DTA Control System 1.2 Installation and Operation Guide

Please Read

Important

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

Notices

Trademark Acknowledgments

- Cisco and the Cisco logo are trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: **www.cisco.com/go/trademarks**.
- Third party trademarks mentioned are the property of their respective owners.
- The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1009R)

Publication Disclaimer

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

Copyright

Contents

Chapter 7 Provision DTACS 81

Chapter 8 Configure the Network Time Protocol 131

Chapter 9 Customer Information 135

Appendix A Managing DTACS User Accounts 137

Appendix B Troubleshooting the DTACS Server 153

Appendix C Backup and Restore the DTACS File System and Database 157

Appendix D DTACS Rollback Procedure 173

About This Guide

Introduction

This guide provides installation and operational information for the Digital Transport Adaptor Control System (DTACS) software application. The DTACS application manages and controls Digital Transport Adaptors (DTAs). DTAs are hardware components used within the DBDS network to convert digital channels into analog services. The DTACS application, combined with DTAs, allow Multiple System Operators (MSOs) to support customers who use standard definition televisions to access cable services.

Purpose

This guide provides step-by-step instructions for installing the DTACS software on the DTACS platform for the first time. This guide also provides steps to upgrade to a new version of software.

Audience

This guide is written for field service engineers, system operators and operations personnel who are responsible for the initial installation and upgrades of DTACS software.

Read the Entire Guide

Please review this entire guide before beginning the installation. If you are uncomfortable with any of the procedures, contact Cisco® Services at 1-866-787-3866 for assistance.

Important: Complete all of the procedures in this guide in the order in which they are presented. Failure to follow all of the instructions may lead to undesirable results.

Required Skills and Expertise

System operators or engineers who install the Download Server software need the following skills:

- Knowledge of UNIX
- An understanding of network IP addresses

Download Manuals

Sun Microsystems has made several Sun Netra T5220 and T5440 manuals available on the Internet. Download the *Sun Netra™ T5220 Server Service Manual* (part number 820-3012-12 , copyright July, 2008, Revision A) and other Sun Netra™ manuals from the following websites:

- http://docs.sun.com/app/docs/coll/netra-t5220?l=en
- http://docs.sun.com/app/docs/coll/netra-t5440?l=en

Should Sun Microsystems update the manuals, however, you may find discrepancies between the procedures in this book and those in the Sun documentation. In this case, the more recent version should supersede the older version.

Document Version

This is the fourth formal release of this document. In addition to minor text and graphic changes, the following table provides the technical changes to this document.

Description	**See Topic**
Update the procedures to restore the DTACS file system	***Backup and Restore the DTACS File System and Database*** (on page 157)

1

DBDS Service Delivery Network

Introduction

This chapter explains how the DTACS Server fits into the Digital Broadband Delivery System (DBDS) service delivery network. This chapter also describes the how the DTACS Server works with elements of the Digital Network Control System (DNCS).

In This Chapter

DBDS Components

Overview of the Service Delivery Network

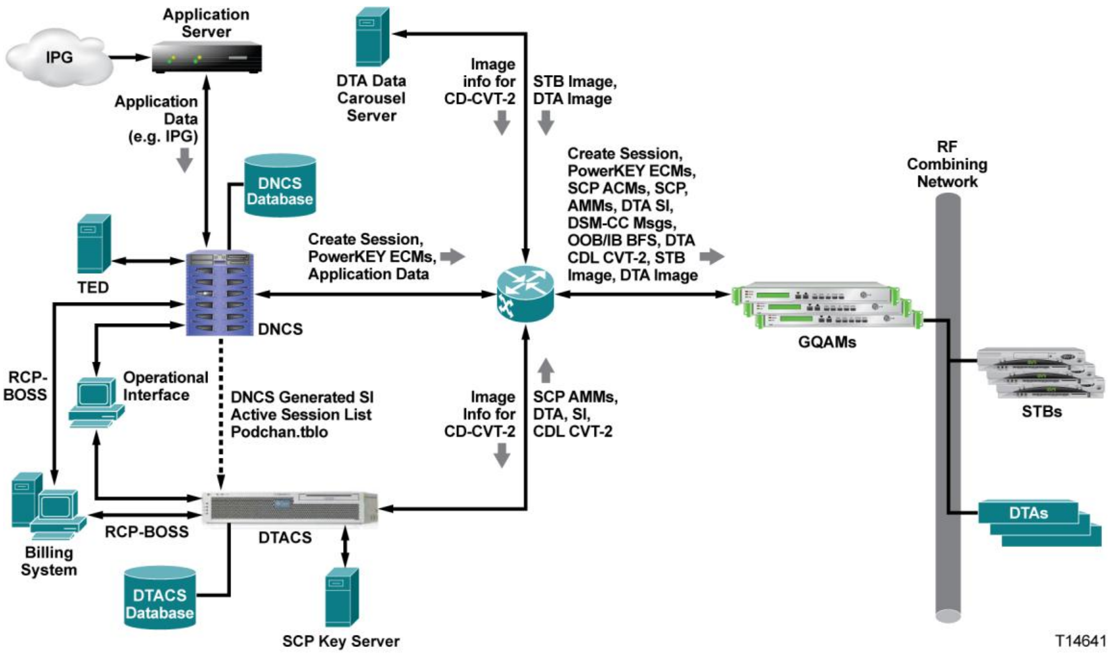
The DBDS is a network of hardware and software elements that delivers video, audio, digital data, and applications to a service provider's subscribers. The DNCS manages and provides information about elements in the network.

A Digital Transport Adapter (DTA) is a device that allows subscribers to view digital content on an analog cable-ready television without the use of a set-top box. The DTACS Server works with the DNCS to deliver content to Digital Transport Adapters (DTAs) in a subscriber's home.

DTACS software resides on the DTACS Server and allows MSOs to perform the following tasks:

- Configure the DTACS Server to work with the DNCS
- Synchronize the DTACS database with elements of the DNCS database
- Start, stop and monitor processes running on the DTACS Server
- Provision and manage DTA units

The following diagram illustrates the architecture of the DTACS Server and shows how it works with elements of the DNCS.


IPG
Application Server
Application Data (e.g. IPG)
DTA Data Carousel Server
Image info for CD-CVT-2
STB Image, DTA Image
DNCS Database
TED
DNCS
Create Session, PowerKEY ECMs, Application Data
Create Session, PowerKEY ECMs, SCP ACMs, SCP, AMMs, DTA SI, DSM-CC Msgs, OOB/IB BFS, DTA CDL CVT-2, STB Image, DTA Image
RF Combining Network
GQAMs
STBs
RCP-BOSS
Operational Interface
DNCS Generated SI Active Session List Podchan.tblo
Image Info for CD-CVT-2
SCP AMMs, DTA, SI, CDL CVT-2
Billing System
RCP-BOSS
DTACS
DTACS Database
SCP Key Server
DTAs
T14641

2

Before You Begin

Introduction

This chapter provides procedures which must be completed on the DNCS before installing and configuring the DTACS.

In This Chapter

Update DNCS

You must perform the following tasks on the Digital Network Control System (DNCS) before you install DTACS software:

- Log in to the DNCS as a **root** user
- Create a dtacs user on the DNCS server
- Add dtacshost information to the /etc/hosts and/etc/hosts.equiv files
- Verify that your system meets the software requirements

Log on to DNCS

Follow these steps to log on to the DNCS.

1 Log on to the DNCS console as a **dncs** user. The password prompt appears.

2 Type the password for the dncs user. The Solaris Common Desktop Environment (CDE) desktop appears.

3 Open an xterm window and change to a **root** user. An xterm window opens and a password prompt for the root user appears.

Example:

```
$ xterm -sb -sl 100000 -e su - &
```

4 Type the password for the **root** user and press **Enter**. The prompt for the root user (#) appears.

Create a DTACS User on DNCS

Follow these steps to create a dtacs user on the DNCS server.

1 Type **useradd -u 503 -g500 -c "dtacs user" -d/export/home/dtacs -s /bin/ksh -m -k/etc/skel dtacs; passwd dtacs -K lock_after_retries=no** at the prompt.

Results:

- A dtacs user is created on the DNCS server
- A home directory (/export/home/dtacs) is created for the dtacs user on the DNCS server
- The New Password prompt appears

2 Type the new password for the dtacs user and press **Enter**. A prompt to retype the password appears.

3 Type the password again and press **Enter**.

Add dtacshost Entry to Files

Follow these steps to update the /etc/hosts and /etc/hosts.equiv files.

1. On the DNCS, open the **/etc/hosts** file using your favorite editor. The editor displays the contents of the /etc/hosts file.
2. Type the following line at the end of the file.

   <ipaddress> dtacshost dtacs

   Notes:

   - Substitute the IP address of the machine for <ipaddress>
   - Press the Tab key after you type the IP address
3. Save your changes to the file and exit the editor.
4. Open the **/etc/hosts.equiv** file using your favorite editor. The editor displays the contents of the /etc/hosts.equiv file.
5. Type the following lines at the end of the file and press **Enter** at the end of each line:

   dtacshost dtacs

   dtacshost dncs

   dtacshost root
6. Save your changes to the file and exit the editor.
7. On the DTACS, open the **/etc/hosts** file.
8. Type **#** at the beginning of the following line to comment the line out:

   <ipaddress> appservatm appserv_host ppv_manager_host vc_server_host config_manager_host
9. Save your changes to the file and exit the editor.

Verify Software Requirements

You must verify that the correct versions of software are installed on the QAMs and on the DNCS server. The following list shows the versions of software that must be installed and operating correctly:

- MQAM software must be version 2.7.0.2 or greater
- GQAM software must be version 4.3.9 or greater
- DNCS software must be version 4.3.0.14p5 and any applicable emergency patches approved for your site.

Note: These are *minimum* software versions. Your versions may be higher.

To check the software versions, type **pkginfo -l [packagename] |grep VERSION** and press **Enter**.

Example:

```
$ pkginfo -l SAImqam |grep VERSION
VERSION 2.7.0
```

You must also verify that the package structure on DNCS corresponds to the service tiers you plan to make available to the DTAs.

Source Definition Requirement

GQAMs and MQAMs using specified software versions must be the only QAMs used for sources that will be offered to DTAs.

Set Up QAM Sessions

Set Up GQAM Sessions

The GQAM modulator receives data on a Gigabit Ethernet (GbE) input and, if necessary, encrypts the data before modulating it onto an radio frequency (RF) carrier for distribution to DTAs. The GQAM modulator can also send the modified data to network hubs on up to 16 transport streams.

Before you install software on the DTACS Server, you should log in to the DNCS and set up sessions on the GQAM. These sessions will be used on the DTACS Server.

Consider the following before you begin provisioning GQAMs on the DNCS:

- You must provision the GigE port of the GQAM for use with the DTACS
- If your network uses hubs, the DTACS GQAM and its frequencies need to be available to all the hubs in the network
- Though you can use any frequencies available to the GQAM, the following frequencies are the most efficient for use with DTAs:

Type	EIA	Frequency (Mhz)
STD	81	567
STD	82	573
STD	83	579
STD	84	585
STD	85	591
STD	100	651
STD	101	657
STD	68	489
STD	69	495
STD	126	807
HRC	81	564.0282
HRC	82	570.0285

Note: To enable DTAs to boot quickly, some of the DTACS channels should be one of these frequencies.

Modify Ports on the Router

Contact your system administrator to find out which GQAM will be used for DTACS sessions. This GQAM will display content on the DTA and its frequencies should be plant-wide. These frequencies will not be used on a specific hub.

After you obtain this information, you must perform the following steps.

1. Enable GigE GQAM ports for IP PIM sparse-mode.
2. Enable GigE GQAM ports for IP IGMP Version 3.
3. Enable multicast routing on DNCS VLAN on the router.

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 GQAM software release.

Back Up the System

If you are upgrading an existing DTACS, you should back up the file system to tape and back up the database before you begin. Follow the procedures in this section.

Note: This section only includes basic instructions for backing up and restoring the system. If you need more detailed instructions or backup options, refer to *DBDS Backup and Restore Procedures For SR 2.2 Through 4.3 User Guide* (part number 4013779).

Back Up the File System to Tape

Use this procedure to back up the DTACS file system to tape.

Note: Skip this section if you are installing a new DTACS.

Important: An external tape device should be attached to your DTACS and should be powered on.

1. Insert the maintenance DVD into the DVD drive of the DTACS.
2. Type **df -n** and press **Enter**. Verify that /cdrom is listed in the list of mounted file systems that appears.
3. Label a blank tape with the following information:

   [DTACS Server] File System Backup [Date]
   [Site Name]
   [Software Version]
   [DTACS Maintenance DVD x.x.x]
4. Insert the blank tape into the tape drive of the DTACS Server and wait for the green light to stop flashing.
5. As root, type **devfsadm** and press **Enter**.
6. Type **mt status** and press **Enter** to confirm that the tape is attached.
7. Type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v** and then press **Enter**. The system backs up the DTACS Server file system, ejects the tape, and displays a message when the backup is complete. This process may take up to an hour to complete.
8. When the backup is complete, remove the tape and store it in a safe place.

Back Up the Database

Use this procedure to back up the DTACS database to tape.

Notes:

- Skip this section if you are installing a new DTACS.

- The DTACS Server can be running while you back up the Informix database.
- It may take up to 30 minutes to back up the database.
- The external tape drive should be connected to your DTACS server.

1 Insert the DTACS DVD into the DVD drive.

2 From a root xterm window, type **df -n** and then press **Enter**. A list of the mounted filesystems appears.

Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.

3 Label your backup tape with the following information:

[DTACS Server] Database Backup [Day of the Week]

[Site Name]

[Software Version]

DTACS DVD [version]

[Tape #]

Notes:

- Customize the label with the day of the week, site name, and software version for the site you are backing up.
- If your database backup requires more than one tape, be sure to note the tape number on the label.

4 Insert the tape into an external tape drive that has been connected to the DTACS Server.

Type **/cdrom/cdrom0/s3/backup_restore/backupDatabase -v** and then press **Enter**. The system instructs you to mount tape 1 on /dev/rmt/0h and then press **Return** to continue.

5 Press **Enter**. The system backs up your Informix database.

Notes:

- The message "Successfully completed the database backup" appears when the backup has completed successfully.
- If the database backup was not successful, the system displays an error message. Call Cisco Services at 1-866-787-3866 for assistance in resolving the error message.

6 Remove the tape and store it in a safe place.

3

Installing the DTACS Software for the First Time

This chapter describes the Sun Netra T5220 and T5440 servers, on which you will install the DTACS software. In addition, this chapter contains procedures for installing DTACS software for the first time on the system.

Notes:

- The Sun Netra T5220 and T5440 servers were tested by Telcordia Technologies, Inc. and were given the Telcordia Network Equipment Building Standards (NEBS) Level 3 certification.
- If you are upgrading DTACS software at a site that already supports DTACS, go to either ***Upgrade the DTACS Server Software Using a DVD*** (on page 45) or ***Upgrade the DTACS Server Software Using CDs*** (on page 53), as appropriate.

In This Chapter

Introducing the DTACS Servers and the ILOM Port

The DTACS Servers

We have chosen the Sun Netra T5220 and T5440 servers for the DTACS platform. These servers use Sun's UltraSPARC T2 processors and Solaris architecture, and are designed to easily mount within a standard computer rack.

These servers are configured with the following components.

Sun Netra T5220	Sun Netra T5440
Up to eight core 1.2-GHz UltraSPARC T2 processors	Up to eight core 1.2-GHz UltraSPARC T2 Plus processors; two processors per system
16 slots with up to 64 GB memory	32 slots with up to 128 GB memory
2 x 146 GB hard drives	12 x 146 GB hard drives
Integrated Lights Out Manager Management	Integrated Lights Out Manager Management
Four 10/100/1000 Mbps Ethernet ports	Four 10/100/1000 Mbps Ethernet
Serial Management Port	Serial Management Port
Network Management Port	Network Management Port
2 eight-lane PCIe slots	10 PCI slots: 8 PCIe
4 four-lane PCIe slots	2x PCI-Express slots
2 PCI-X slots	2 PCI-X slots
Two hot-swappable power supplies	Four 2+2 redundant, hot-swappable power supplies

Taken as a whole, the serial management port and the network management port of the DTACS servers constitute the Sun Integrated Lights Out Management (ILOM) port. The ILOM port is a system controller that allows the servers to be managed and administered from remote locations. Through the ILOM port, you can monitor and control the servers through a serial connection (using the SERIAL MGT port) or an Ethernet connection (using the NET MGT port).

Important: Your DTACS server should have the appropriate video and SCSI cards installed before the unit is ever shipped to you. Contact Cisco Services if these cards have not yet been installed.

Log On to the DTACS Server

Important: These instructions assume that the DTACS server has not yet been configured.

Complete the following steps to connect a laptop to the DTACS server and configure the network management port.

1 Connect a laptop computer to the serial management port of the DTACS server.

2 Start the HyperTerminal application on the laptop and configure the application with the following parameters:

Note: The HyperTerminal application allows one computer to communicate with another computer.

- Baud rate-9600
- Data bits-8
- Parity-none
- Stop bit-1
- Flow control-no

Note: You must connect your laptop to the serial management port on the DTACS server to configure the server's network management port.

3 If necessary, power on the DTACS server.

4 From the login prompt on the terminal, log on with the username **root** and the password **changeme**. The -> prompt appears. This is the prompt for the ILOM command line interface (CLI).

5 Do you want to change the ILOM root password?

- If **yes**, type set **/SP/users/root password** and press **Enter**. Go to step 6.
- If **no**, go to ***Configure the Service Processor Network Management Port*** (on page 14).

6 When prompted, enter the new password, and then enter it a second time.

Configure the Service Processor Network Management Port

Complete the following steps to configure the network management port.

1 Type **set /SP/network pendingipdiscovery=static** and press **Enter** to disable DHCP for the network management port.

2 Type **set /SP/network pendingipaddress=<xxx.xxx.xxx.xxx>** and press **Enter** to set the IP address of the network management port.

Note: Replace <xxx.xxx.xxx.xxx> with the IP address for the network management port.

3 Type **set /SP/network/pendingipgateway=<xxx.xxx.xxx.xxx>** and press **Enter** to set the Default Gateway for the network management port.

Note: Replace <xxx.xxx.xxx.xxx> with the gateway IP address for the network management port.

4 Type **set /SP/network pendingipnetmask=<xxx.xxx.xxx.xxx>** and press **Enter** to set the network mask for the network management port.

Note: Replace <xxx.xxx.xxx.xxx> with the network mask for the network management port.

5 Type **set /SP/services/ssh state=enabled** and press **Enter** to configure the network management port to use SSH.

6 Type **set /SP/network state=enabled** and press **Enter** to enable the network management port.

7 Type **show /SP/network** and press **Enter** to display the current network management port settings.

8 If any of the settings are incorrect, retype the necessary command to set the parameter to the proper value and then repeat step 7.

9 Type **set /SP/network commitpending=true** and press **Enter** to complete and implement the new network management port settings.

10 Type **show /SP/network** and press **Enter** to display the current network management port settings and to verify that the settings are correct.

Example: Output should look similar to the following settings.

```
commitpending = (Cannot show property)
dhcp_server_ip = none
ipaddress = xx.xx.xxx.xx
ipdiscovery = static
ipgateway = xx.xx.xxx.x
ipnetmask = 255.255.255.0
macaddress = 00:14:4F:EB:4C:E1
pendingipaddress = xx.xx.xxx.xx
pendingipdiscovery = static
pendingipgateway = xx.xx.xxx.x
pendingipnetmask = 255.255.255.0
state = enabled
```

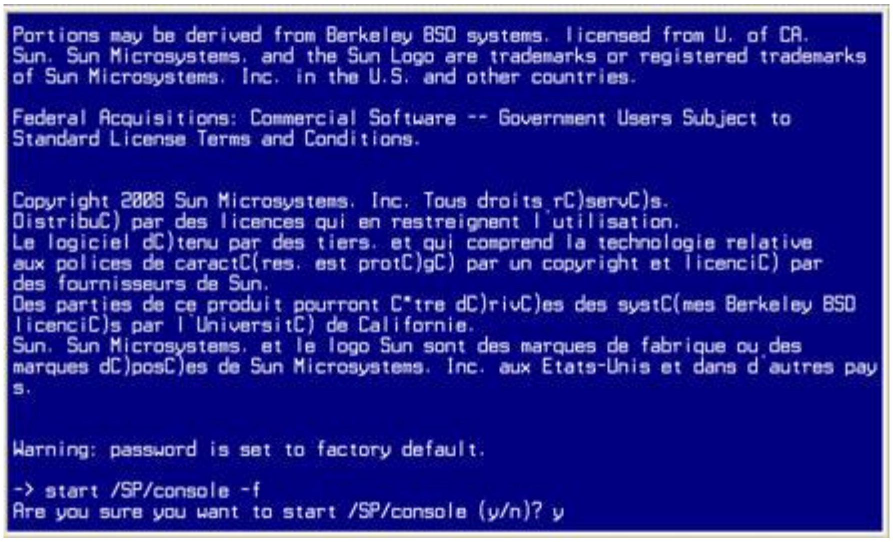
Connect to the Console of the DTACS Server

Important: For initial installation, you should use the ILOM port to connect from a laptop to the serial management port of the DTACS server.

Connect to the Console Via the ILOM Port

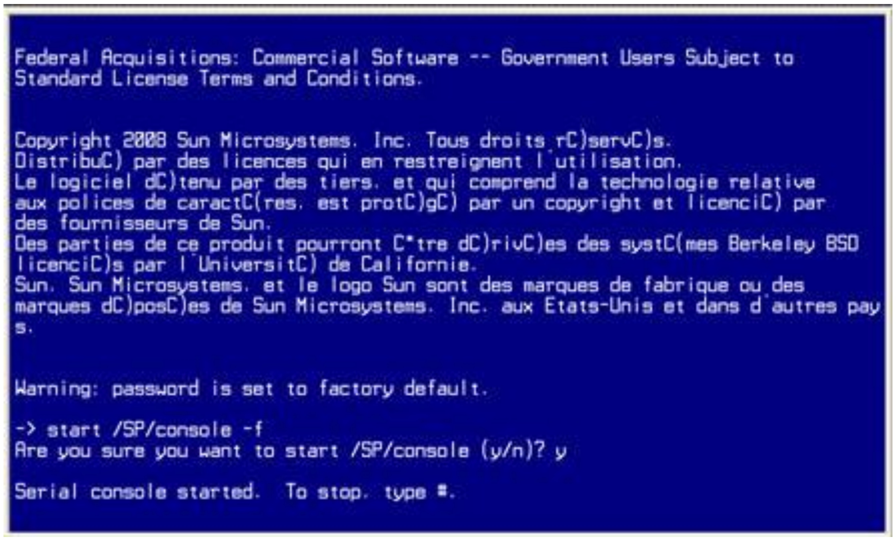
Complete the following steps to open a secure shell session and connect to the console of the DTACS server.

