache** to change to the Cache directory.

8 Type **ls** to view the contents of the Cache directory.

> **CAUTION:**
>
> **Verify that you are in the Firefox Cache directory (/export/home/dtacs/.mozilla/firefox/*******.default/Cache/) before you type the next command.**
>
> **When you type the next command you will delete all files in the directory.**

9 Type **pwd** at the prompt to verify that you are in the Firefox Cache directory. The directory name appears at the system prompt.

10 Type **rm -rf *** to remove files in the directory.

11 Type **ls** at the prompt to verify that all files have been removed from the directory.

12 Start the DTACS WUI.

Note: After restarting tomcat, wait for few minutes before opening DTACS WUIs. The tomcat server takes several minutes to restart and bind to the DTACS WUI interface.

Channels Not Displaying in Available Sources List for BSG

If a channel/source is not displaying in the BSG Associate Sources Available Sources list, make sure that the source is present in the hub-specific channel map on the DNCS.

The Hub ID you assigned to the BSG must have that source in its channel map on the DNCS for that source to display in the Available Sources list.

The Source is in the Channel Map

If the source is in the correct channel map on the DNCS, synchronize the DTACS database. The source should display in the list.

The Source is Not in the Channel Map

If the source is not in the correct channel map on the DNCS, follow these instructions:

1. Add that source to the hub channel map in the DNCS.
2. Wait for the DNCS SAM to generate a new POD_Data file and distribute it (check with your system administrator as to the appropriate amount of time).
3. Synchronize the DTACS database. The source should display in the list.

DTA Time Zone Value is Not Populated

If you realize that the Time Zone value of your DTAs is not populated (generally after an NVM reset or an instant hit), make sure that you follow the UTC Offset guidelines described in ***System Configuration Settings*** (on page 15). The data for that field must be entered exactly as described or the DTAs will not recognize the value.

Check DTACS IP Streams

You can check the IP streams as they leave the DTACS to verify that they are routed correctly and that the SI and AMM streams are transmitting data.

Important: These commands may change depending on your network setup. Contact your system administrator for more information.

Check the System Information IP Stream

Follow these instructions to check the SI IP stream.

1 Log into the DTACS as root user.

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

snoop -v -x0 -d e1000g0 host [SI_DEST_IPADDR] port [SI_DEST_IPPORT]

Notes:

- Substitute the system information message destination IP address for **[SI_DEST_IPADDR]**.
- Substitute the system information destination IP port for **[SI_DEST_IPPORT]**.
- Do not type the brackets in the command.
- To log the data to a file, append the following to the command:

  2>&1 [path/filename]

  where **path** is the path to the directory where you want to save the log, and **filename** is the name of the log file.

Results: If data is flowing, you will see a series of hexadecimal numbers. If you see no output, there may be a problem.

Check the AMM IP Stream

Follow these instructions to check the Authorization Management Message (AMM) IP stream.

1 Log into the DTACS as root user.

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

snoop -v -x0 -d e1000g0 host [AMM_DEST_IPADDR] port [AMM_DEST_IPPORT]

Notes:

- Substitute the AMM destination IP address for **[AMM_DEST_IPADDR]**.
- Substitute the AMM destination IP port for **[AMM_DEST_IPPORT]**.
- Do not type the brackets in the command.

- To log the data to a file, append the following to the command:

  2>&1 [path/filename]

  where **path** is the path to the directory where you want to save the log, and **filename** is the name of the log file.

Results: If data is flowing, you will see a series of hexadecimal numbers. If you see no output, there may be a problem.

Index

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 4036706 Rev A