1 At the => prompt, type **start /SP/console -f** and press **Enter**. A message asks if you want to start the console.



```
Portions may be derived from Berkeley BSD systems, licensed from U. of CA.
Sun, Sun Microsystems, and the Sun Logo are trademarks or registered trademarks
of Sun Microsystems, Inc. in the U.S. and other countries.

Federal Acquisitions: Commercial Software -- Government Users Subject to
Standard License Terms and Conditions.


Copyright 2008 Sun Microsystems, Inc. Tous droits rC)servC)s.
DistribuC) par des licences qui en restreignent l'utilisation.
Le logiciel dC)tenu par des tiers, et qui comprend la technologie relative
aux polices de caractC(res, est protC)gC) par un copyright et licenciC) par
des fournisseurs de Sun.
Des parties de ce produit pourront C*tre dC)rivC)es des systC(mes Berkeley BSD
licenciC)s par l'UniversitC) de Californie.
Sun, Sun Microsystems, et le logo Sun sont des marques de fabrique ou des
marques dC)posC)es de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pay
s.


Warning: password is set to factory default.

-> start /SP/console -f
Are you sure you want to start /SP/console (y/n)? y
```

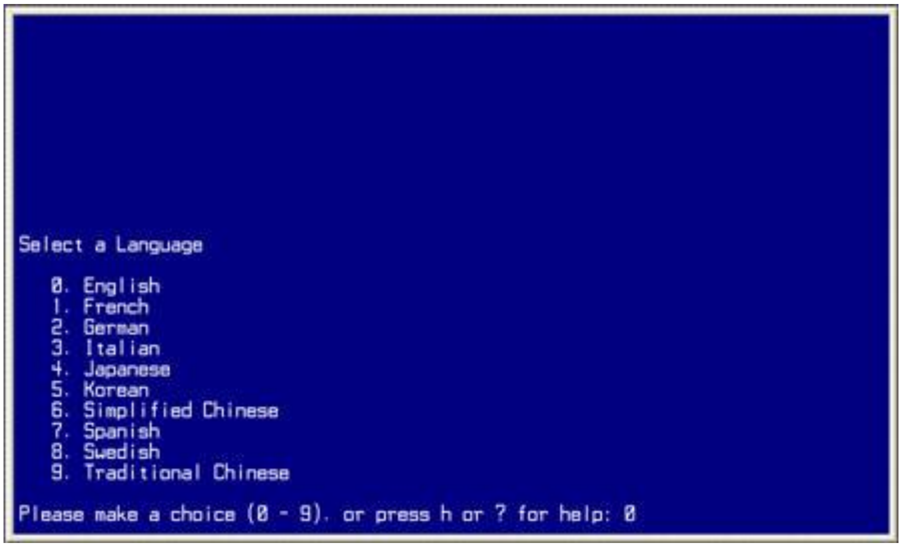
2 Type **y** for yes and press **Enter**. A message indicates that the console has started and instructs you to type #. to exit the console.



```
Federal Acquisitions: Commercial Software -- Government Users Subject to
Standard License Terms and Conditions.


Copyright 2008 Sun Microsystems, Inc. Tous droits rC)servC)s.
DistribuC) par des licences qui en restreignent l'utilisation.
Le logiciel dC)tenu par des tiers, et qui comprend la technologie relative
aux polices de caractC(res, est protC)gC) par un copyright et licenciC) par
des fournisseurs de Sun.
Des parties de ce produit pourront C*tre dC)rivC)es des systC(mes Berkeley BSD
licenciC)s par l'UniversitC) de Californie.
Sun, Sun Microsystems, et le logo Sun sont des marques de fabrique ou des
marques dC)posC)es de Sun Microsystems, Inc. aux Etats-Unis et dans d'autres pay
s.


Warning: password is set to factory default.

-> start /SP/console -f
Are you sure you want to start /SP/console (y/n)? y

Serial console started.  To stop, type #.
```

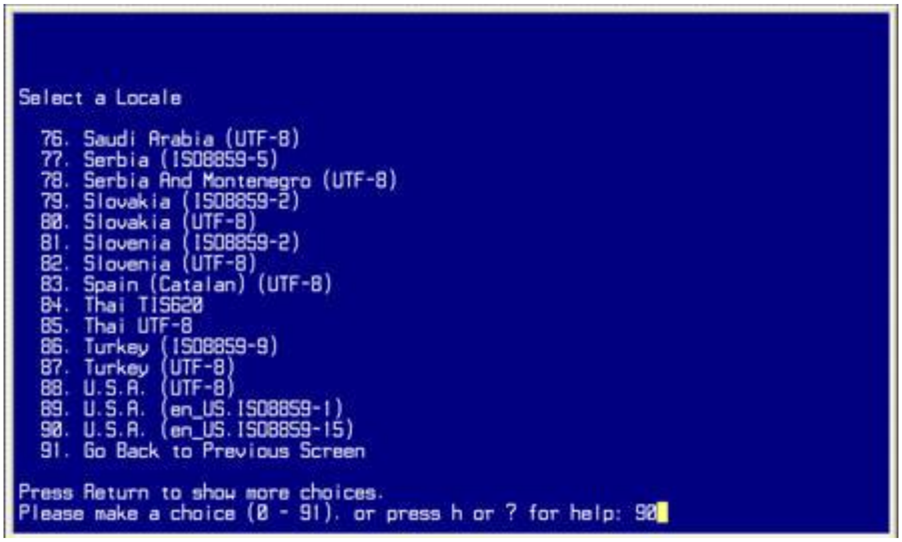
3 Press **Enter**. The Select a Language screen appears.

Note: The Select a Language screen is one screen in a series of screens. During this series of screens, you will often have to select a configuration parameter from a list of parameters. Use the arrow keys to navigate through your choices and make selections by pressing the spacebar. The system usually places an X beside the selected parameter.



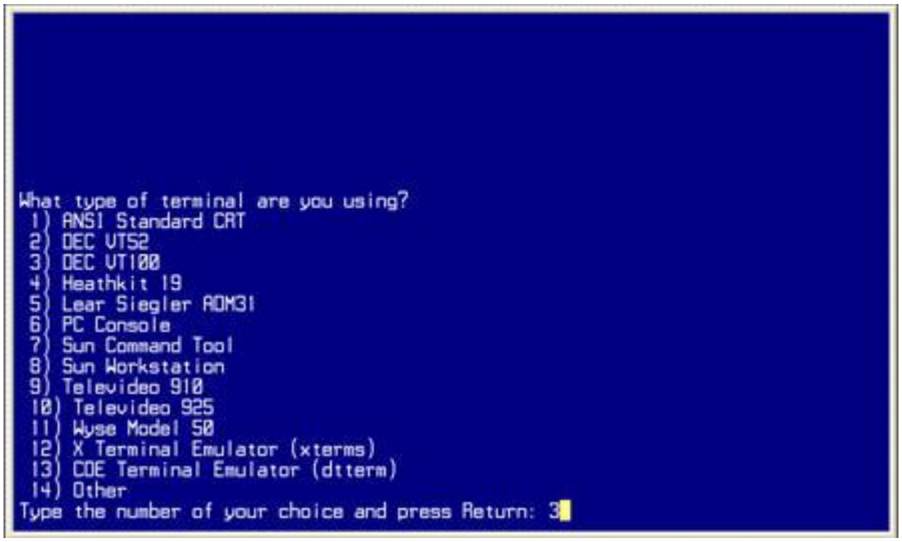
```
Select a Language

   0. English
   1. French
   2. German
   3. Italian
   4. Japanese
   5. Korean
   6. Simplified Chinese
   7. Spanish
   8. Swedish
   9. Traditional Chinese

Please make a choice (0 - 9). or press h or ? for help: 0
```

4 Type a number that corresponds to your desired language and press **Enter**. The window prompts you to enter your locale.



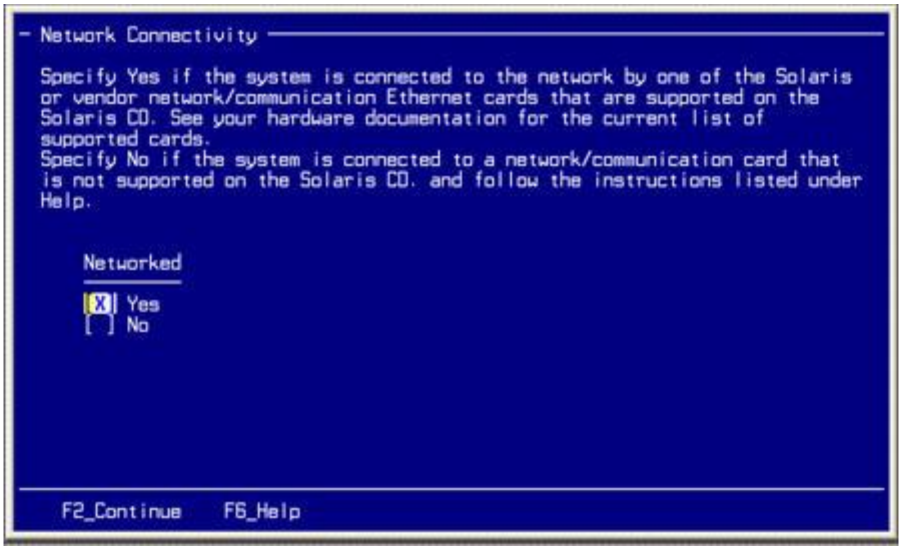
```
Select a Locale

  76. Saudi Arabia (UTF-8)
  77. Serbia (ISO8859-5)
  78. Serbia And Montenegro (UTF-8)
  79. Slovakia (ISO8859-2)
  80. Slovakia (UTF-8)
  81. Slovenia (ISO8859-2)
  82. Slovenia (UTF-8)
  83. Spain (Catalan) (UTF-8)
  84. Thai TIS620
  85. Thai UTF-8
  86. Turkey (ISO8859-9)
  87. Turkey (UTF-8)
  88. U.S.A. (UTF-8)
  89. U.S.A. (en_US.ISO8859-1)
  90. U.S.A. (en_US.ISO8859-15)
  91. Go Back to Previous Screen

Press Return to show more choices.
Please make a choice (0 - 91). or press h or ? for help: 90
```

5 Type a number that corresponds to your locale and press **Enter**. The window prompts you to identify your terminal type.



```
What type of terminal are you using?
 1) ANSI Standard CRT
 2) DEC VT52
 3) DEC VT100
 4) Heathkit 19
 5) Lear Siegler ADM31
 6) PC Console
 7) Sun Command Tool
 8) Sun Workstation
 9) Televideo 910
 10) Televideo 925
 11) Wyse Model 50
 12) X Terminal Emulator (xterms)
 13) CDE Terminal Emulator (dtterm)
 14) Other
Type the number of your choice and press Return: 3
```

6 Type the number that corresponds to DEC VT100 and press **Enter**. The window prompts you to identify if the system is connected to the network.



- Network Connectivity

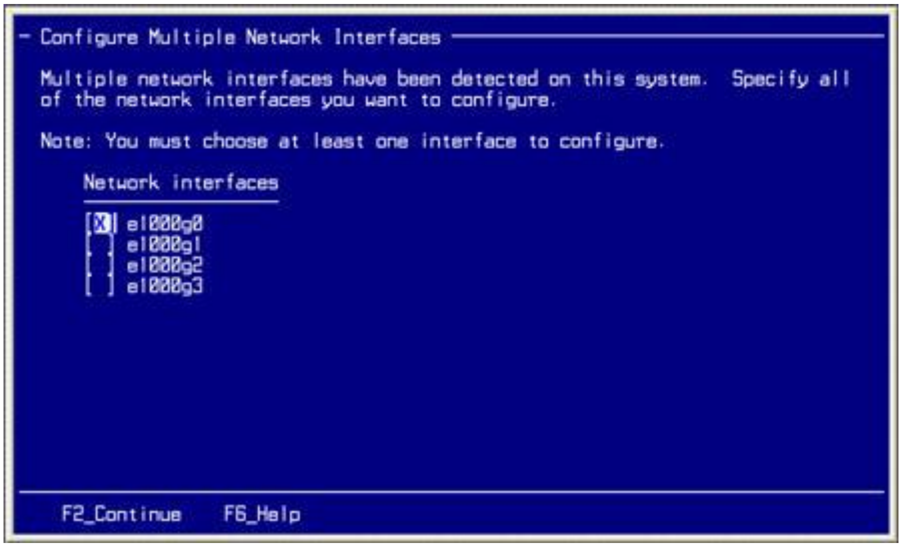
Specify Yes if the system is connected to the network by one of the Solaris or vendor network/communication Ethernet cards that are supported on the Solaris CD. See your hardware documentation for the current list of supported cards.
Specify No if the system is connected to a network/communication card that is not supported on the Solaris CD. and follow the instructions listed under Help.

Networked

☒ Yes
□ No

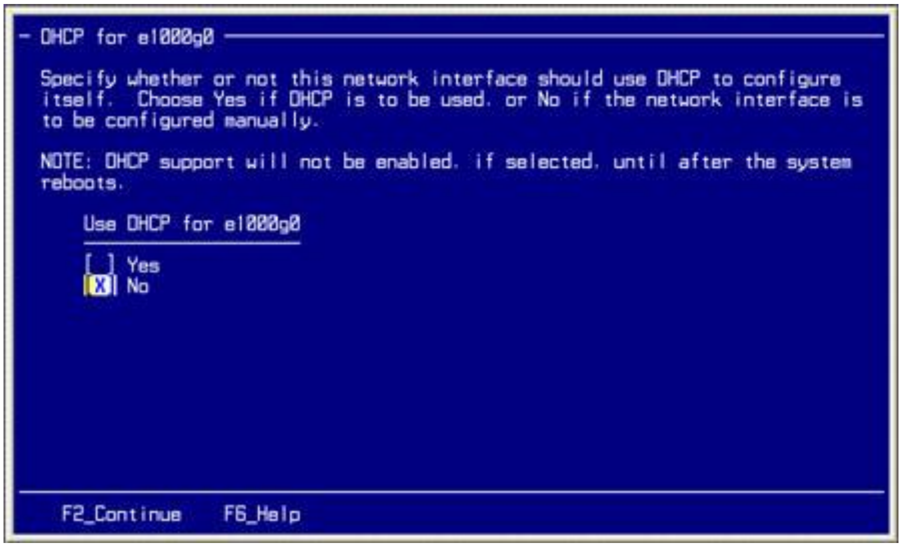
7 Select **Yes** and press **F2**. The window prompts you to select the network interface you want to configure.

Note: The value in the screen below is *only* an example. Choose the appropriate option for your system.



```
- Configure Multiple Network Interfaces ────────────────────────────────

  Multiple network interfaces have been detected on this system.  Specify all
  of the network interfaces you want to configure.

  Note: You must choose at least one interface to configure.

      Network interfaces
      ──────────────────

      [X] e1000g0
      [ ] e1000g1
      [ ] e1000g2
      [ ] e1000g3

────────────────────────────────────────────────────────────────────────
    F2_Continue    F6_Help
```

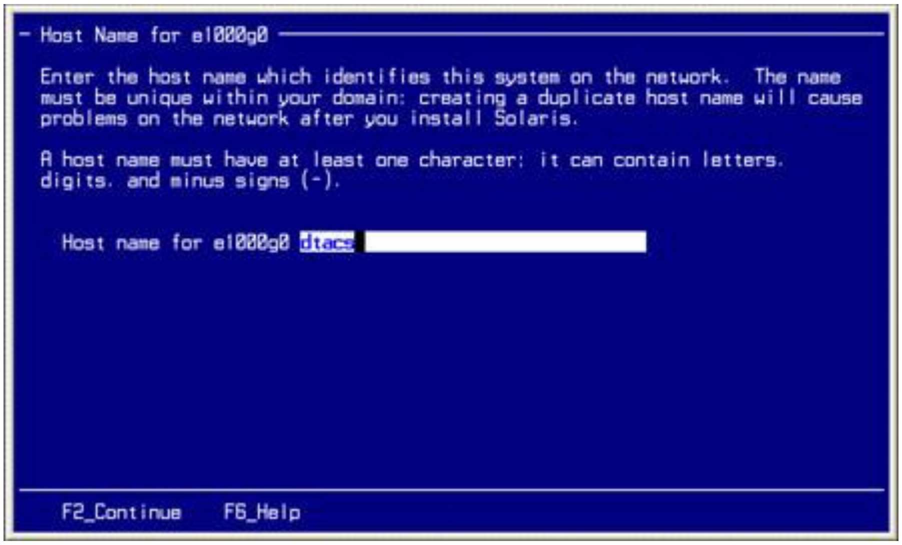
8 Select **e10000g0** and press **F2**. The window prompts you to indicate if DHCP should be enabled for the network interface.



```
- DHCP for e1000g0 ─────────────────────────────────────────────────────

  Specify whether or not this network interface should use DHCP to configure
  itself.  Choose Yes if DHCP is to be used, or No if the network interface is
  to be configured manually.

  NOTE: DHCP support will not be enabled, if selected, until after the system
  reboots.

      Use DHCP for e1000g0
      ────────────────────

      [ ] Yes
      [X] No

────────────────────────────────────────────────────────────────────────
    F2_Continue    F6_Help
```

9 Select the appropriate response and press **F2**. The window prompts you to enter the host name that identifies this system on the network.

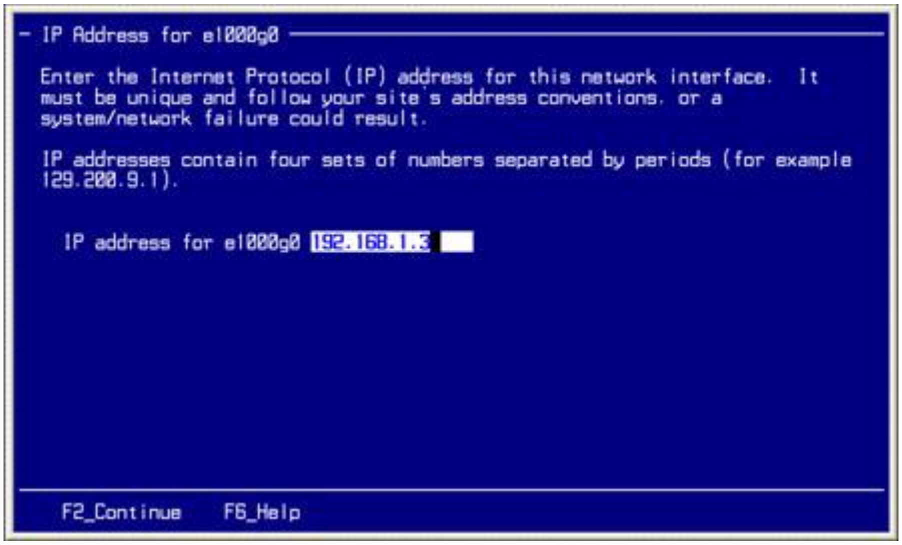
Note: The value in the screen below is *only* an example. Enter the appropriate value for your system.



```
- Host Name for e1000g0 ───────────────────────────────────────

  Enter the host name which identifies this system on the network.  The name
  must be unique within your domain; creating a duplicate host name will cause
  problems on the network after you install Solaris.

  A host name must have at least one character; it can contain letters,
  digits, and minus signs (-).

    Host name for e1000g0 dtacs
```

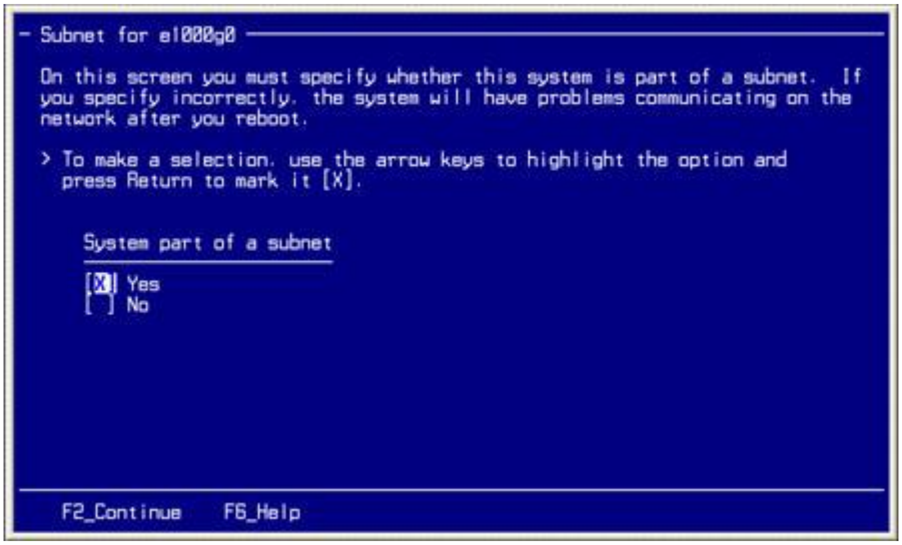
10 Type the host name (example, dtacs) and press **F2**. The window prompts you to enter the IP address for the e1000g0 interface.

Note: The value in the screen below is *only* an example. Enter the appropriate value for your system.



```
- IP Address for e1000g0 ──────────────────────────────────────

  Enter the Internet Protocol (IP) address for this network interface.  It
  must be unique and follow your site's address conventions, or a
  system/network failure could result.

  IP addresses contain four sets of numbers separated by periods (for example
  129.200.9.1).

    IP address for e1000g0 192.168.1.3
```

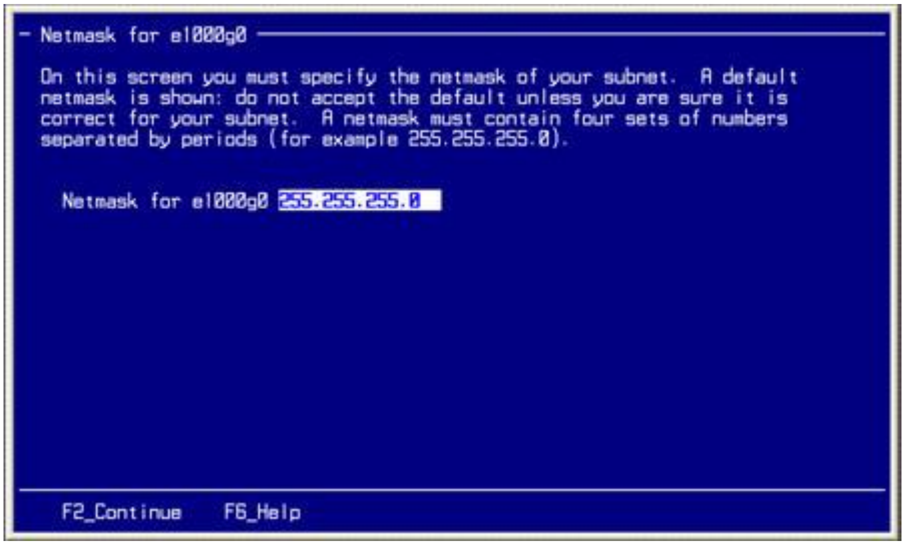
11 Enter the IP address for the e1000g0 interface and press **F2**. The window prompts you to specify if the system is part of a subnet.



```
- Subnet for e1000g0

  On this screen you must specify whether this system is part of a subnet.  If
  you specify incorrectly, the system will have problems communicating on the
  network after you reboot.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].

      System part of a subnet

      [X] Yes
      [ ] No

    F2_Continue    F6_Help
```

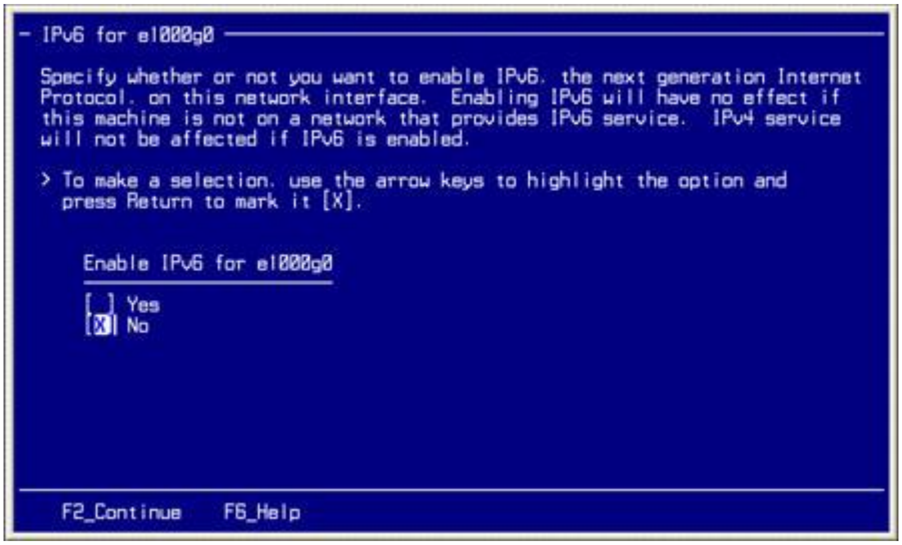
12 Select **Yes** and press **F2**. The window prompts you to enter the netmask for the subnet.

Note: The value in the screen below is *only* an example. Enter the appropriate value for your system.



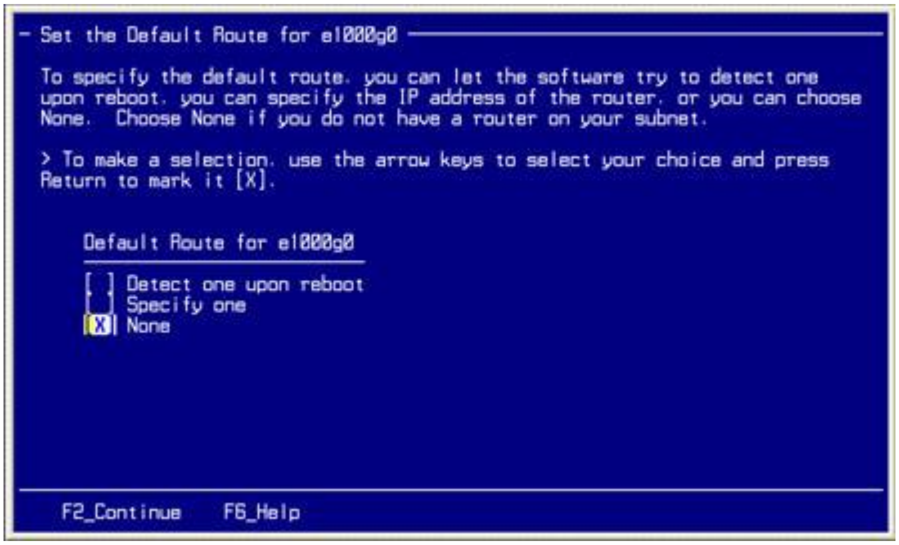
```
- Netmask for e1000g0

  On this screen you must specify the netmask of your subnet.  A default
  netmask is shown; do not accept the default unless you are sure it is
  correct for your subnet.  A netmask must contain four sets of numbers
  separated by periods (for example 255.255.255.0).

    Netmask for e1000g0 255.255.255.0

    F2_Continue    F6_Help
```

13 Enter the netmask for the e1000g0 interface and press **F2**. The window prompts you to indicate if IPv6 should be enabled.



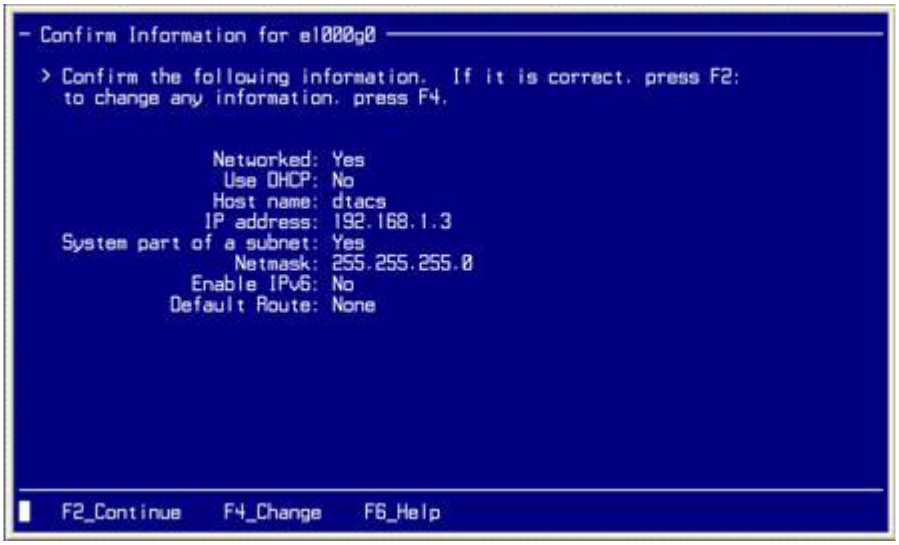
```
- IPv6 for e1000g0 ----------------------------------------------------------

  Specify whether or not you want to enable IPv6, the next generation Internet
  Protocol, on this network interface.  Enabling IPv6 will have no effect if
  this machine is not on a network that provides IPv6 service.  IPv4 service
  will not be affected if IPv6 is enabled.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].

      Enable IPv6 for e1000g0
      -----------------------
      [ ] Yes
      [X] No


   F2_Continue    F6_Help
```

14 Select **No** and press **F2**. The window prompts you to define the default route for the e1000g0 interface.



```
- Set the Default Route for e1000g0 -----------------------------------------

  To specify the default route, you can let the software try to detect one
  upon reboot, you can specify the IP address of the router, or you can choose
  None.  Choose None if you do not have a router on your subnet.

  > To make a selection, use the arrow keys to select your choice and press
  Return to mark it [X].

      Default Route for e1000g0
      -------------------------
      [ ] Detect one upon reboot
      [ ] Specify one
      [X] None


   F2_Continue    F6_Help
```

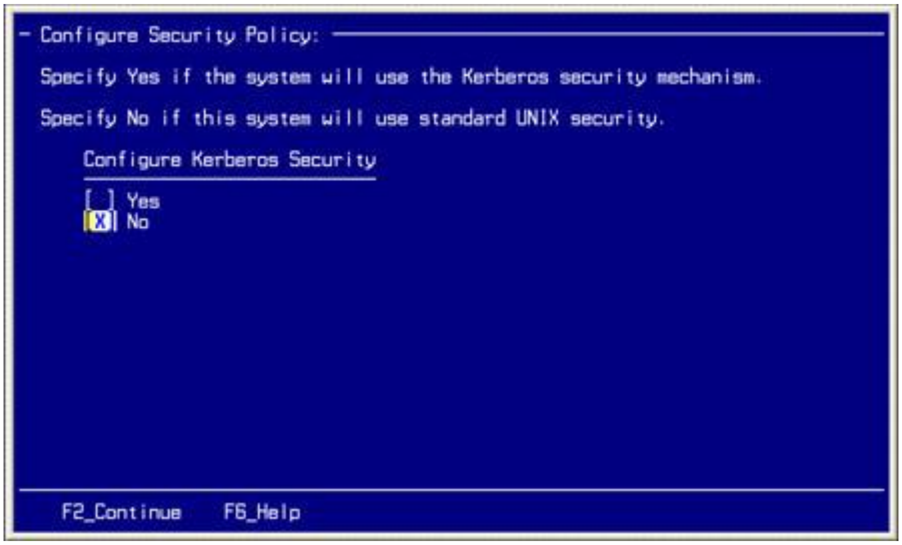
15 Select **None** and press **F2**. The window prompts you to confirm the network information.



```
- Confirm Information for e1000g0 ─────────────────────────────────

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.


                   Networked: Yes
                    Use DHCP: No
                   Host name: dtacs
                  IP address: 192.168.1.3
     System part of a subnet: Yes
                     Netmask: 255.255.255.0
                 Enable IPv6: No
               Default Route: None
```

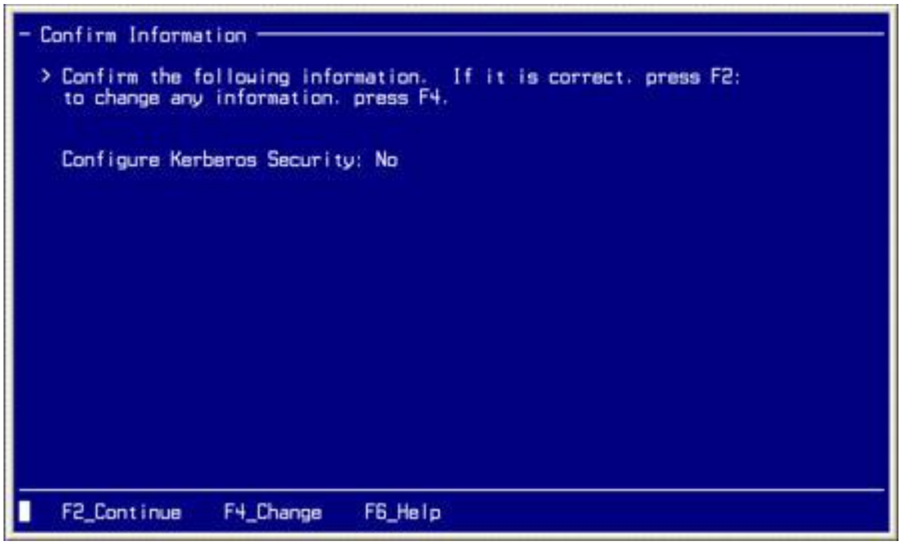
16 Verify that the configuration is correct and press **F2**. The window prompts you to specify whether your system will use the Kerberos security.

Note: If you need to change any configuration parameters, press **F4**. Then follow the on-screen instructions.



```
- Configure Security Policy: ─────────────────────────────────────

  Specify Yes if the system will use the Kerberos security mechanism.

  Specify No if this system will use standard UNIX security.

      Configure Kerberos Security
      ───────────────────────────
      [ ] Yes
      [X] No
```

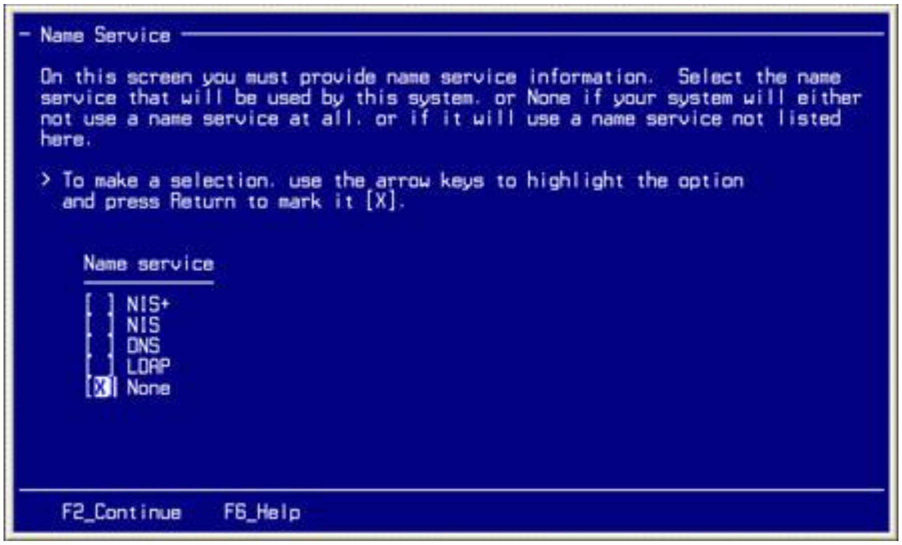
17 Select **No** and press **F2**. The window prompts you to confirm the selection you made regarding Kerberos.



```
- Confirm Information -------------------------------------------------------

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.

    Configure Kerberos Security: No

-----------------------------------------------------------------------------
    F2_Continue    F4_Change    F6_Help
```

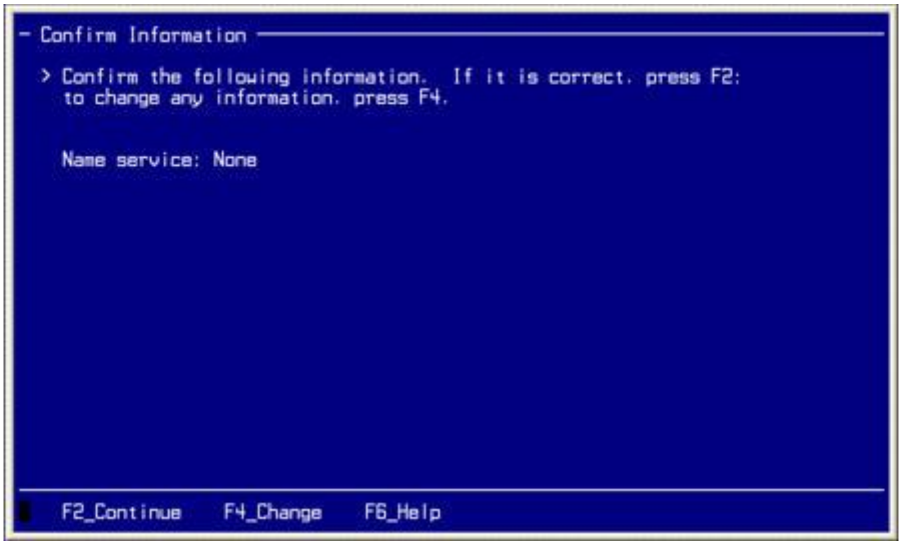
18 Review the Kerberos configuration and press **F2** if the settings are correct. The window prompts you to select the name service for your system.

Note: If you need to change any configuration parameters, press **F4**. Then follow the on-screen instructions.



```
- Name Service --------------------------------------------------------------

  On this screen you must provide name service information.  Select the name
  service that will be used by this system, or None if your system will either
  not use a name service at all, or if it will use a name service not listed
  here.

  > To make a selection, use the arrow keys to highlight the option
    and press Return to mark it [X].

      Name service
      ____________
      [ ] NIS+
      [ ] NIS
      [ ] DNS
      [ ] LDAP
      [X] None

-----------------------------------------------------------------------------
    F2_Continue    F6_Help
```

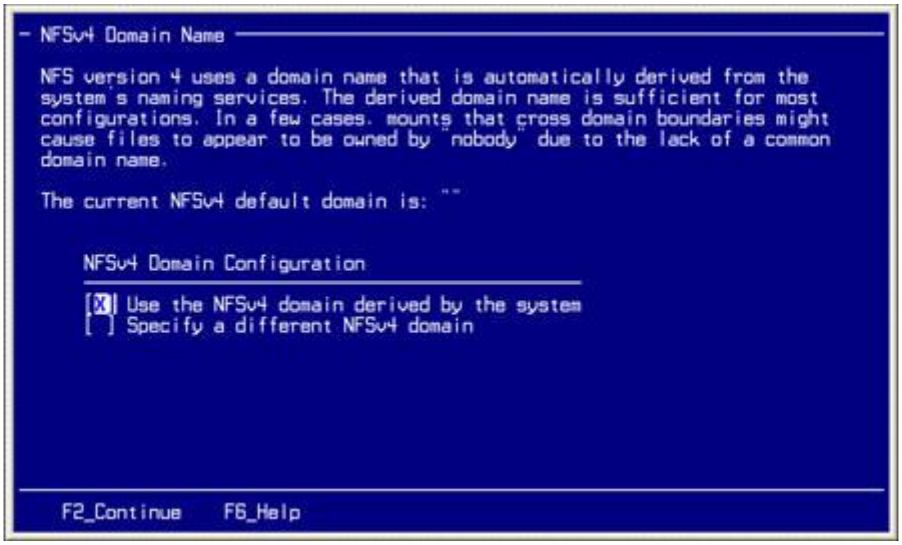
19 Select **None** and press **F2**. The window prompts you to confirm the selection you made regarding the name service.



```
- Confirm Information

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.

    Name service: None
```

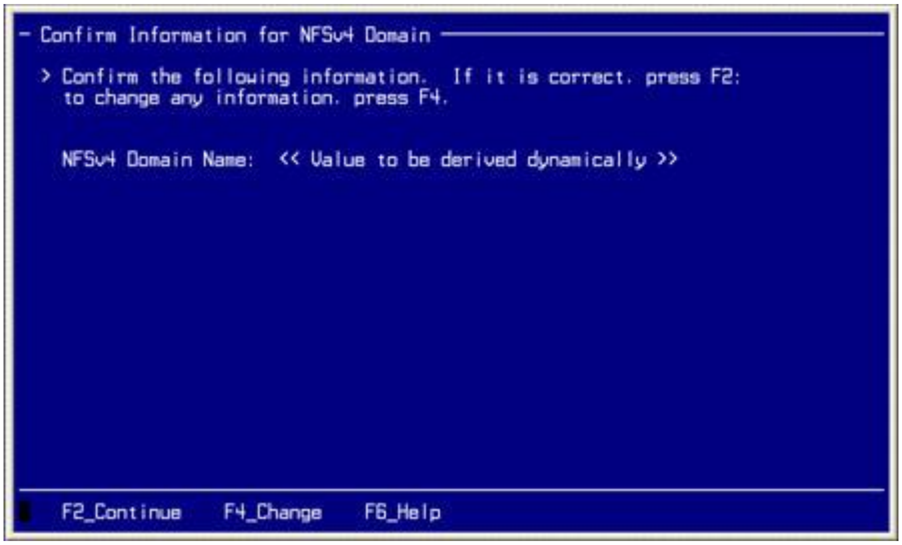
20 Verify that the name service information is correct and press **F2**. The window updates and prompts you to indicate the NFSv4 domain for your system.

Note: If you need to change the configuration, press **F4**. Then follow the on-screen instructions.



```
- NFSv4 Domain Name

  NFS version 4 uses a domain name that is automatically derived from the
  system's naming services. The derived domain name is sufficient for most
  configurations. In a few cases, mounts that cross domain boundaries might
  cause files to appear to be owned by "nobody" due to the lack of a common
  domain name.

  The current NFSv4 default domain is: ""

      NFSv4 Domain Configuration
      ----------------------------------------------
      [X] Use the NFSv4 domain derived by the system
      [ ] Specify a different NFSv4 domain
```

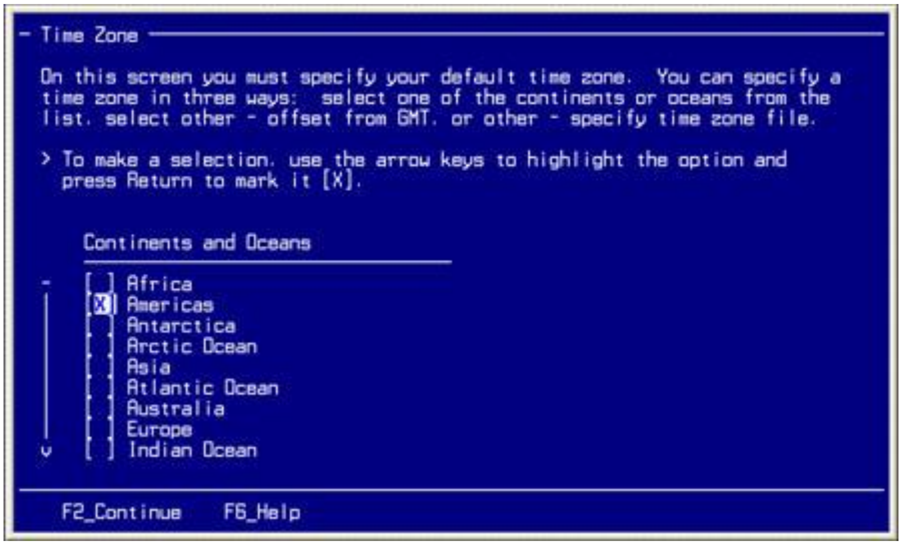
21 Select **Use the NFSv4 domain derived by the system** and press **F2**. The window prompts you to confirm the selection you made regarding the NFSv4 domain name.



```
- Confirm Information for NFSv4 Domain ----------------------------------------

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.

    NFSv4 Domain Name:  << Value to be derived dynamically >>

--------------------------------------------------------------------------------
    F2_Continue    F4_Change    F6_Help
```

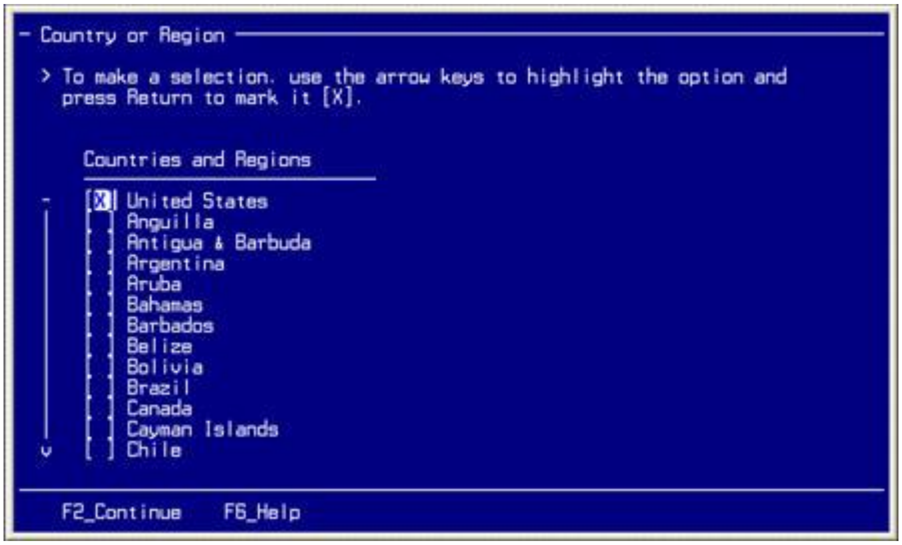
22 Verify that the configuration for the NFSv4 domain name is correct and press **F2**. The window prompts you to define the country or region where the system is located.

Note: If you need to change the configuration, press **F4**. Then follow the on-screen instructions.



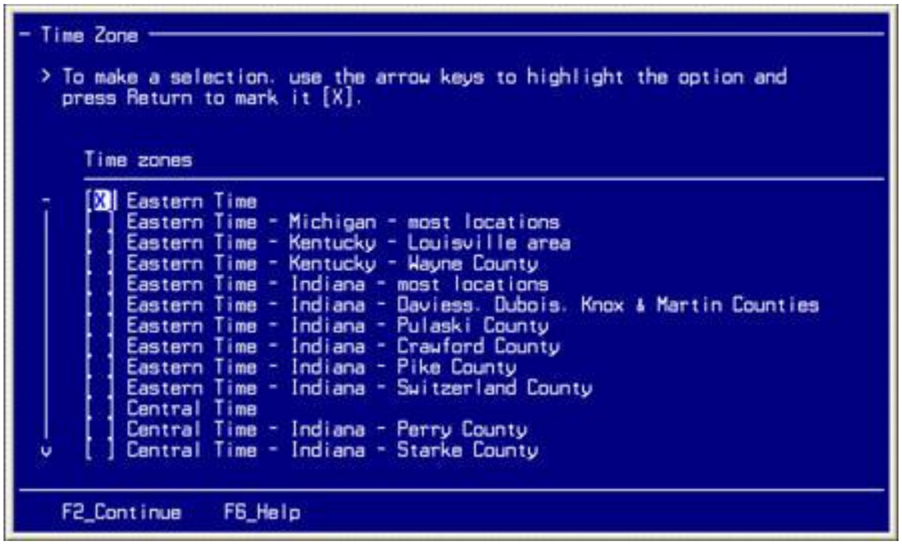
```
- Time Zone ---------------------------------------------------------------------

  On this screen you must specify your default time zone.  You can specify a
  time zone in three ways:  select one of the continents or oceans from the
  list, select other - offset from GMT, or other - specify time zone file.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].

      Continents and Oceans
      ----------------------------------
  -   [ ] Africa
  |   [X] Americas
  |   [ ] Antarctica
  |   [ ] Arctic Ocean
  |   [ ] Asia
  |   [ ] Atlantic Ocean
  |   [ ] Australia
  |   [ ] Europe
  v   [ ] Indian Ocean

--------------------------------------------------------------------------------
    F2_Continue    F6_Help
```

23 Select the appropriate time zone and press **F2**. The window prompts you to define the country where the system is located.



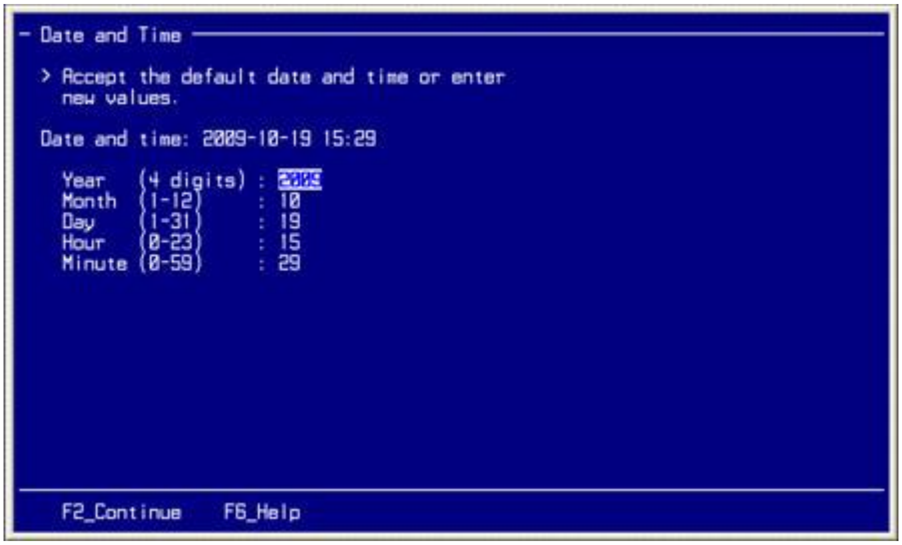
```
- Country or Region ─────────────────────────────────────────────

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].

      Countries and Regions
      ───────────────────────
  -   [X] United States
  |   [ ] Anguilla
  |   [ ] Antigua & Barbuda
  |   [ ] Argentina
  |   [ ] Aruba
  |   [ ] Bahamas
  |   [ ] Barbados
  |   [ ] Belize
  |   [ ] Bolivia
  |   [ ] Brazil
  |   [ ] Canada
  |   [ ] Cayman Islands
  v   [ ] Chile

───────────────────────────────────────────────────────────────
    F2_Continue    F6_Help
```

24 Select the appropriate country or region and press **F2**. The window prompts you to define the time zone.



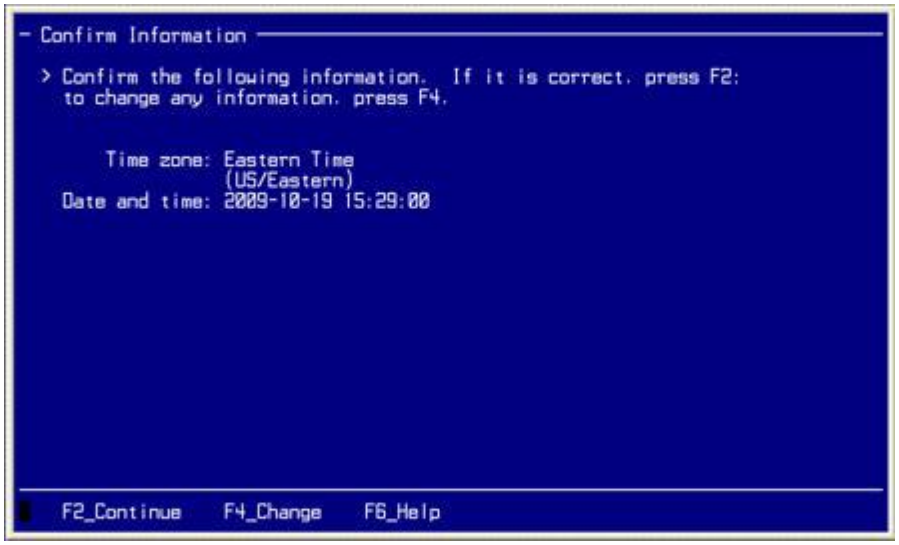
```
- Time Zone ─────────────────────────────────────────────────────

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].

      Time zones
      ─────────────────────────────────────────────────────────
  -   [X] Eastern Time
  |   [ ] Eastern Time - Michigan - most locations
  |   [ ] Eastern Time - Kentucky - Louisville area
  |   [ ] Eastern Time - Kentucky - Wayne County
  |   [ ] Eastern Time - Indiana - most locations
  |   [ ] Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
  |   [ ] Eastern Time - Indiana - Pulaski County
  |   [ ] Eastern Time - Indiana - Crawford County
  |   [ ] Eastern Time - Indiana - Pike County
  |   [ ] Eastern Time - Indiana - Switzerland County
  |   [ ] Central Time
  |   [ ] Central Time - Indiana - Perry County
  v   [ ] Central Time - Indiana - Starke County

───────────────────────────────────────────────────────────────
    F2_Continue    F6_Help
```

25 Select the appropriate time zone and press **F2**. The window prompts you define the date and time.



```
- Date and Time

  > Accept the default date and time or enter
    new values.

  Date and time: 2009-10-19 15:29

    Year   (4 digits) : 2009
    Month  (1-12)     : 10
    Day    (1-31)     : 19
    Hour   (0-23)     : 15
    Minute (0-59)     : 29

    F2_Continue    F6_Help
```

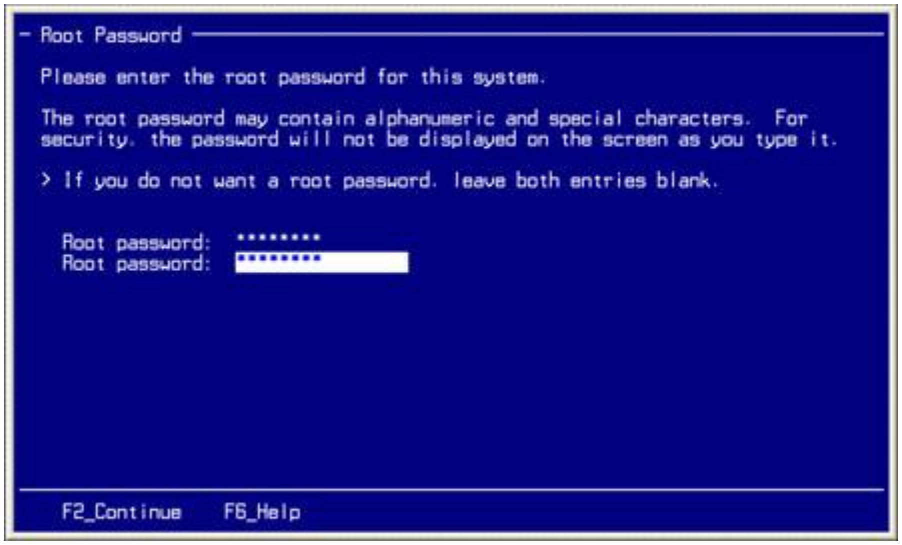
26 Select the default values, if they are correct, or type in the correct values and press **F2**. The window prompts you to confirm all date and time information.



```
- Confirm Information

  > Confirm the following information.  If it is correct, press F2;
    to change any information, press F4.

        Time zone: Eastern Time
                   (US/Eastern)
    Date and time: 2009-10-19 15:29:00

    F2_Continue    F4_Change    F6_Help
```

27 Verify that the configuration is correct and press **F2**. The window prompts you to enter the password for the root user.

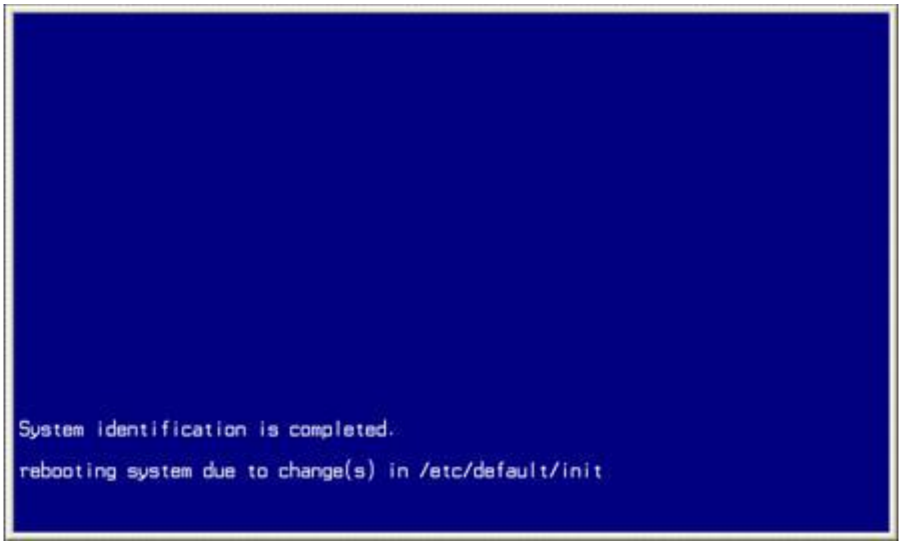
Note: If you need to change the configuration, press **F4**. Then follow the on-screen instructions.



```
- Root Password --------------------------------------------------------
  Please enter the root password for this system.

  The root password may contain alphanumeric and special characters.  For
  security, the password will not be displayed on the screen as you type it.

  > If you do not want a root password, leave both entries blank.

    Root password:  ********
    Root password:  ********

------------------------------------------------------------------------
    F2_Continue    F6_Help
```

28 Type the root password and press **Enter**. Then re-enter the root password and press **F2**. The system identification for the operating system completes and the system reboots.

Note: For the initial system configuration, type **2g3n3r!c** for the root password.



```
System identification is completed.

rebooting system due to change(s) in /etc/default/init
```

29 Type **shutdown -y -g0 -i0** and press **Enter**. The ok> prompt appears.

30 Go to ***Install the DTACS Software*** (on page 30).

Install the DTACS Software

This section provides the steps necessary to install the DTACS software for the first time.

Important: Be sure that you are using the procedures in this section to install the DTACS software for the first time. If you are upgrading DTACS software at a site where it is already installed, use the upgrade procedures found later in this book.

In the series of screens that follow, you will often have to select a configuration parameter from a list of parameters. Use the arrow keys to navigate through your choices and make selections by pressing the spacebar. The system usually places an X beside the selected parameter.

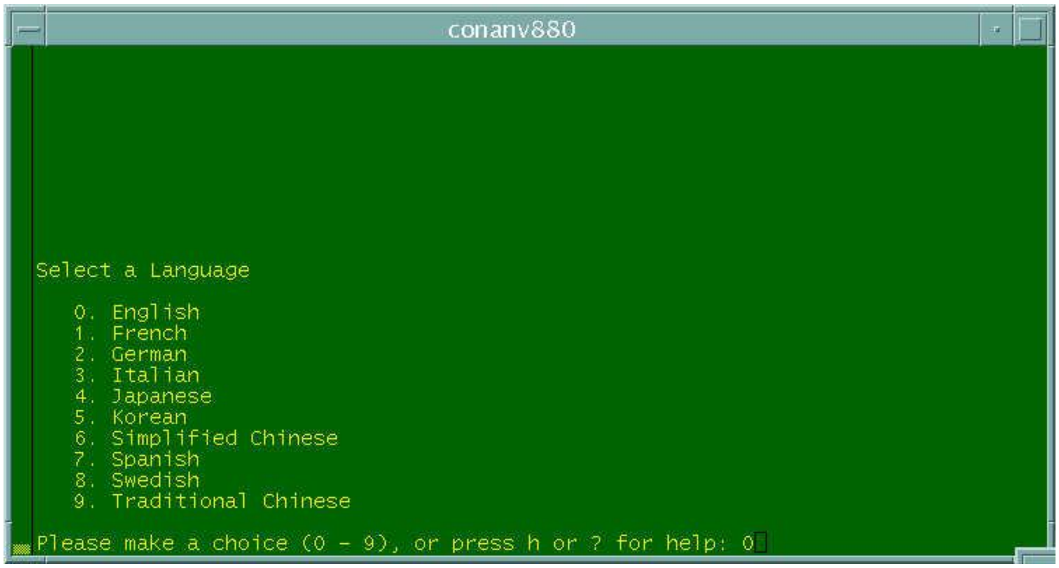
Important: Be certain that there are no network cables installed or connected to the DTACS at this time.

1 Insert the Maintenance DVD into the DVD drive of the DTACS.

2 At the ok> prompt, type **boot cdrom - install** and press **Enter**. The server boots from the DVD.

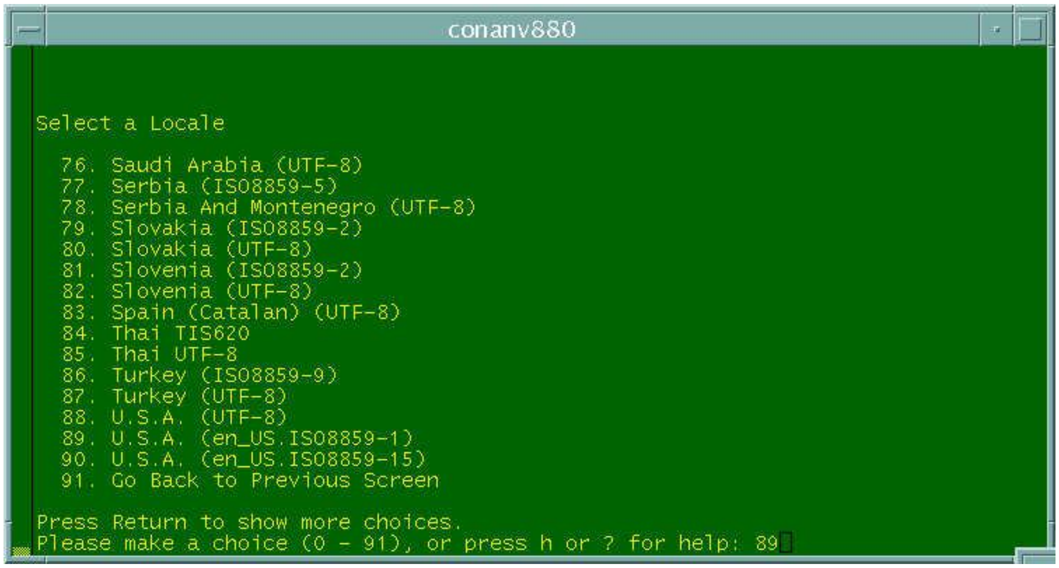
Results:

- The DTACS server reboots and the installation script begins.
- The Select a Language window appears.



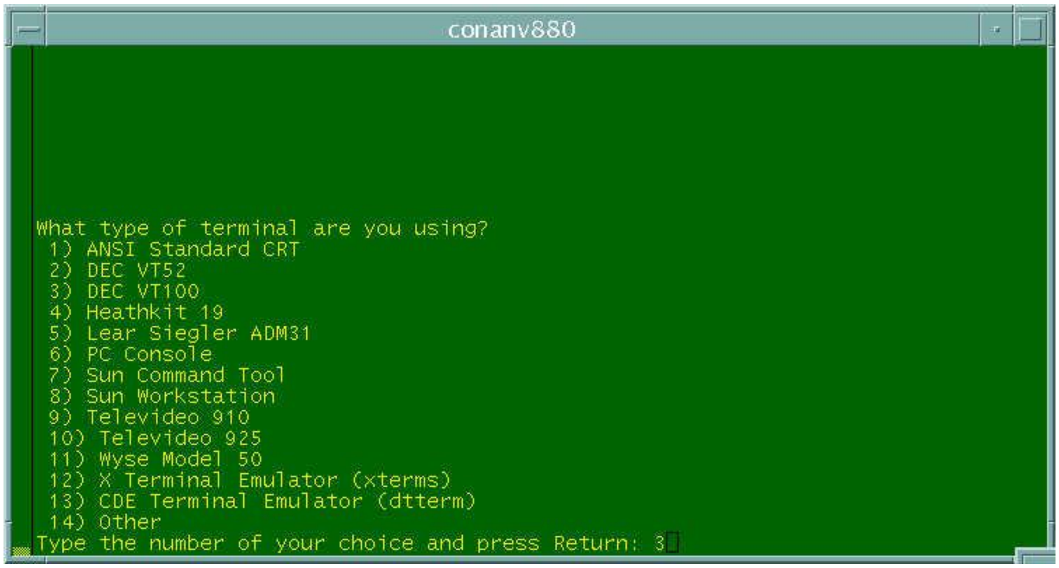
```
Select a Language

    0. English
    1. French
    2. German
    3. Italian
    4. Japanese
    5. Korean
    6. Simplified Chinese
    7. Spanish
    8. Swedish
    9. Traditional Chinese

Please make a choice (0 - 9), or press h or ? for help: 0
```

3 Type a number that corresponds to your desired language and press **Enter**. The window prompts you to identify your locale.



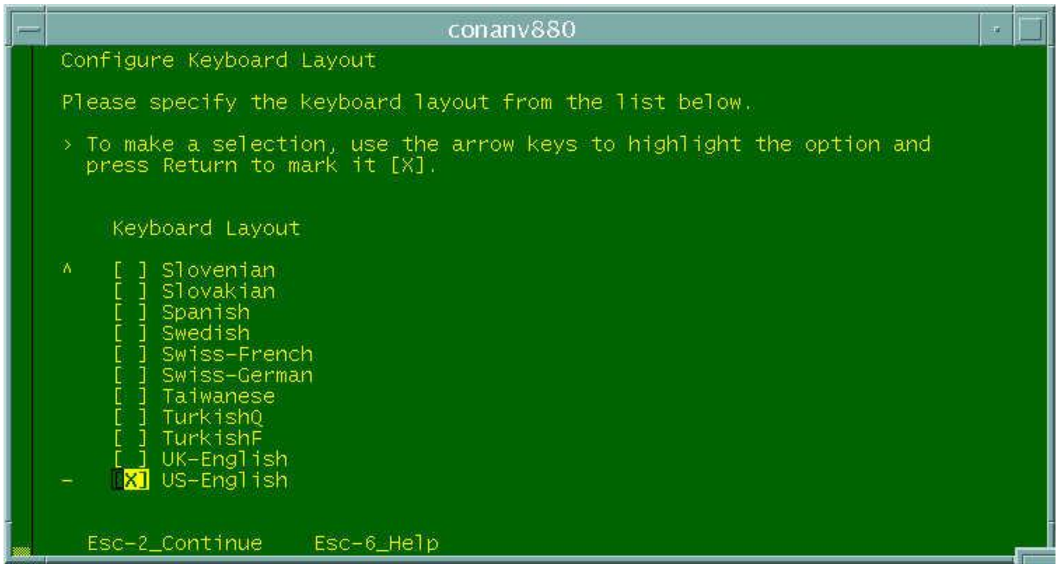
```
Select a Locale

  76. Saudi Arabia (UTF-8)
  77. Serbia (ISO8859-5)
  78. Serbia And Montenegro (UTF-8)
  79. Slovakia (ISO8859-2)
  80. Slovakia (UTF-8)
  81. Slovenia (ISO8859-2)
  82. Slovenia (UTF-8)
  83. Spain (Catalan) (UTF-8)
  84. Thai TIS620
  85. Thai UTF-8
  86. Turkey (ISO8859-9)
  87. Turkey (UTF-8)
  88. U.S.A. (UTF-8)
  89. U.S.A. (en_US.ISO8859-1)
  90. U.S.A. (en_US.ISO8859-15)
  91. Go Back to Previous Screen

Press Return to show more choices.
Please make a choice (0 - 91), or press h or ? for help: 89
```

4 Type a number that corresponds to your locale and press **Enter**. The window prompts you to identify the type of terminal you are using.



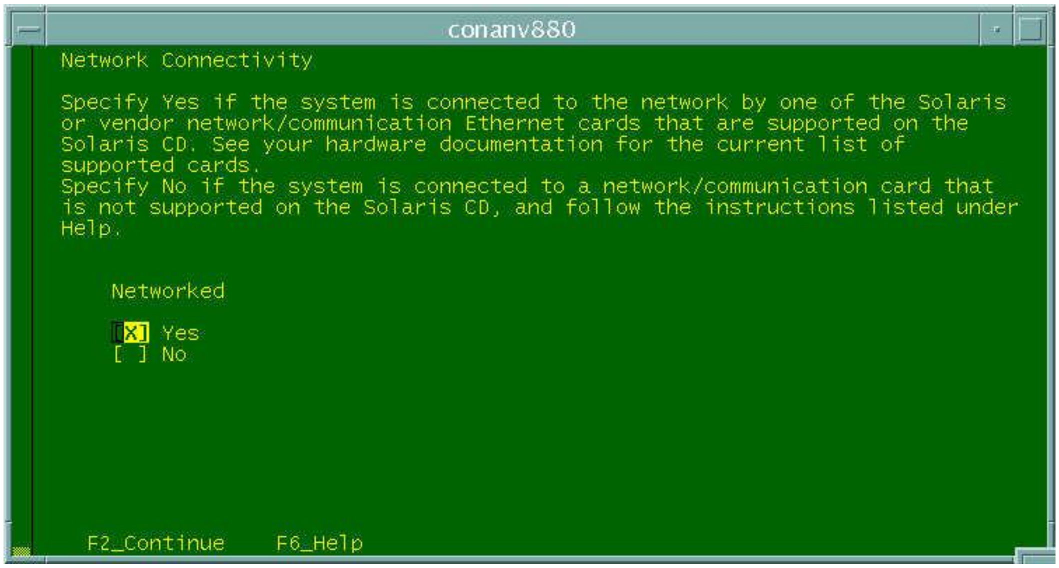
```
What type of terminal are you using?
 1) ANSI Standard CRT
 2) DEC VT52
 3) DEC VT100
 4) Heathkit 19
 5) Lear Siegler ADM31
 6) PC Console
 7) Sun Command Tool
 8) Sun Workstation
 9) Televideo 910
 10) Televideo 925
 11) Wyse Model 50
 12) X Terminal Emulator (xterms)
 13) CDE Terminal Emulator (dtterm)
 14) Other
Type the number of your choice and press Return: 3
```

5 Type a number that corresponds to DEC VT100 and press **Enter**. The window prompts you to specify a keyboard layout.



```
Configure Keyboard Layout

Please specify the keyboard layout from the list below.

> To make a selection, use the arrow keys to highlight the option and
  press Return to mark it [X].


    Keyboard Layout

^   [ ] Slovenian
    [ ] Slovakian
    [ ] Spanish
    [ ] Swedish
    [ ] Swiss-French
    [ ] Swiss-German
    [ ] Taiwanese
    [ ] TurkishQ
    [ ] TurkishF
    [ ] UK-English
-   [X] US-English


  Esc-2_Continue    Esc-6_Help
```

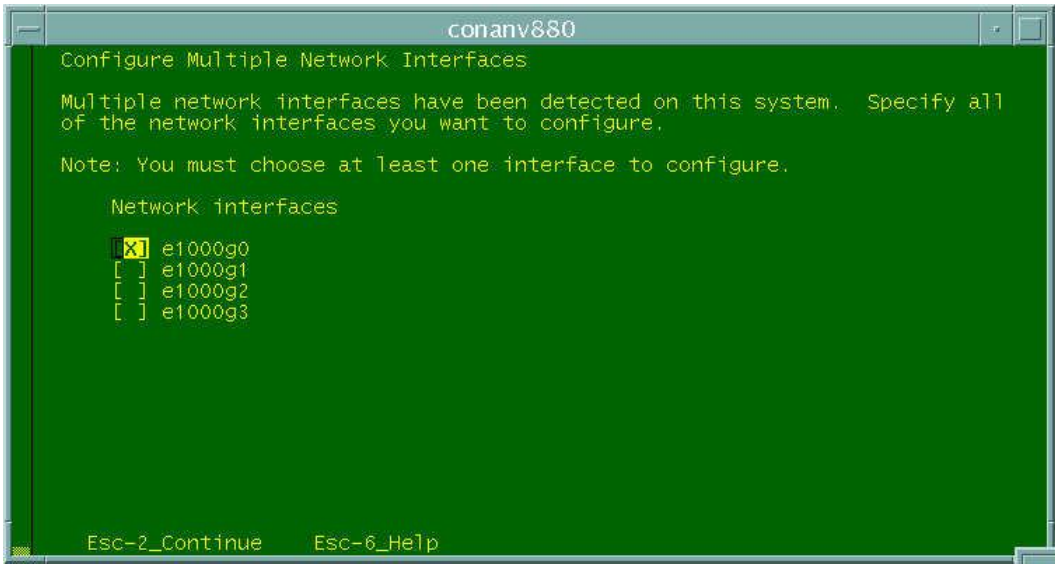
6 Select **US-English** (or the keyboard layout you want to use) and press **Esc** and **2** simultaneously (**Esc+2)**. The window asks whether the system is connected to the network through a Solaris-compatible Ethernet card.



```
Network Connectivity

Specify Yes if the system is connected to the network by one of the Solaris
or vendor network/communication Ethernet cards that are supported on the
Solaris CD. See your hardware documentation for the current list of
supported cards.
Specify No if the system is connected to a network/communication card that
is not supported on the Solaris CD, and follow the instructions listed under
Help.


    Networked

    [X] Yes
    [ ] No







  F2_Continue    F6_Help
```

7 Select **Yes** and press **F2**. The window prompts you to select the network interface that you want to configure.

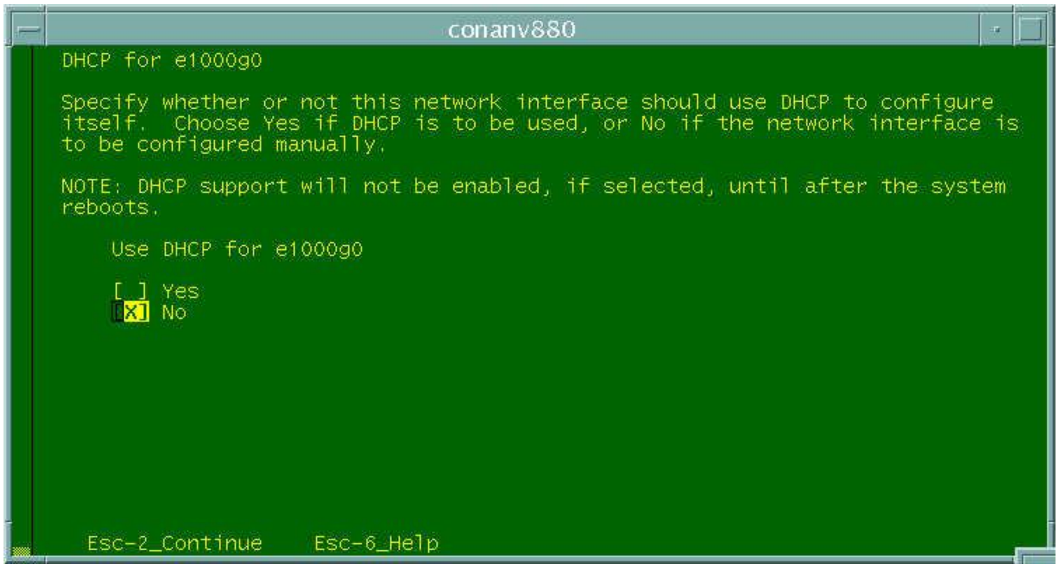
Note: On some systems, the window may also prompt you to press Esc+2 to continue. Either method (Esc+2 or F2) will work.



```
conanv880
Configure Multiple Network Interfaces

Multiple network interfaces have been detected on this system.  Specify all
of the network interfaces you want to configure.

Note: You must choose at least one interface to configure.

    Network interfaces

    [X] e1000g0
    [ ] e1000g1
    [ ] e1000g2
    [ ] e1000g3

  Esc-2_Continue    Esc-6_Help
```

8 Select **e1000g0** and press **Esc+2**. The window prompts you to specify whether the Dynamic Host Configuration Protocol (DHCP) is to be used to configure the e1000g0 interface.

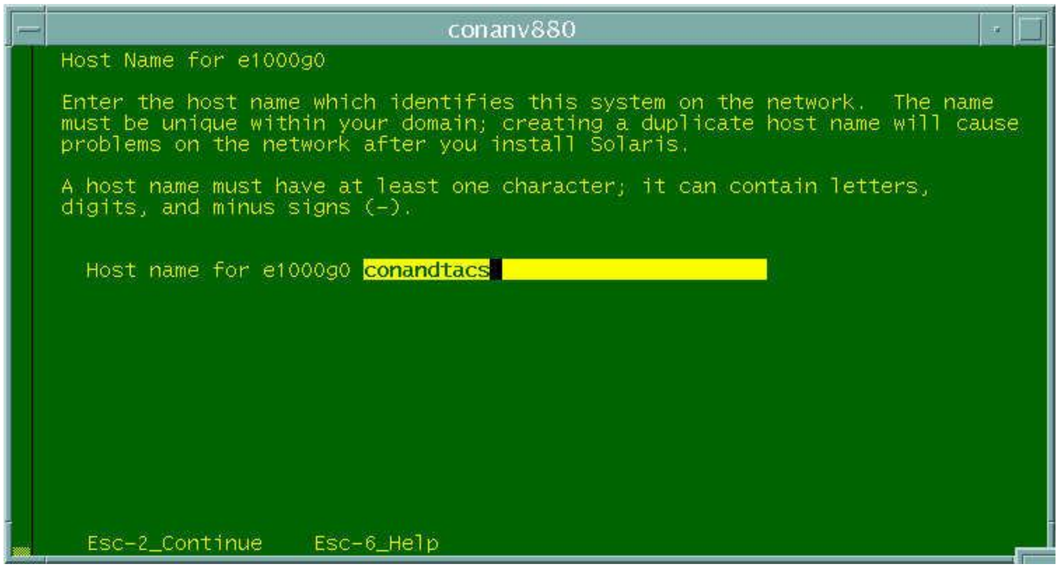
Note: Alternately, you can press F2.



```
conanv880
DHCP for e1000g0

Specify whether or not this network interface should use DHCP to configure
itself.  Choose Yes if DHCP is to be used, or No if the network interface is
to be configured manually.

NOTE: DHCP support will not be enabled, if selected, until after the system
reboots.

    Use DHCP for e1000g0

    [ ] Yes
    [X] No

  Esc-2_Continue    Esc-6_Help
```

9 Select **No** and press **Esc+2**. The window prompts you to enter the host name that identifies this system on the network.

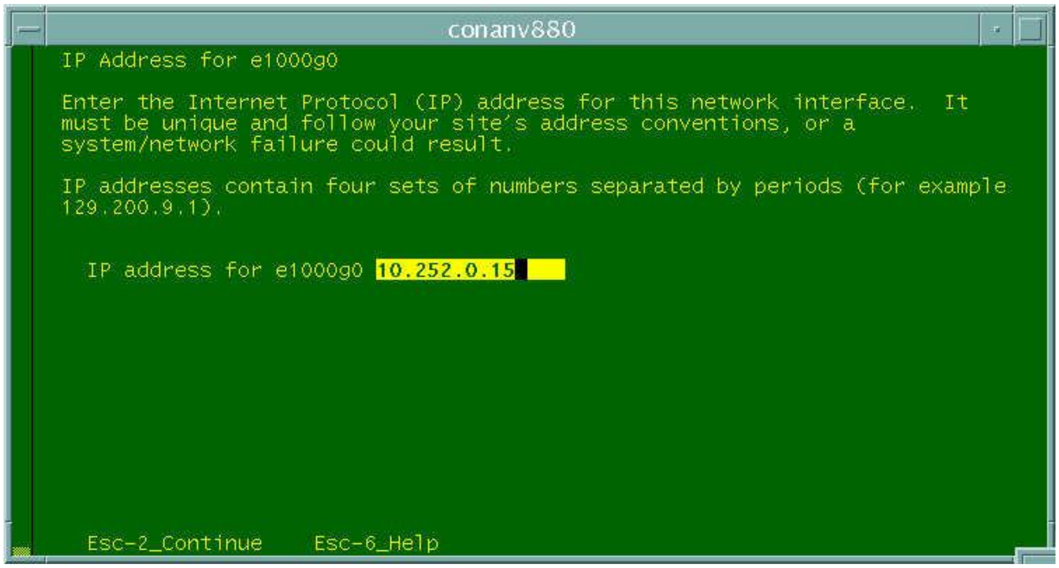
Note: The value in the screen below is *only* an example. Enter the appropriate value for your system.



```
Host Name for e1000g0

Enter the host name which identifies this system on the network.  The name
must be unique within your domain; creating a duplicate host name will cause
problems on the network after you install Solaris.

A host name must have at least one character; it can contain letters,
digits, and minus signs (-).


  Host name for e1000g0 conandtacs
```

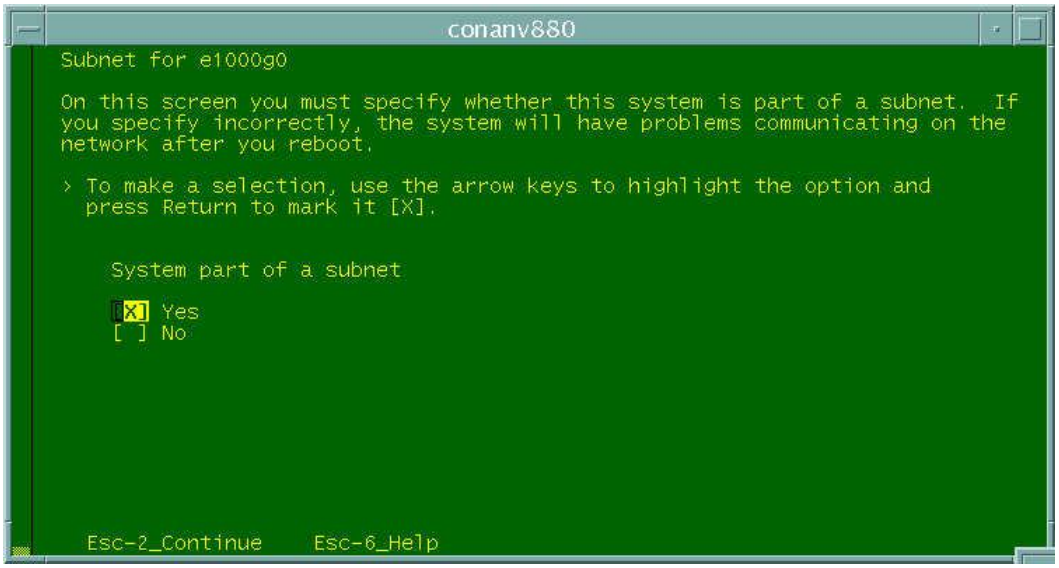
10 Type the host name (example, conandtacs) and press **Esc+2**. The window prompts you to enter the IP address for the e1000g0 interface.

Note: The value in the screen below is *only* an example. Enter the appropriate value for your system.



```
IP Address for e1000g0

Enter the Internet Protocol (IP) address for this network interface.  It
must be unique and follow your site's address conventions, or a
system/network failure could result.

IP addresses contain four sets of numbers separated by periods (for example
129.200.9.1).


  IP address for e1000g0 10.252.0.15
```

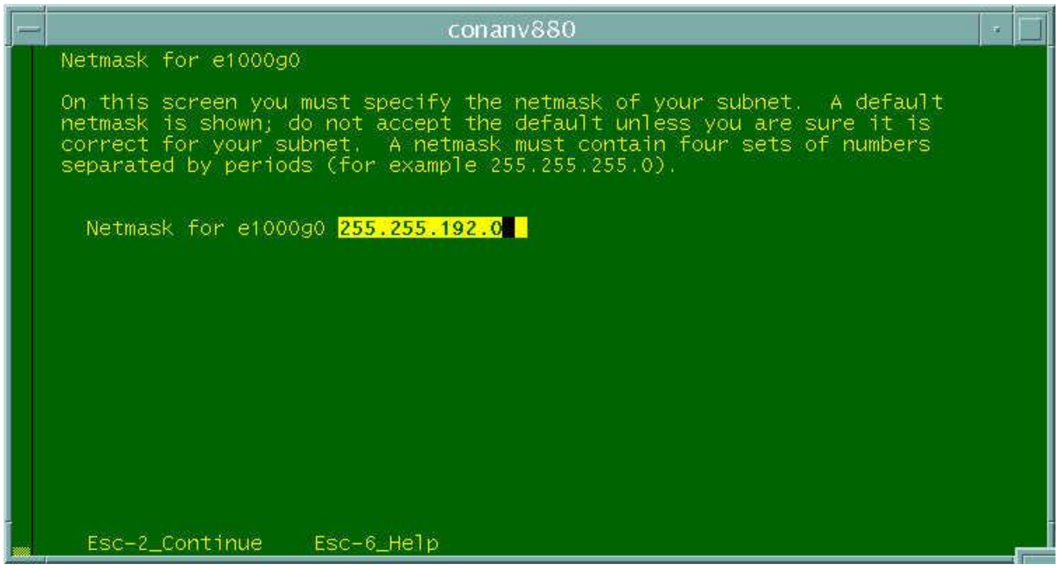
11 Type the IP address and press **Esc+2**. The window prompts you to specify whether your system is part of a subnet.



```
conanv880
Subnet for e1000g0

On this screen you must specify whether this system is part of a subnet.  If
you specify incorrectly, the system will have problems communicating on the
network after you reboot.

> To make a selection, use the arrow keys to highlight the option and
  press Return to mark it [X].


    System part of a subnet

    [X] Yes
    [ ] No









  Esc-2_Continue    Esc-6_Help
```

12 Select **Yes** and press **Esc+2**. The window prompts you to specify the netmask for the e1000g0 interface.

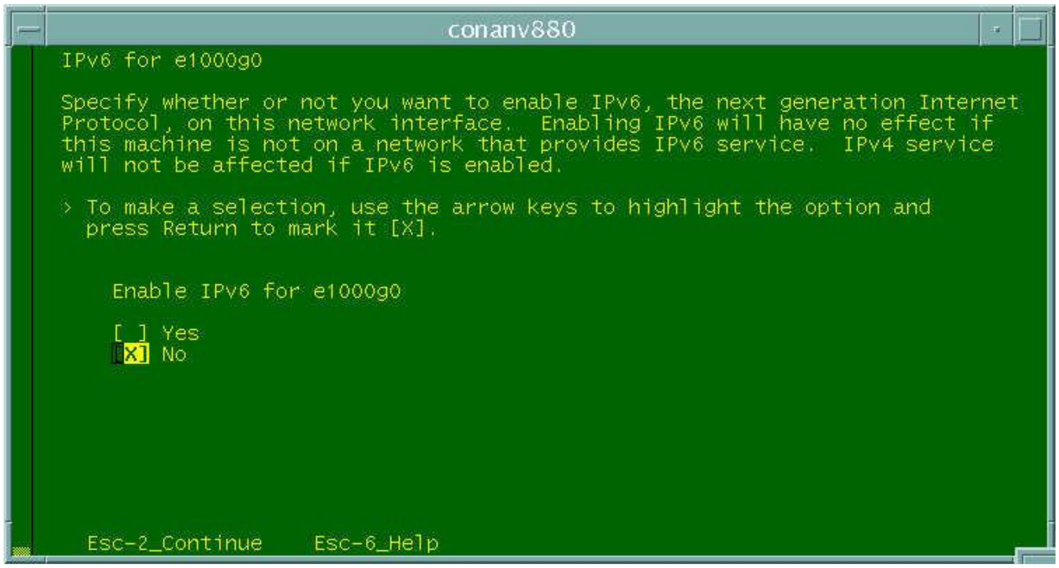
Note: The value in the screen below is *only* an example. Enter the appropriate value for your system.



```
conanv880
Netmask for e1000g0

On this screen you must specify the netmask of your subnet.  A default
netmask is shown; do not accept the default unless you are sure it is
correct for your subnet.  A netmask must contain four sets of numbers
separated by periods (for example 255.255.255.0).


  Netmask for e1000g0 255.255.192.0















  Esc-2_Continue    Esc-6_Help
```

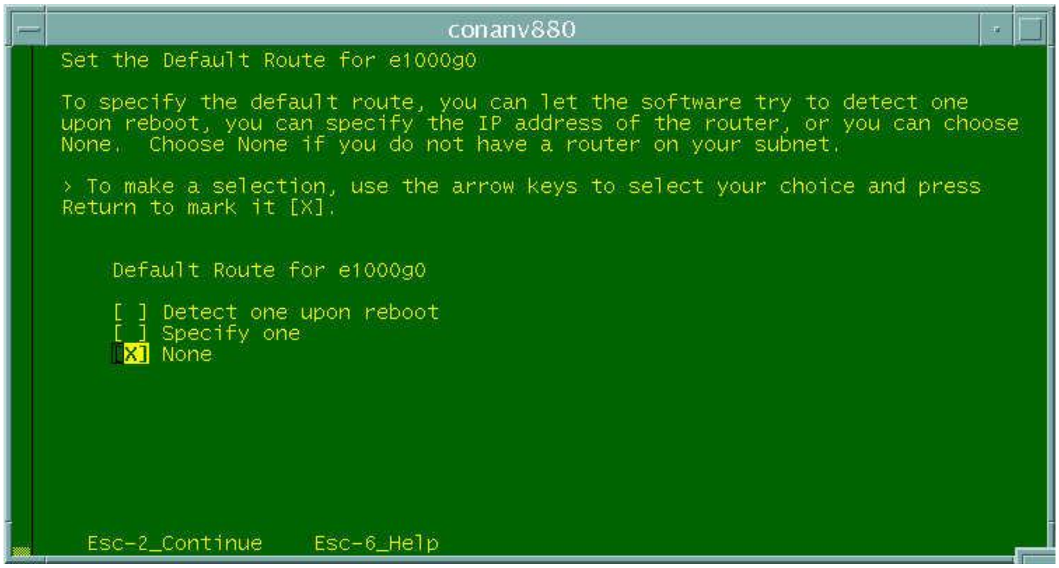
13 Type the netmask for your site and press **Esc+2**. The window prompts you to specify whether you want to enable the IPv6 Internet protocol on the e1000g0 interface.

Note: This guide uses a netmask of 255.255.192.0 as an example. Enter the netmask for your site.



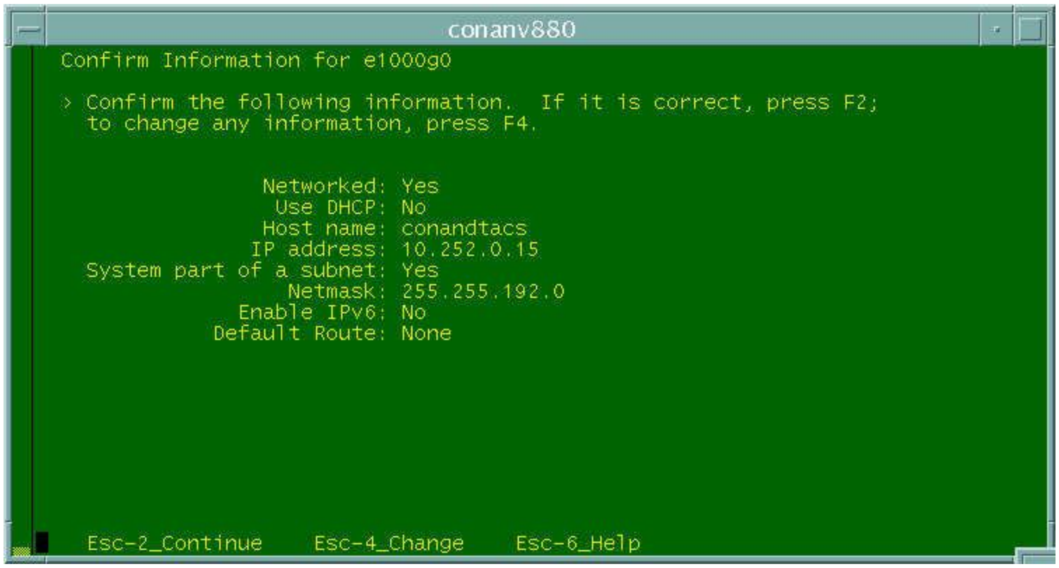
```
IPv6 for e1000g0

Specify whether or not you want to enable IPv6, the next generation Internet
Protocol, on this network interface.  Enabling IPv6 will have no effect if
this machine is not on a network that provides IPv6 service.  IPv4 service
will not be affected if IPv6 is enabled.

> To make a selection, use the arrow keys to highlight the option and
  press Return to mark it [X].


    Enable IPv6 for e1000g0

    [ ] Yes
    [X] No
```

14 Select **No** and press **Esc+2**. The window updates and prompts you to set the default route for the interface.



```
Set the Default Route for e1000g0

To specify the default route, you can let the software try to detect one
upon reboot, you can specify the IP address of the router, or you can choose
None.  Choose None if you do not have a router on your subnet.

> To make a selection, use the arrow keys to select your choice and press
Return to mark it [X].


    Default Route for e1000g0

    [ ] Detect one upon reboot
    [ ] Specify one
    [X] None
```

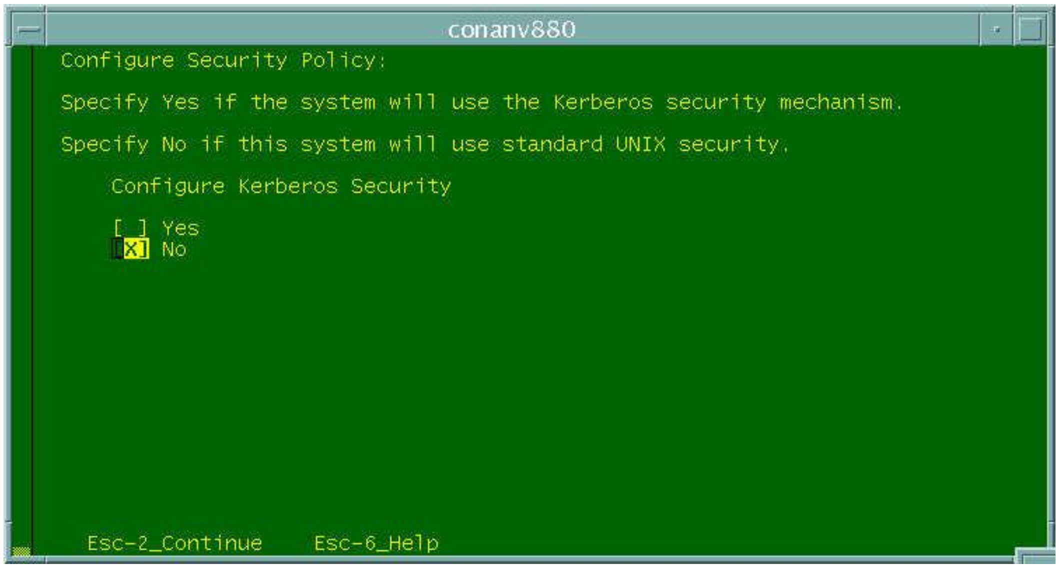
15 Select **None** and press **Esc+2**. The window updates and asks that you confirm the network configuration.



```
Confirm Information for e1000g0

 > Confirm the following information.  If it is correct, press F2;
   to change any information, press F4.


                Networked: Yes
                 Use DHCP: No
                Host name: conandtacs
               IP address: 10.252.0.15
   System part of a subnet: Yes
                  Netmask: 255.255.192.0
              Enable IPv6: No
             Default Route: None









   Esc-2_Continue    Esc-4_Change    Esc-6_Help
```

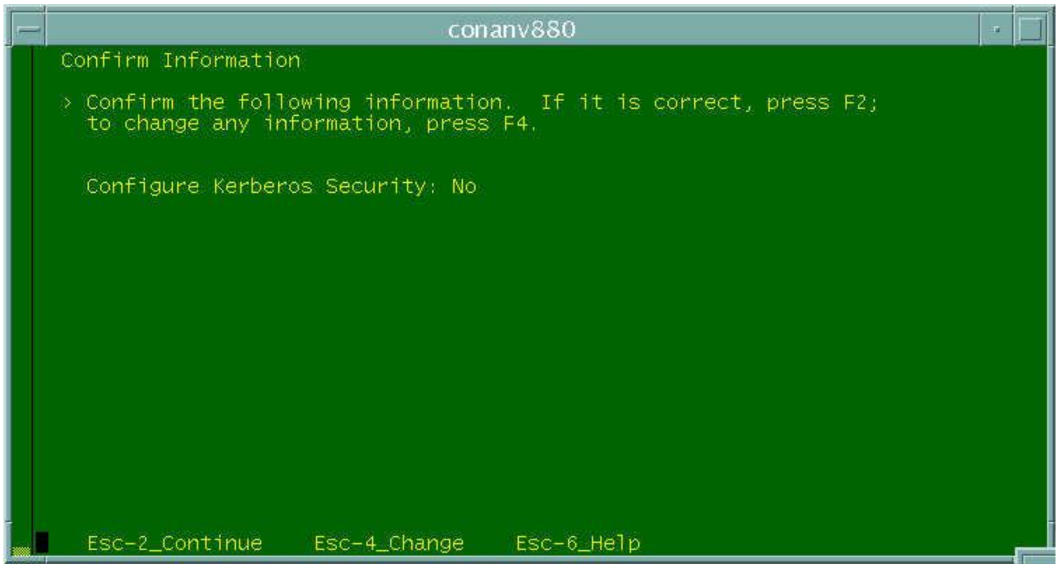
16 Review the configuration and press **Esc+2**. The window prompts you to specify whether your system will use the Kerberos security.

Note: If you need to change any configuration parameters, press Esc+4, and then follow on-screen instructions to make any changes.



```
Configure Security Policy:

Specify Yes if the system will use the Kerberos security mechanism.

Specify No if this system will use standard UNIX security.

    Configure Kerberos Security

    [ ] Yes
    [X] No











   Esc-2_Continue    Esc-6_Help
```

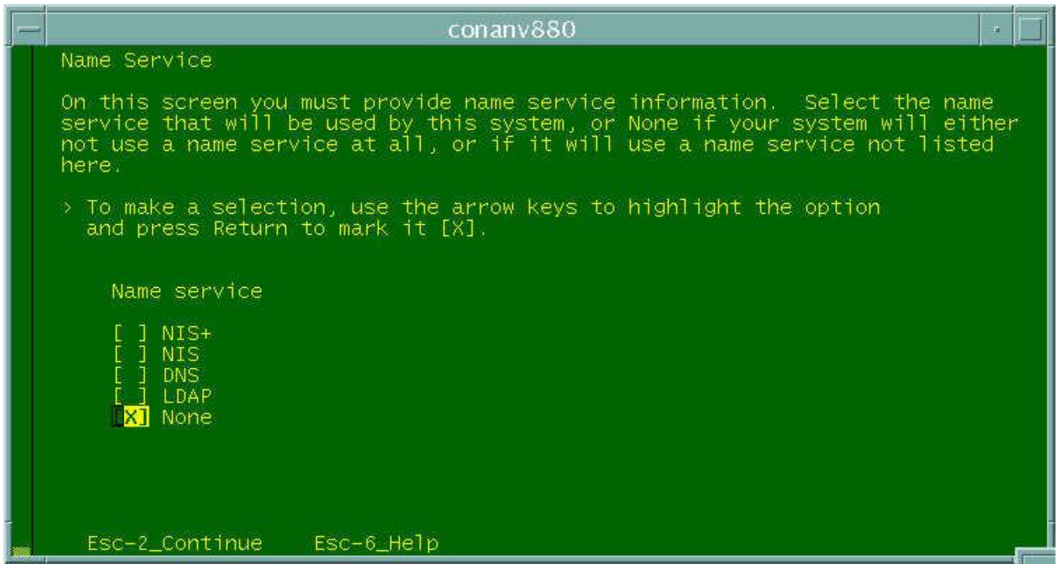
17 Select **No** and press **Esc+2**. The window updates to ask you to confirm that you made the correct selection regarding Kerberos network security.



```
conanv880
Confirm Information

> Confirm the following information.  If it is correct, press F2;
  to change any information, press F4.

  Configure Kerberos Security: No



  Esc-2_Continue    Esc-4_Change    Esc-6_Help
```

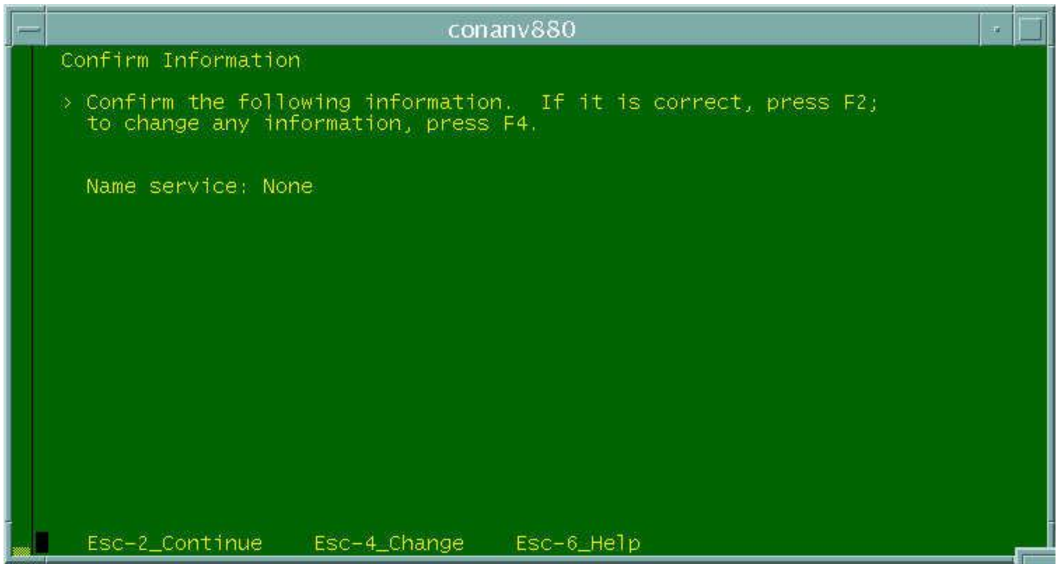
18 Review the Kerberos configuration and press **Esc+2**. The window prompts you to select the Name service for your system.

Note: If you need to change the Kerberos configuration, press Esc+4, and then follow on-screen instructions to make the change.



```
conanv880
Name Service

On this screen you must provide name service information.  Select the name
service that will be used by this system, or None if your system will either
not use a name service at all, or if it will use a name service not listed
here.

> To make a selection, use the arrow keys to highlight the option
  and press Return to mark it [X].


    Name service

    [ ] NIS+
    [ ] NIS
    [ ] DNS
    [ ] LDAP
    [X] None



  Esc-2_Continue    Esc-6_Help
```

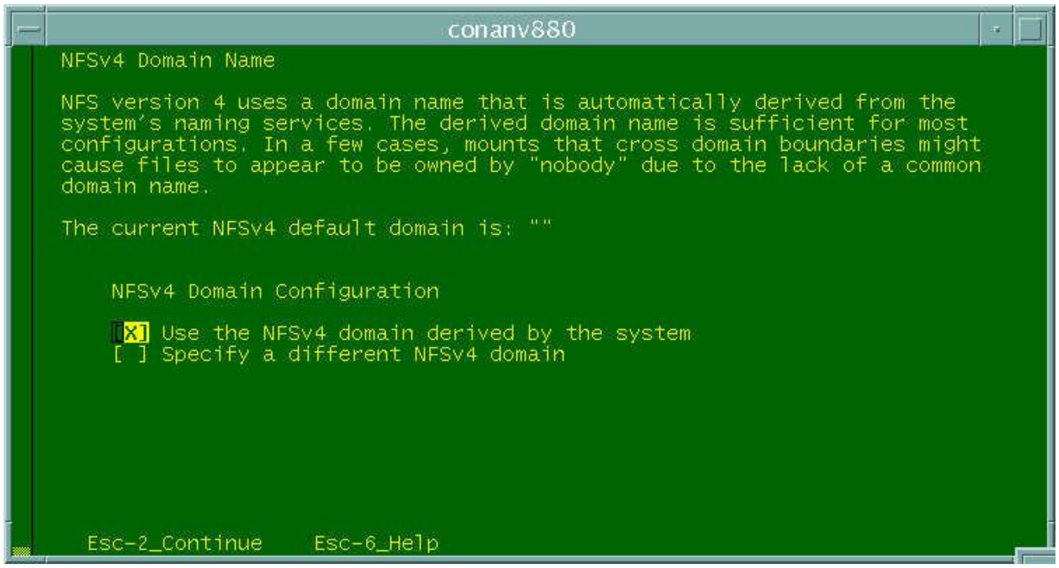
19 Select **None** and press **Esc+2**. The window prompts you to confirm that you made the correct decision regarding the Name service.



```
Confirm Information

> Confirm the following information.  If it is correct, press F2;
  to change any information, press F4.


  Name service: None
```

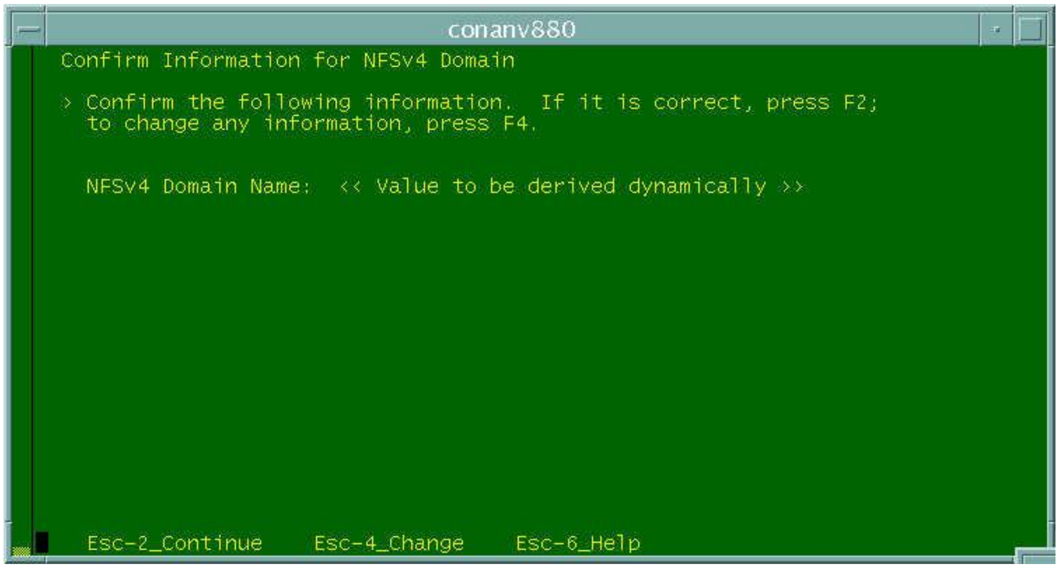
20 Review the Name service configuration and press **Esc+2**. The window prompts you to select your NFSv4 Domain Name.

Note: If you need to change the Name service configuration, press Esc+4, and then follow on-screen instructions to make the change.



```
NFSv4 Domain Name

NFS version 4 uses a domain name that is automatically derived from the
system's naming services. The derived domain name is sufficient for most
configurations. In a few cases, mounts that cross domain boundaries might
cause files to appear to be owned by "nobody" due to the lack of a common
domain name.

The current NFSv4 default domain is: ""


    NFSv4 Domain Configuration

    [X] Use the NFSv4 domain derived by the system
    [ ] Specify a different NFSv4 domain
```

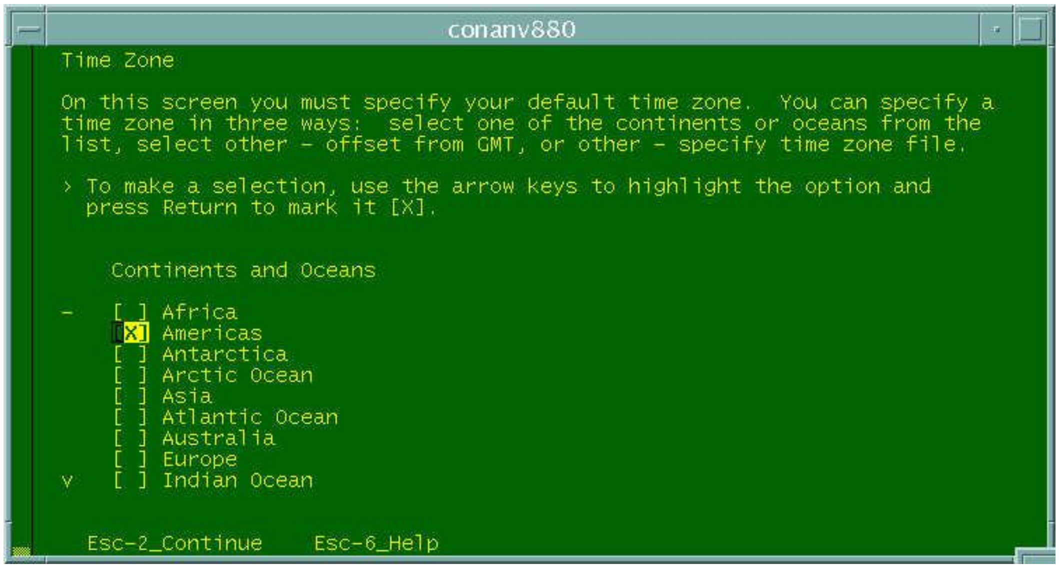
21 Select **Use the NFSv4 domain derived by the system** and press **Esc+2**. The window updates to ask you to confirm that you made the correct selection regarding NFSv4 Domain Configuration.



```
conanv880
Confirm Information for NFSv4 Domain

> Confirm the following information.  If it is correct, press F2;
  to change any information, press F4.

  NFSv4 Domain Name:  << Value to be derived dynamically >>

  Esc-2_Continue    Esc-4_Change    Esc-6_Help
```

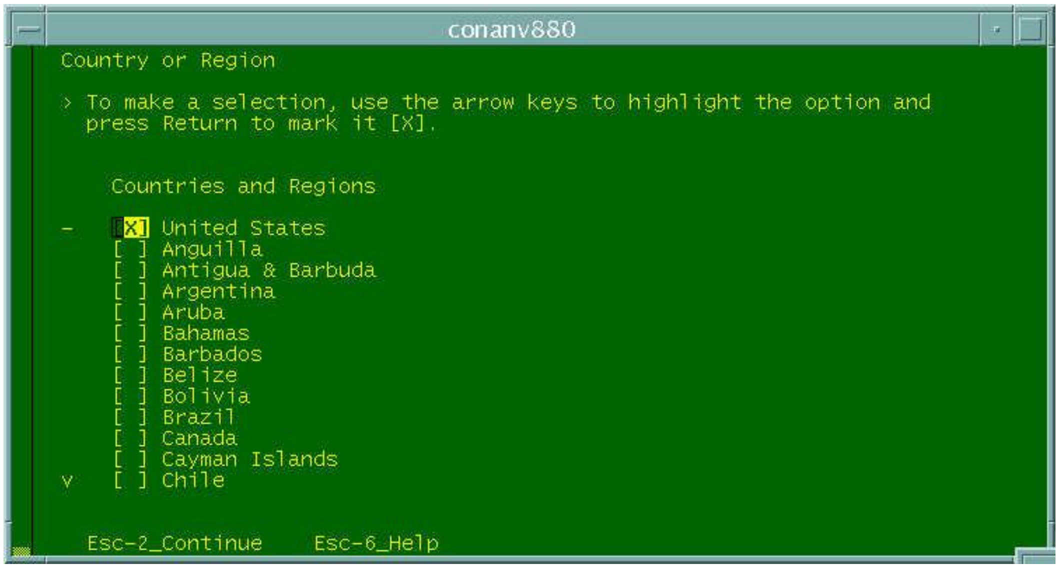
22 Review the NFSv4 Domain Name configuration and press **Esc+2**. The window prompts you to select your default time zone.

Note: If you need to change the NFSv4 Domain Name configuration, press Esc+4, and then follow on-screen instructions to make the change.



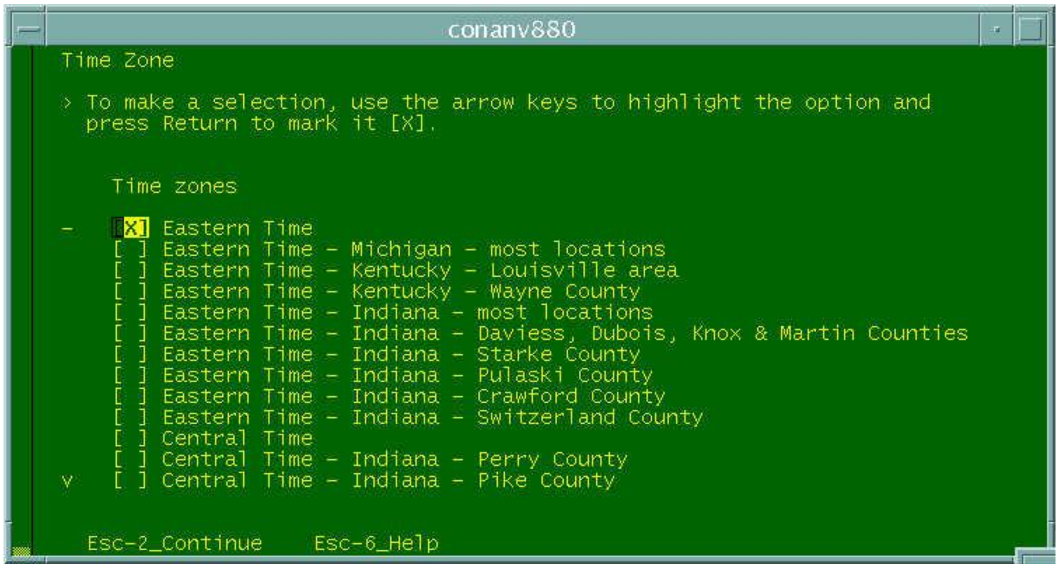
```
conanv880
Time Zone

On this screen you must specify your default time zone.  You can specify a
time zone in three ways:  select one of the continents or oceans from the
list, select other - offset from GMT, or other - specify time zone file.

> To make a selection, use the arrow keys to highlight the option and
  press Return to mark it [X].

    Continents and Oceans

-   [ ] Africa
    [X] Americas
    [ ] Antarctica
    [ ] Arctic Ocean
    [ ] Asia
    [ ] Atlantic Ocean
    [ ] Australia
    [ ] Europe
v   [ ] Indian Ocean

  Esc-2_Continue    Esc-6_Help
```

23 Select **Americas** and press **Esc+2**. The window prompts you to specify the appropriate country or region.



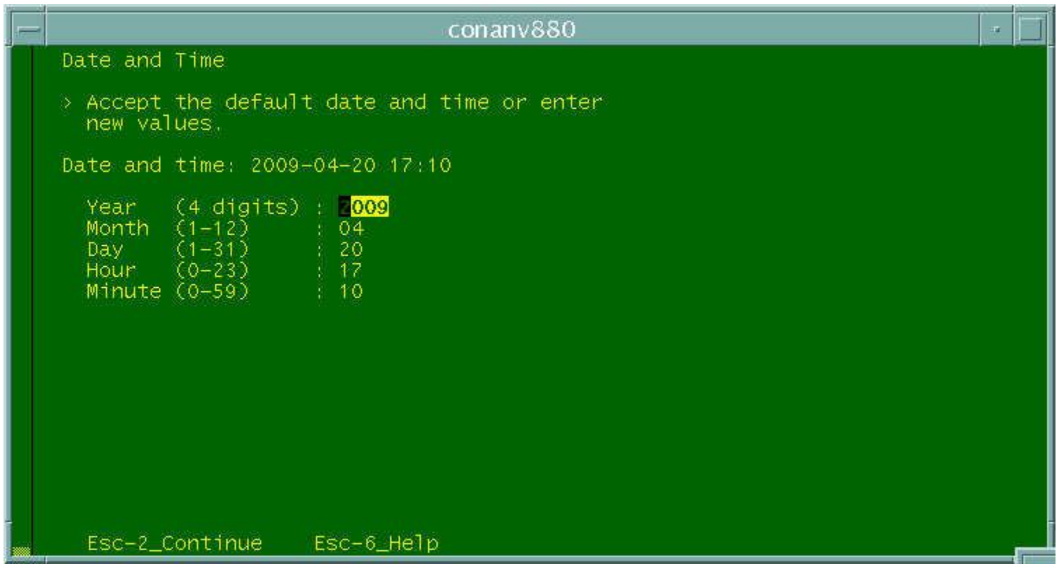
```
Country or Region

> To make a selection, use the arrow keys to highlight the option and
  press Return to mark it [X].


    Countries and Regions

-   [X] United States
    [ ] Anguilla
    [ ] Antigua & Barbuda
    [ ] Argentina
    [ ] Aruba
    [ ] Bahamas
    [ ] Barbados
    [ ] Belize
    [ ] Bolivia
    [ ] Brazil
    [ ] Canada
    [ ] Cayman Islands
v   [ ] Chile


  Esc-2_Continue    Esc-6_Help
```

24 Select the appropriate country or region and press **Esc+2**. The window prompts you to select the appropriate time zone.



```
Time Zone

> To make a selection, use the arrow keys to highlight the option and
  press Return to mark it [X].


    Time zones

-   [X] Eastern Time
    [ ] Eastern Time - Michigan - most locations
    [ ] Eastern Time - Kentucky - Louisville area
    [ ] Eastern Time - Kentucky - Wayne County
    [ ] Eastern Time - Indiana - most locations
    [ ] Eastern Time - Indiana - Daviess, Dubois, Knox & Martin Counties
    [ ] Eastern Time - Indiana - Starke County
    [ ] Eastern Time - Indiana - Pulaski County
    [ ] Eastern Time - Indiana - Crawford County
    [ ] Eastern Time - Indiana - Switzerland County
    [ ] Central Time
    [ ] Central Time - Indiana - Perry County
v   [ ] Central Time - Indiana - Pike County


  Esc-2_Continue    Esc-6_Help
```

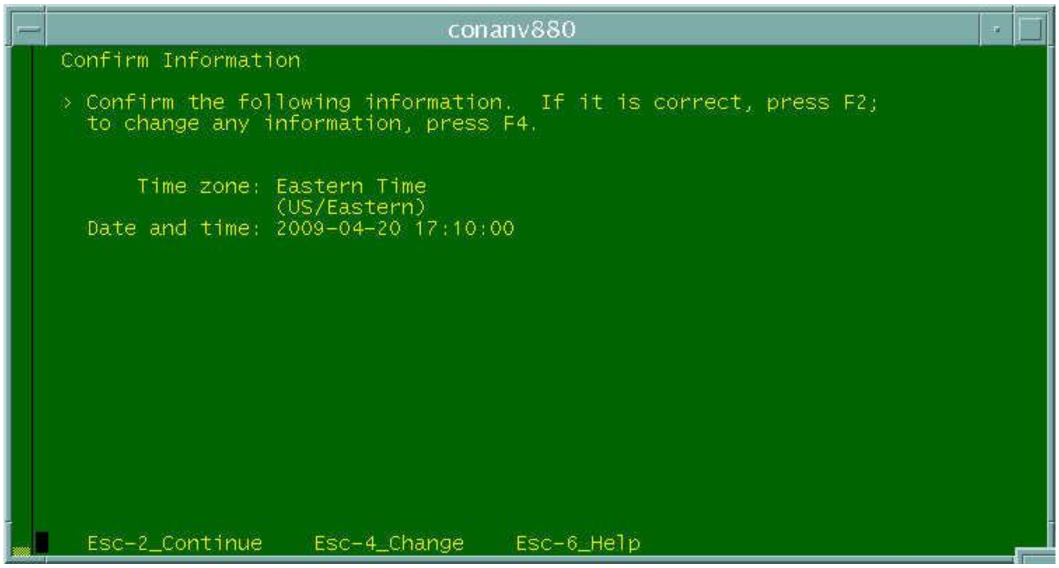
25 Select the appropriate time zone and press **Esc+2**. The window prompts you to select the appropriate time and date.



```
conanv880
Date and Time

> Accept the default date and time or enter
  new values.

Date and time: 2009-04-20 17:10

  Year   (4 digits) : 2009
  Month  (1-12)     : 04
  Day    (1-31)     : 20
  Hour   (0-23)     : 17
  Minute (0-59)     : 10

  Esc-2_Continue    Esc-6_Help
```

26 Select the default value, if it is correct, or type in the correct values and press **Esc+2**. The window prompts you to confirm the date and time information.

The installation completes and the login prompt appears.



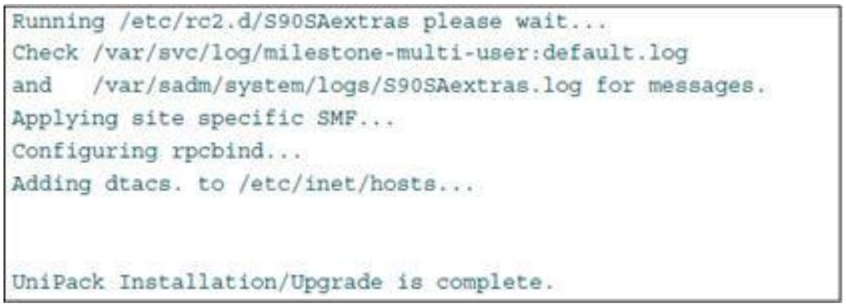
```
conanv880
Confirm Information

> Confirm the following information.  If it is correct, press F2;
  to change any information, press F4.


      Time zone: Eastern Time
                 (US/Eastern)
  Date and time: 2009-04-20 17:10:00

  Esc-2_Continue    Esc-4_Change    Esc-6_Help
```

27 Review the date and time information and press **Esc+2**. The window updates and asks you to provide the root password for the system.

Notes:

- If you need to change the date and time information, press **Esc+4**, and then follow on-screen instructions to make the change.
- The system runs the installation scripts on the DVD and displays information about the progress of the installation on the server's console.
- A message appears when the installation is complete.

Example:



```
Running /etc/rc2.d/S90SAextras please wait...
Check /var/svc/log/milestone-multi-user:default.log
and   /var/sadm/system/logs/S90SAextras.log for messages.
Applying site specific SMF...
Configuring rpcbind...
Adding dtacs. to /etc/inet/hosts...


UniPack Installation/Upgrade is complete.
```

28 When a message indicates that the installation is complete, type the root password and then press **Enter**. The system asks you to type the root password again.

29 Type the root password a second time and press **Esc+2**. The installation process continues and the console login prompt appears then the installation process has completed.

30 Login as **root** user.

31 Go to ***Post-Installation Tasks*** (on page 59).

4

Upgrade the DTACS Server Software Using a DVD

Introduction

This chapter provides procedures to upgrade the DTACS Server using a DVD. You will use these procedures to perform a major upgrade.

Important:

- If you are performing a CD upgrade, do not use these procedures. You should use the procedures in ***Upgrade the DTACS Server Software Using CDs*** (on page 53) instead.
- This procedure makes use of Live Upgrade, which is a Solaris utility that allows operating system or application upgrades in an inactive boot environment while the active boot environment continues to run without interruption. Therefore, *do not shut down the DTACS processes* until you are instructed to do so.

In This Chapter

Upgrade DTACS Software

Detaching File System Mirrors

Follow this procedure to temporarily detach the file system mirrors on the T5220 or T5440 DTACS server. File system mirrors refer to the mirrors of the DTACS server that contain file system data.

1 As **root** user, type **metastat | more** and press **Enter**. The system displays the status of all the metadevices on the DTACS server.

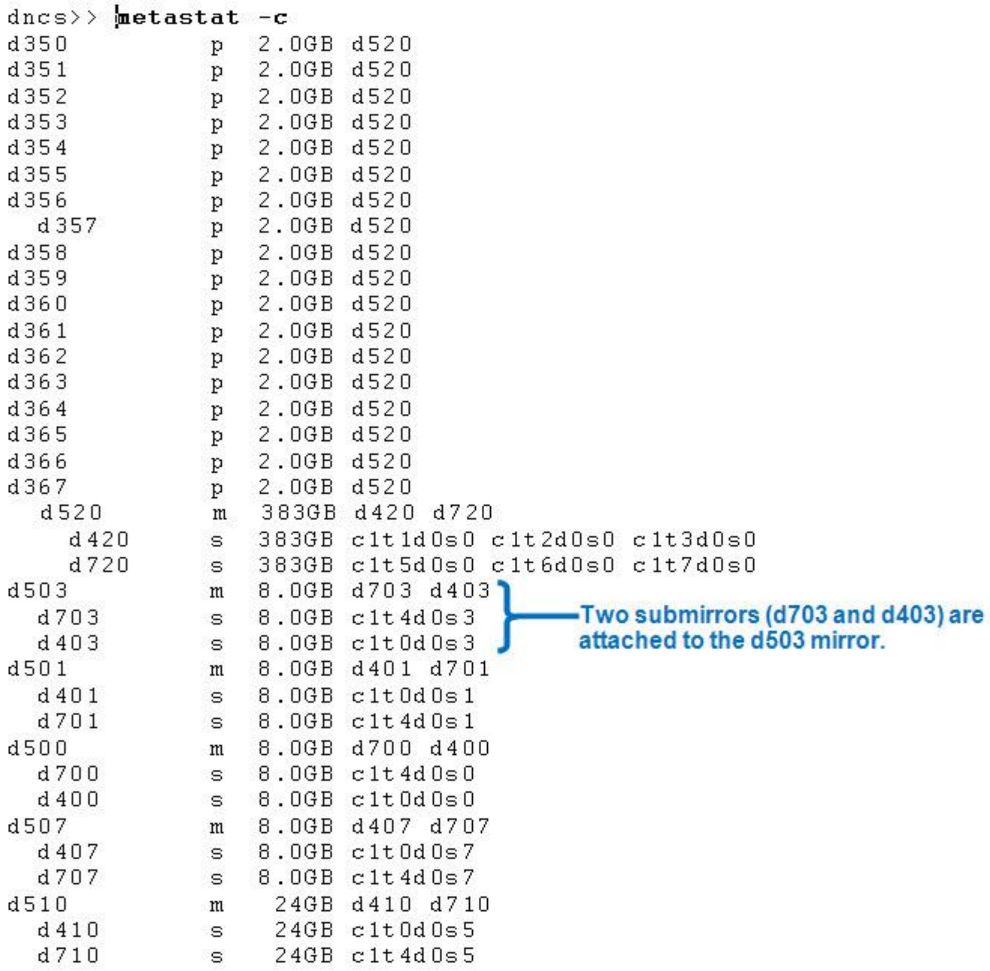
   Note: Press the **spacebar**, if necessary, to page through the output.

2 Do all of the metadevices display a state of **Okay**?

   - If **yes**, go to step 3.
   - If **no**, call Cisco Services.

3 Type **metastat -c** and press **Enter** to verify whether or not the mirrors are attached. Each device should be mirrored and should have two submirrors listed under each mirror device:

Example:



```
dncs>> metastat -c
d350            p   2.0GB d520
d351            p   2.0GB d520
d352            p   2.0GB d520
d353            p   2.0GB d520
d354            p   2.0GB d520
d355            p   2.0GB d520
d356            p   2.0GB d520
  d357          p   2.0GB d520
d358            p   2.0GB d520
d359            p   2.0GB d520
d360            p   2.0GB d520
d361            p   2.0GB d520
d362            p   2.0GB d520
d363            p   2.0GB d520
d364            p   2.0GB d520
d365            p   2.0GB d520
d366            p   2.0GB d520
d367            p   2.0GB d520
  d520          m   383GB d420 d720
    d420        s   383GB c1t1d0s0 c1t2d0s0 c1t3d0s0
    d720        s   383GB c1t5d0s0 c1t6d0s0 c1t7d0s0
d503            m   8.0GB d703 d403
  d703          s   8.0GB c1t4d0s3
  d403          s   8.0GB c1t0d0s3
d501            m   8.0GB d401 d701
  d401          s   8.0GB c1t0d0s1
  d701          s   8.0GB c1t4d0s1
d500            m   8.0GB d700 d400
  d700          s   8.0GB c1t4d0s0
  d400          s   8.0GB c1t0d0s0
d507            m   8.0GB d407 d707
  d407          s   8.0GB c1t0d0s7
  d707          s   8.0GB c1t4d0s7
d510            m    24GB d410 d710
  d410          s    24GB c1t0d0s5
  d710          s    24GB c1t4d0s5
```

Two submirrors (d703 and d403) are attached to the d503 mirror.

Important: If any metadevice is followed by an indicator listed in parentheses, then the metadevice is not Okay. Call Cisco Services.

4 Are all of the mirrors attached?

- If **yes**, go to step 5.
- If **no**, type **/cdrom/cdrom0/s3/sai/scripts/attach_mirrors** and press **Enter**.

  Note: Attaching the mirrors may take an hour or longer.

5 Type /**cdrom/cdrom0/s3/sai/scripts/detach_UFSmirrors** and press **Enter**. A confirmation message appears.

6 Type **y** and then press **Enter**. The system checks for metadevice errors, disables the file system mirroring function on the DTACS server, and displays the following message: **Successfully detached UFS submirrors on this machine**

7 Type **metastat -c** and then press **Enter** to view the current status of the file system mirrors. The d7xx file system mirrors should now be detached.

Note: The d7xx database mirrors are still attached. They are detached during the execution of the detach_DBmirrors script.

Remove POD_Data Directory

If you are upgrading from DTACS 1.1 to DTACS 1.2, you must remove the POD_Data directory before you proceed. This procedure helps to ensure that the database sync you perform later will be successful.

Important: This procedure is only necessary if you are upgrading from DTACS 1.1 to DTACS 1.2. If you are upgrading from any version of DTACS 1.2, you should skip this procedure and go to ***Upgrading a DTACS Server*** (on page 48).

1 Type **cd /dvs/dvsFiles** and press **Enter**.

2 Type **ls -l** and press **Enter**. Does the POD_Data directory exist?

- If **yes**, type **rm -R POD_Data** and press **Enter** to delete the directory. Then, go to ***Upgrading a DTACS Server*** (on page 48).
- If **no**, go to ***Upgrading a DTACS Server*** (on page 48)

Upgrading a DTACS Server

Note: Before you begin, be sure that you have backed up the file system to tape and backed up the database. Refer to Back Up the System (Upgrades Only) for more information.

1 Type **/cdrom/cdrom0/s3/sai/scripts/doLiveUpgrade** and press **Enter**. The system displays a message about the Live Upgrade and asks if you want to continue.

2 Type **y** and then press **Enter**.

Results:

- The system configuration is checked.

  Important: This system check should complete in about a minute. If the script that checks the system configuration takes longer than a few minutes to complete, call Cisco Services.
- The disk information is displayed.
- The live upgrade of the DTACS server occurs.

  The DTACS image is extracted on the unused disks of the DTACS server. This step may take 30 minutes or longer to complete.
- The system asks if you want to back up the key files.

  Important:

  – Ignore any on-screen directives to reboot the system.

  – **You must back up any user accounts that you previously created.** These accounts are located in the /export/home directory path (for example, /export/home/admin1).

  – You must back up the directory path where your download images reside (for example, /dvs/dtacs/dtacsFiles).

3 Type **y** and press **Enter**.

Results:

- The system lists the key files and directories that will be backed up and restored as part of the upgrade.
- The system asks if you want to add to the above list.

4 Examine the list of key files and directories that will be backed up. Do you want to add any key files or directories?

- If **yes**, type **y** and press **Enter**, then follow the on-screen instructions. When you are finished, type **n** and press **Enter**.
- If **no**, type **n** and press **Enter**.

Result: The system displays a **Do you want to continue?** message.

5 Type **y** and press **Enter**. The system generates a key file list and backs up the key files.

6 Did the backup of key files complete without error?

- If **yes**, the system resets the eeprom boot device and doLiveUpgrade completes.
- If **no**, contact Cisco Services.

7 Type **more /var/sadm/system/logs/doLiveUprade.log** and then press **Enter** to review the installation log file.

Note: Troubleshoot any issues you encounter to the best of your ability. Call Cisco Services for assistance, if required.

Stop the cron Jobs

To stop the cron jobs, type **svcadm -v disable -s cron** and press **Enter**. The system stops all cron jobs on the DTACS Server.

Stop the DTACS Processes

⚠ **CAUTION:**

The remaining procedures in this chapter and the following chapter need to be completed in a maintenance window.

Stop DTACS Processes

1 From an administrator window, type **sux - dtacs** and press **Enter**.

2 Enter the password for the dtacs users when prompted.

3 Type **dtacsStop** and press **Enter**. The DTACS processes begin to stop.

4 Type **pgrep -fl dvs** and press **Enter** to verify that the processes have stopped.

Note: You can also monitor the processes from the WUI.

5 Close all DTACS-related WUIs.

6 Type **exit** and press **Enter** to exit the DTACS user. You are now an administrative user.

7 As root user, type **showActiveSessions** and press **Enter**. One of the following messages appears:

- A message indicating that the INFORMIXSERVER is Idle, **OR**
- A message listing active sessions

8 Did the message in step 8 indicate that there are active sessions?

- If **yes**, follow these instructions.

  i Type **killActiveSessions** and press **Enter**. The system removes all active sessions from the database.

  ii Type **showActiveSessions** and press **Enter**.

  iii If a message appears indicating that there are active sessions, wait a few minutes and then repeat steps a and b. Call Cisco Services if there are still active sessions after you repeat steps a and b.

- If **no**, go to ***Detaching Database Mirrors*** (on page 50).

Detaching Database Mirrors

1 Type **/cdrom/cdrom0/s3/sai/scripts/detach_DBmirrors** and then press **Enter**. The following message appears:

```
This script will detach Database submirrors so that they can be used during
the Live Upgrade (LU) process.


If you are not SURE what this means, please quit now.


Are you SURE you want to do this?
```

2 Type **y** and then press **Enter**. The following message appears:

```
After the Database submirrors are detached, the machine needs to be booted
using the upgrade disks. So answer "yes" when prompted about activating the
Alternate Boot Environment (ABE).


Do you want to activate the Alternate Boot Environment?
```

3 Type **y** and then press **Enter**. The system detaches the database mirrors, and the "Activation of boot environment DTACS successful" message appears at the conclusion of the script.

4 Type **lustatus** and press **Enter**.

Example: You should see output similar to the following. This example shows that the new system release will be active upon reboot.

```
Boot Environment          Is         Active   Active     Can     Copy
Name                      Complete   Now      On Reboot  Delete  Status
-----------------------------------------------------------------------
SAIdtacs_1.1.0.4           yes        yes      no         no       -
DTACS                      yes        no       yes        no       -
```

If the output that you see does not resemble this example, call Cisco Services.

5 Type **init 6** and press **Enter**.

Results:

- The DTACS reboots several times. On the first reboot, the system builds the disk mirrors and reboots.
- The system restores the Key Files and reboots.
- The system begins to build the new database and restores the dtacsdb database. This operation could take more than 45 minutes to complete, depending on the size of the database.

6 Log on to the CDE window of the DTACS as root user.

Important: Do *not* start DTACS processes.

7 Are you also performing a CD upgrade on the server?

- If **yes**, go to ***Upgrade the DTACS Server Software Using CDs*** (on page 53).
- If **no**, go to ***Post-Installation Tasks*** (on page 59).

5

Upgrade the DTACS Server Software Using CDs

Important: This chapter includes instructions both for performing a CD upgrade immediately after a DVD upgrade (live upgrade) and for performing a standalone CD upgrade. Please follow each step carefully to make sure that you execute the correct steps.

This chapter provides procedures to upgrade the DTACS Server using CDs. Use these procedures if you are performing a package install.

Important: If you are performing a DVD upgrade, do not use these procedures. You should use the procedures in ***Upgrade the DTACS Server Software Using a DVD*** (on page 45) instead.

In This Chapter

What is the Upgrade Path for the DTACS?

The CD upgrade procedure you use depends on the upgrade path for your DTACS. Depending on the upgrade path, go to one of the following sections:

- For a standalone CD upgrade, go to ***Check the Status of the Mirrors*** (on page 55).
- For a CD upgrade immediately following a DVD upgrade (live upgrade), go to ***Upgrade a DTACS Server from a CD*** (on page 57).

Check the Status of the Mirrors

Note: Before you begin, be sure that you have backed up the file system to tape and backed up the database. Refer to Back Up the System (Upgrades Only) for more information.

1. Log in as a dtacs user and type **pgrep -fl dvs** and press **Enter**.
2. Does the system indicate that all of the processes, including dtacsInitd, are running?
   - If **yes**, go to step 3.
   - If **no**,type **dtacsStart** and press **Enter** to start all of the processes. Then, go to step 3.
3. Check the operation of your system (for example, are all processes green).
4. Is your DTACS operating properly?
   - If **yes**, go to step 5.
   - If **no**, troubleshoot your system or call Cisco Services to remedy any issues. Once the system is operating correctly, go to step 5.
5. Type **metastat -c** and press **Enter** to check the status of the mirrors. Each device should be mirrored and should have two submirrors underneath it.

   Example:

   ```
   .
   .
   .
   d520     m
      d720  s
      d420  s
   d500     m
      d700  s
      d400  s
   .
   .
   .
   ```
6. As a dtacs user, type **dtacsStop** and press **Enter** to stop all of the dtacs processes. Use **pgrep -fl dvs** to verify that all of the processes are stopped before you go to step 7.
7. Close all DTACS WUIs.
8. Type **dtacsKill** and press **Enter** to kill the dtacsInitd process. Use **pgrep -fl dvs** to verify that dtacsInitd does not appear in the output before you go to step 9.
9. Insert the most recent DTACS maintenance DVD.
10. Type **/cdrom/cdrom0/s3/backup_restore/mirrState -d** and press **Enter** to detach the mirrors.

11 Type **metastat -c** and press **Enter**. The output should appear similar to the following example:

```
.
.
.
d520    m
   d420 s
d500    m
   d400 s
.
.
.
```

12 Go to ***Upgrade a DTACS Server from a CD*** (on page 57) to continue.

Upgrade a DTACS Server from a CD

1. Remove the maintenance DVD and insert the upgrade CD.
2. Type **cd /cdrom/cdrom0** and press **Enter**.
3. Type **install_pkg** and press **Enter**.
   - **a** Type **y** to continue
   - **b** Press **Enter** to continue. The system asks if you have backed up your DNCS host.
   - **c** Type **yes** and press **Enter**.
   - **d** Type **d** (default) or enter a value and then press **Enter** to define the number of days before EMMs are deleted. The system prompts you to confirm the installation configuration.
   - **e** Review the install configuration parameters. If they are OK, press **c** to continue. Otherwise, follow the on-screen instructions to modify.
4. When complete, check the following logs for errors:
   - - /var/log
   - - /dvs/dtacs/tmp/corefiles (check for any core dumps)
   - - /var/sadm/system/logs (includes install logs).

   You should see messages that say **SUCCESS: No differences found for dtacsdb**.
5. Did you perform a DVD upgrade (live upgrade) prior to the CD upgrade?
   - If **yes**, go to ***Post-Installation Tasks*** (on page 59).
   - If **no**, go to step 6.
6. Change to dtacs user; then type **dtacsStart** and press **Enter** to restart the DTACS processes.

   Important: If all WUIs do not display, you should stop and restart Tomcat by entering the following as root:

   ```
   # svcadm disable svc:/network/apache-tomcat:default
   # svcadm enable svc:/network/apache-tomcat:default
   ```
7. Is your DTACS system operating properly?
   - If **yes**, go to step 8.
   - If **no**, troubleshoot your system or call Cisco Services to remedy any issues. Once the system is operating correctly, go to step 8.
8. Remove the upgrade CD and re-insert the maintenance DVD.
9. Type **/cdrom/cdrom0/s3/backup_restore/mirrState -a** and press **Enter** to sync the mirrors.

6

Post-Installation Tasks

This chapter contains instructions for tasks that must be completed after DTACS has been installed for the first time.

In This Chapter

Check The Software Version Number

Follow these instructions to check the installed software versions on the DTACS server.

1 If necessary, insert the DTACS DVD into the DVD drive of the DTACS server.

2 Type **/cdrom/cdrom0/s3/sai/scripts/utils/listpkgs -i** and press **Enter**. The system displays a listing of installed packages

3 Record the version number in the Actual Results column of the accompanying table for each package name (Pkg Name) listed.

Component	Pkg Name	Expected Results	Actual Results
DTACS Application	SAIdtacs	d1.2.0.x	
DTACS Platform	SAIdtacsplat	1.0.0.x	
DTACS Help	SAIdtacshelp	1.2.0.x	
Tools	SAItools	4.2.1.x	
Solaris Patches	SAIpatch	4.5.0.x	
Simple Content Protection Update	SAIScpUpd	1.0.0.x	

4 Do the *first three digits* of the Actual Results match the first three digits of the Expected Results for each component in the table in step 3?

Important: The build number (the fourth digit of the version number) may differ.

- If **yes**, you have completed this procedure.
- If **no**, call Cisco Services and inform them of the discrepancy.

Verify the Ownership of /dvs/dtacs/OCDL

Follow these steps to verify that the owership of the /dvs/dtacs/OCDL directory is correct:

1 Login as root user.

2 Type **cd /dvs/dtacs** and press **Enter** to change to the /dvs/dtacs directory.

3 Type **ls -la OCDL** and press **Enter** to view the ownership for the OCDL directory.

4 Does the system indicate that the ownership is dtacs:dtacs?

- If **yes**, then the directory ownership is correct.
- If **no**, then type **chown dtacs:dtacs OCDL** and press **Enter** to change the ownership.

Connect to the Monitor and Keyboard

If you have a monitor and keyboard to install, you should set them up now. Complete the following steps to connect a monitor and keyboard to your server and to set the system environment to use the monitor and keyboard for output and input.

Important: Only perform this procedure if you are attaching a keyboard and monitor to your DTACS Server.

Note: You should still have access to the DTACS Server via the ILOM port and be logged in as root user.

1. Attach the monitor's video cable to the graphics card's video port, and then tighten the thumbscrews to secure the connection.
2. Connect the monitor's power cord to an AC outlet.
3. Connect the USB keyboard cable to one USB port and the USB mouse cable to the other USB port on the DTACS Server server back panel.
4. If the ILOM prompt (→) does not appear, type **#.** and press **Enter**.
5. At the ILOM prompt, type **set /HOST send_break_action=break** and press **Enter**.
6. Type **start /SP/console -f** and press **Enter**.
7. When prompted, type **r** (for reset) and press **Enter**.
8. Does the OK prompt appear?
   - If **yes**, go to step 9.
   - If **no**, type **set /HOST send_break_action=break** and press **Enter** to send another break. The OK prompt appears. Go to step 9.
9. At the OK prompt, type **setenv input-device keyboard** and press **Enter**. The input device is now set to the keyboard.
10. At the OK prompt, type **setenv output-device screen** and press **Enter**. The output device is now set to the screen (monitor).
11. Type **shutdown -y -g0 -i6** and press **Enter**. The system reboots, and the monitor and keyboard are now the active input and output devices for the server.
12. Login as **root** user.

Verify the DTACS User ID (for New Installs)

Note: This procedure is only necessary if you have completed a new install. If you have upgraded an existing DTACS, you can skip this procedure and go to ***Build the Database*** (on page 65).

The DTACS server has enhanced security enabled. Enhanced security prevents the root user from logging in to the DTACS server remotely. You must use the DTACS server's console to log in as a root user.

Enhanced security also prevents you from directly logging into the server as the dtacs user. To access the dtacs account, you must login as a root or administrative user and then assume the role of a dtacs user by typing the **sux - dtacs** command.

1. As **root** user, type **sux - dtacs** at the system prompt to verify that a DTACS user id exists on the DTACS server.
2. Does the system prompt you to enter a password?
   - If **yes**, then the dtacs user exists. Go to step 3.
   - If **no** (a message indicates that the ID is unknown), the the dtacs user does not exist. Press **Enter** and go to ***Add Additional User Accounts*** (on page 64).
3. Type **exit** to return to root user.
4. Type **passwd dtacs** and press **Enter**. The system prompts you to enter a new password for the dtacs user.
5. Type a password for the dtacs user and press **Enter**. The system prompts you to re-enter the password.
6. Re-type the password for the dtacs user and press **Enter**.
7. Go to ***Add Additional User Accounts*** (on page 64) to create a new DTACS user ID with an administrative role.

Add Additional User Accounts

This procedure allows you to perform a couple of tasks:

- If the procedure ***Verify the DTACS User ID (for New Installs)*** (on page 63) indicated that the dtacs user does not exist, use this procedure to create a dtacs role.
- After you verify the user ID, use this procedure to create DTACS user accounts with other roles.

Follow these steps to add new user roles for the DTACS server.

1 Login to the DTACS server as a **root** user. The password prompt appears.

2 Type the password for the root user and press **Enter**. The root prompt appears.

3 Type **/dvs/dtacs/etc/create_users** and press **Enter**. A menu similar to the following example appears.

Example:

```
--------------------------
Choose Type of User to Add
--------------------------
1: Add Regular User (has no DTACS privileges)

2: Add Operator (has DTACS read privileges)
3: Add Administrator (has DTACS read & write privileges)
Please enter choice or 'Q' to exit:
```

4 Type **3** to add an administrator and press **Enter**. A message prompts you to enter a username.

Important: If you are creating the dtacs role, select option 1 and use **dtacs** as the user name.

5 Type the username **dtacsadm** and press **Enter**. A message prompts you to continue.

6 Type **y** to continue and press **Enter**. A message prompts you to enter a new password.

7 Type **2g3n3r!c** (the default password for the dtacsadm user) and press **Enter**. A prompt to re-enter the new password appears.

8 Re-type the password and press **Enter**. The new dtacsadm user is created.

9 Repeat these steps to create a user with the role of DTACS operator (option 2), if needed, or other users as desired.

Note: See ***Managing DTACS User Accounts*** (on page 137) for additional information about creating and deleting users on the DTACS server. The appendix also contains information about security on the DTACS server.

Build the Database

Complete the following steps to manually run the buildDtacsDb script and build the DTACS database.

Note: This procedure is *required* for an initial install of DTACSDVD1.2.x.x.

1. As **root**, type **buildDtacsDb** and press **Enter**.
2. When the database build completes, type **more /dvs/dtacs/convert.out** and press **Enter**.
3. Review the file and make sure there are no errors or warnings.
4. Were there errors or warnings?
   - If **yes**, call Cisco Services.
   - If **no**, go to step 5.
5. Did the file indicate that there were *No differences found*?
   - If **yes**, go to step 6.
   - If **no**, call Cisco Services.
6. Type **dbaccess dtacsdb -** and press **Enter**.
7. Were you able to access the DTACS database?
   - If **yes**, go to step 8.
   - If **no**, call Cisco Services.
8. At the > prompt within the database, type **select * from mc_config where mc_name="S-A DB Conversion";** and press **Enter**. The mc_param_date displays the version of DTACS code you just loaded.

   Example:

   ```
   mc_param_data   from 1.0_0_5_0 to 1.1_0_1_0 Attempt 1
   ```
9. Did the correct version of code display?
   - If **yes**, press **Ctrl+C** and press **Enter** to exit the database.
   - If **no**, call Cisco Services.

Edit Network Configuration Files (New Installs Only)

You must edit several network configuration files on the DTACS server. You can edit these files using any text editor on the system connected to the DTACS server's serial management port.

Note: You only need to complete this section if you are installing a new DTACS for the first time. If you are upgrading an existing DTACS, you can skip this section.

Important: The list of files that you will edit and the changes you will make will vary based on your site's specific configuration needs.

Contact your system administrator to obtain a list of files that you must edit along with the types of changes that are required for these files. For example, a typical list of files might include the following:

- /etc/rc2.d/S85SAspecial
- /etc/netmasks
- /etc/hosts
- /etc/hostname (network interface files)

  Note: When creating the /etc/hostname. files, the netmask should also be included. For example, `dtacs netmask 255.255.192.0 broadcast +`
- /etc/nodename
- /etc/defaultrouter
- /export/home/informix/etc/sqlhosts

  Note: You may need to add the following lines to the sqlhosts file:

  ```
  dtacsDbServer      onipcstr    dtacs      on_serveripc
  dncsatmDbServer    ontlitcp    dncsatm    informixOnline
  ```

Editing Network Interface Files

Network interface files will probably be on the list of files that must be edited. The network interface file names differ based on server type (T5220 or T5440). The following table lists network interface file names for each server.

T5220 file Names	T5440 File Names
/etc/hostname.e1000g0	/etc/hostname.nxge0
/etc/hostname.e1000g1	/etc/hostname.nxge1
/etc/hostname.e1000g2	/etc/hostname.nxge2

Set Environment Variables (New Installs Only)

The default settings for several important DTACS system variables may be overwritten in the **/export/home/dtacs/.profile** file on the DTACS server. You must verify, or set, the following environment variables in this file.

Notes:

- You only need to complete this section if you are installing a new DTACS for the first time. If you are upgrading an existing DTACS, you can skip this section.
- The default values will be appropriate in most circumstances. Unless otherwise directed, you should choose the default values during initial setup and adjust them later, if necessary.

Important: Whenever you change an environment variable in .profile, you must then source the file. Type **. /export/home/dtacs/.profile** and press **Enter**. (Be sure to type a space between the first . and /.) Then run the dtacsStop and dtacsStart commands.

Variable	Description
AMM_PERCENT_DATARATE	Used by ammDistributor to determine the maximum bandwidth to use as a percentage of the AMM IP stream datarate. The default rate is 80% and the allowed range is 20 to 80 percent.
COMM_MULTICAST_TTL	Overrides the Time-To-Live for IP packets sent by the dataPump.
DTACS_SCP_OPERATION_MODE_VALUE	Overrides the setting of the SCP operations mode when Full SCP or Fixed MPK features are enabled. The variable must be set to a non zero decimal value, otherwise it is ignored. For Full SCP mode, the default value is 0x90. For Fixed MPK mode, the default value is 0x80.
IP_STREAMER_TTL	Overrides the Time-To-Live for IP packets sent by dtacsIpStreamer. The default is 10.
NIT_MSG_RATE (units ms)	Specifies the number of seconds between DTACS system updates of the SCTE-65 Network Information Table (NIT). The default value is 5000 ms, which is once every 5 seconds.

Variable	Description
NTT_MSG_RATE (units ms)	Specifies the number of seconds between DTACS system updates of the SCTE-65 Network Text Table (NTT). The default value is 120,000 ms, which is once every 120 seconds.
SI_INSERT_RATE (units ms)	Specifies the number of seconds between DTACS system updates of the SCTE-65 Short Virtual Channel Table (S-VCT). The default value is 15,000 ms, which is once every 15 seconds. **Note:** This variable determines the rate of the Virtual Channel Map (VCM) and the Source Name Subtable (SNS). The VCM is part of the SVCT, but the SNS is not part of the table.
SYSTEM_TIME_RATE (units seconds)	Specifies the number of seconds between DTACS system updates of the SCTE-65 System Time Table (STT). The default value is 5 seconds.
USP_MAX_SITE_ERRORS	Specifies the limit of USP site announce AMMs that have a different controllerId than the one with which the DTA is provisioned. Once this limit is reached, the DTA will not provide audio and video services.
USP_POST_RESET_WAIT_SECS	Overrides the time to wait after sending Reset/Boot AMMs of the DTA before sending Config/Connect AMMs. The default is 120 seconds.
USP_REPEAT_CONNECT	Turns on periodic retransmission of the Connect AMM for activated DTAs. The default is not to send the Connect AMMs. The variable must be set to an non-zero decimal value, otherwise it is ignored.
USP_SITE_ANNOUNCE_SECS	Overrides the time between transmission of the Site Announce AMM. The default is 20 seconds.

Variable	Description
USP_TIMEOUT_POLICY	Specifies whether the message timeout counter will reset whenever the DTA receives certain messages. Possible values are: ■ **BOTH:** The counter resets whenever the DTA receives either a broadcast message (such as site announce) or a unicast message (such as config). This is the default value. ■ **UNICAST:** The counter only resets when the DTA receives a unicast message.

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.

Edit the /etc/group File

This section describes how to add dtacs to the DNCS entry in the /etc/group file on the DTACS.

1 As **root** user, open the **/etc/group** file in a text editor.

2 Locate the dncs entry and add dtacs to the end of the entry.

Example: dncs::500:dtacs

3 Locate the dtacs entry and add dncs to the end of the entry.

Example: dtacs::503:dncs

4 Save and close the file.

Create Entries in the site_info Database Table

Important:

- This procedure should be performed after you finish an *initial* installation of the DTACS software.
- Change Request number 106248 ("New installation of DTACS does not contain Site ID info") addresses this issue.

1. Type **dbaccess dtacsdb -** and press **Enter** to access the DTACS database.
2. At the **>** prompt, type **select * from site_info;** and press **Enter**.
3. Were there any entries in the site_info table?
   - If **yes**, go to ***Configure DTACS BOSS Proxying for DNCS (Optional)*** (on page 73).
   - If **no**, go to step 4.
4. At the **>** prompt, type **insert into site_info values (1, "DTACS", "00:00:00:00:00:00", "<dtacsatm_ipaddr>", "00:00:00:00:00:00", "dtacs", 1, "", "", 0);** and press **Enter**.

   Note: Substitute the IP address for the dtacsatm interface defined in the /etc/hosts file for <dtacsatm_ipaddr> in the above command.
5. At the **>** prompt, type **select * from site_info;** and press **Enter** to verify that the site_info table is now populated.
6. Press **Ctrl+C** to exit the DTACS database.

Configure DTACS BOSS Proxying for DNCS (Optional)

You can set up the Billing System to send BOSS transactions to DTACS if you prefer. DTACS will then forward any non-DTA related transactions to the associated DNCS. Follow these steps to configure the DTACS BOSS proxying for DNCS.

Note: Your system may or may not use a BOSS Proxy. If it does not, skip this section and go to ***Install Patches*** (on page 74).

1 Type **cd /dvs/dtacs/etc** and press **Enter** to change to the /dvs/dtacs/etc directory.

2 Type **ls -l *bossServer.cfg*** and press **Enter** to see if the bossServer.cfg file exists.

3 Does the system indicate that the bossServer.cfg file exists?

- If **yes**, then you do not need to do anything else. Go to ***Install Patches*** (on page 74).
- If **no**, type **cp bossServer.cfg.sample bossServer.cfg** and press **Enter** to create a new bossServer.cfg file from the sample configuration file provided. Then, go to ***Install Patches*** (on page 74).

Install Patches

If you have any patch software for the DTACS Server, install it now. Instructions for installing the patch software should accompany the DVD that contains the software.

Start DTACS Process and the WUI

Before Using the DTACS WUIs

Before you start using the DTACS WUI, please note these important points.

Understanding Channel Maps

The channel map of a BSG is determined by the channel map of the DNCS Hub ID that is associated with the BSG.

Understand PID Routes

PID routes are created automatically and are based on the sources in the VCTs. Therefore, you must configure VCTs before you edit PID Routes.

Note: MQAMs are the only element types that you can edit on the PID Route Provisioning WUI. You cannot edit GQAM element types.

Starting DTACS Processes

Important: If you attempt to start a DTACS process from the command line while all of the DTACS server processes are already running, you could cause the process to core dump or otherwise disrupt the normal operation of the DTACS server. If this occurs, you should send the core files and logs should to Cisco for evaluation.

1. Type **sux - dtacs** and then press **Enter** to assume the dtacs role. A prompt for the role's password appears.

   Important: If you have not yet created a password for the dtacs user, open a new window and switch to **root**. Type **passwd dtacs** and enter a password when prompted. Re-enter the password when prompted.

2. Type the dtacs password and press **Enter**. A system prompt appears and /export/home/dtacs becomes the active directory.

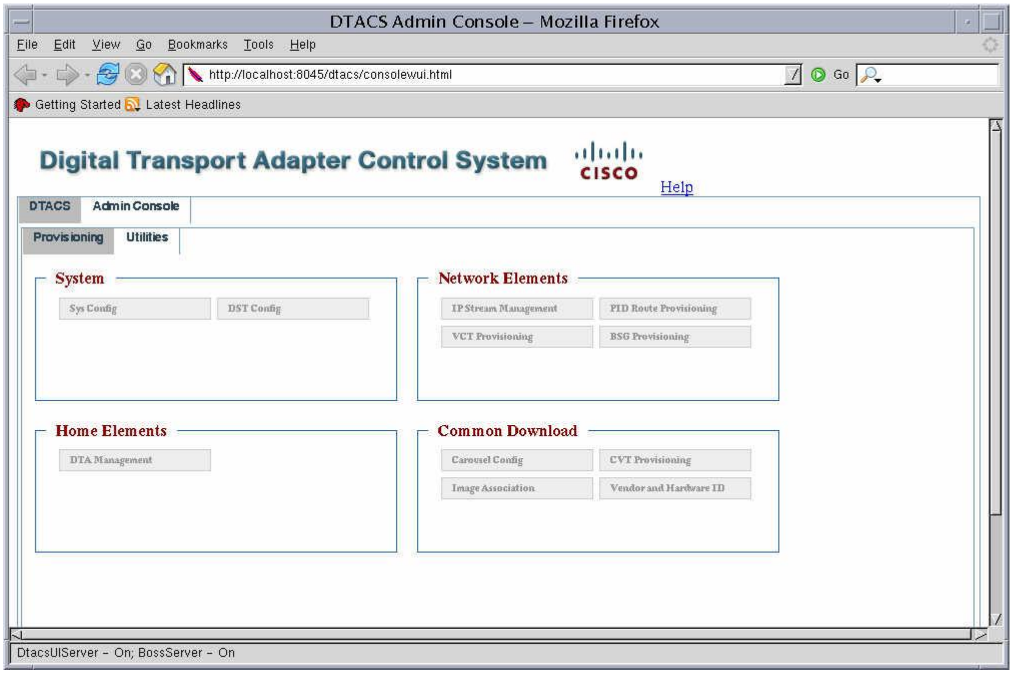
3. Type **dtacsStart** and press **Enter**. The dtacs processes start.

   Important: Be certain that you are starting the DTACS processes as dtacs user. Do not start the processes as root user.

4 Type **dtacsWUIStart** and press **Enter** to start the software and launch the interface.

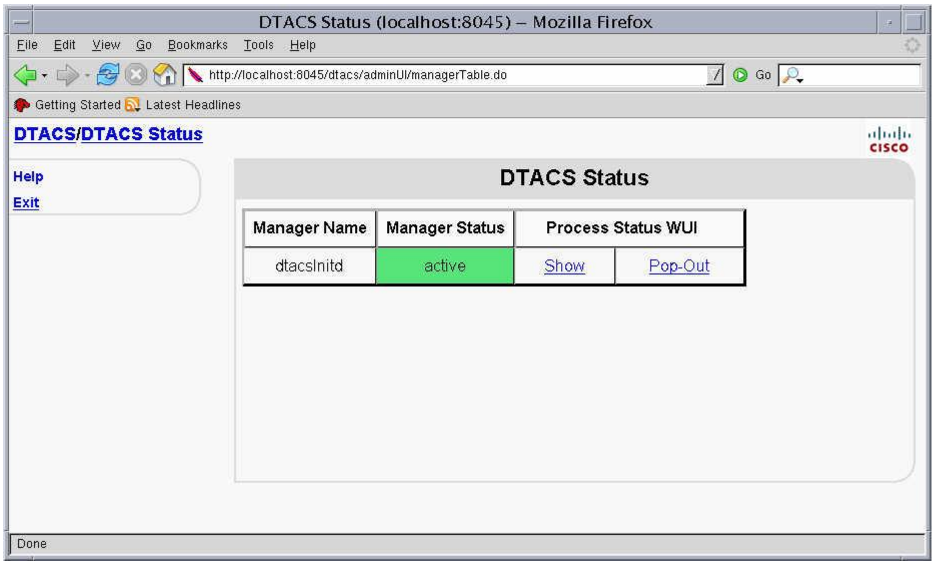
Results:

- If you are launching Firefox for the first time, click **Install Now** to install the application.
- The message 'Launching the DTACS Web UI page in Firefox' appears.
- The DTACS web user interface (WUI) appears.



5 Click the **Admin Console** tab to view the processes. The Admin Console window appears.

6 Click **DTACS Status**. The DTACS Status window appears.

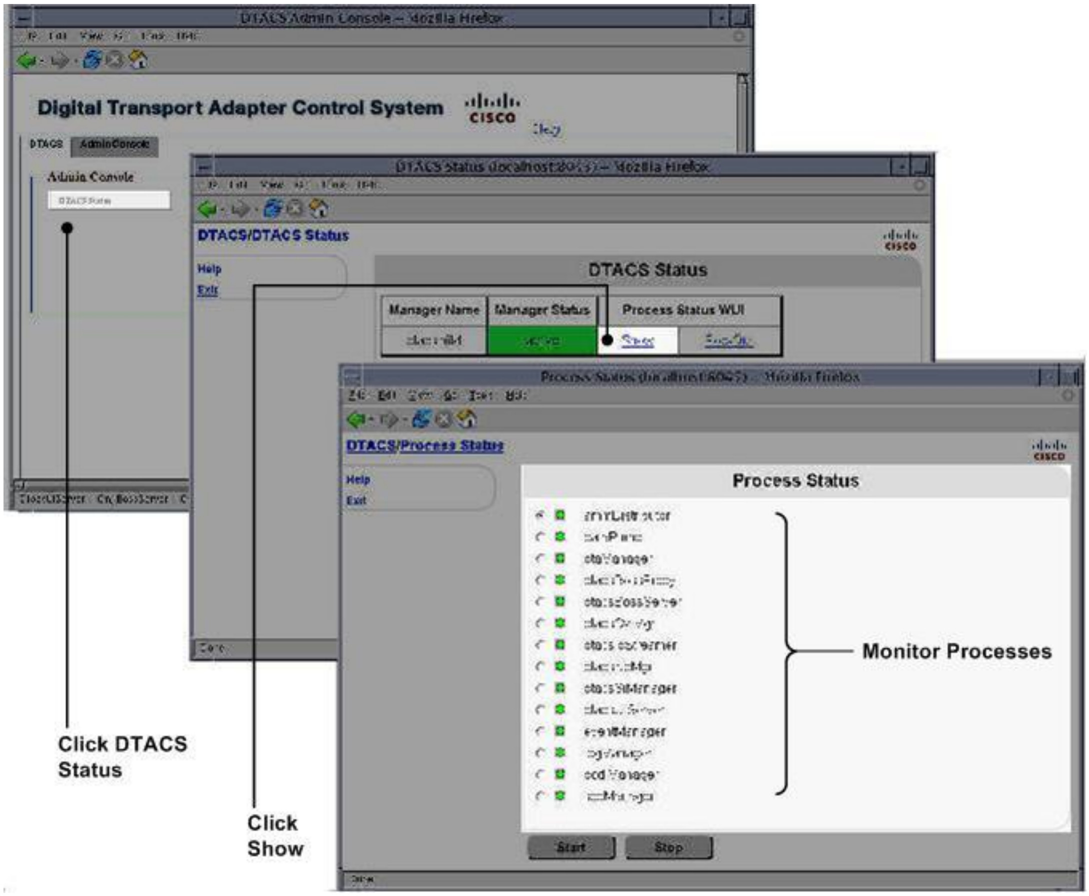

DTACS Status (localhost:8045) – Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8045/dtacs/adminUI/managerTable.do
Go
Getting Started Latest Headlines
DTACS/DTACS Status
CISCO
Help
Exit
Done

DTACS Status

Manager Name	Manager Status	Process Status WUI	
dtacsInitd	active	Show	Pop-Out

7 Choose one of the following to view status processes:

- Click **Show** to view the status of the processes in this window, OR
- Click **Pop-Out** to view the status of the processes in a separate window.



Click DTACS Status

Click Show

Monitor Processes

Each process running on the DTACS Server is listed next to a green, yellow or red indicator. The color of the the indicator shows the status of the process.

- Red means a process has stopped.
- Green means a process is running.
- Yellow means a process has paused.

Note: The color of the indicator may lag slightly behind the actual status of the process. If you stop or start a process, it may take a few seconds before the indicator changes color to show the change in status.

DTACS Processes

The following table briefly describes each of the DTACS processes.

Process	Description
ammDistributor	This process transmits Authentication Management Messages (AMMs) to Digital Transport Adapters (DTAs).
dataPump	This process pumps out encoded images to a specific IP/port combination.
dtacsBossProxy	This process handles backend processing of BOSS transactions that are not supported by DTACS.
dtacsBossServer	This process provides BOSS interfaces to DTACS.
dtacsCvtMgr	This process works with CD2-CVT files. It allows you to create, edit, delete and transmit CD2-CVT file data.
dtacsNeMgr	This process provisions and maintains network configurations that are used to setup PID routes and insert Simple Content Protection and Multi-Program Keys.
dtacsIpStreamer	This process generates System Information (SI) and channel map data transmits data to specific IP addresses.
dtacsSiManager	This process generates SI and channel map data.
dtacsUIServer	This process proxies WUI requests to the appropriate back-end process(es) and the Informix database. The dtacsUIServer process also returns responses from back-end processes and the database to the WUI.
dtaManager	This process provisions and manages DTA devices .
eventManager	This process provides a way to notify system components of events.
logManager	This process an internal process that manages debug logging levels of DTACS packages.
ocdlManager	This process handles requests from the WUI. It creates and manages associations and related CVTs, encodes images and interacts with the database to persist related data.
scpManager	This process provides key management for Simple Content Protection (SCP).

Attach Mirrors After a DVD Live Upgrade

Important: If you have performed a standalone CD upgrade and use mirrState -d to detach mirror, *do not* complete this procedure. You must use mirrState -a to attach mirrors as described in ***Upgrade a DTACS Server from a CD*** (on page 57).

Complete the following procedure *only* if you have installed DTACS server from a DVD.

Important: Be sure that you complete this procedure during the current maintenance window on the night of the server upgrade. If you wait until the following night to complete this procedure, the server will operate an entire day without its disk-mirroring functions in place.

Important Note to Consider

You should follow the procedure in this chapter only under one of the following circumstances:

- You are satisfied with the upgrade and want to commit the system changes. Rolling back an upgrade *after* completing this procedure is time-consuming and takes significant effort.
- You have rolled back from an unsuccessful DVD upgrade and want to synchronize the mirrors.

Attaching Mirrors After a DVD Live Upgrade

In this procedure, you will enable the server's disk-mirroring function of the server. Complete the following steps to log on to the DTACS server and attach the server's mirrors.

Note: It may take up to 60 minutes to complete this process.

1. Verify that the Maintenance DVD is in the DVD drive. If the DVD has been removed, insert it into the DVD drive.
2. Type **df -n** and then press **Enter**. A list of the mounted file systems appears.

   Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.
3. Log on to the DTACS Server as root user.
4. Type **/cdrom/cdrom0/s3/sai/scripts/attach_mirrors** and press **Enter**. A confirmation message appears.
5. Type **y** and press **Enter**. The system executes a script that attaches submirrors to their respective mirrors.
6. When the disk-mirroring function completes, type **eject cdrom** and press **Enter**.

7 Remove the Maintenance DVD from the DVD drive.

8 Type **exit** and then press **Enter**. The root user logs out of the DTACS Server.

7

Provision DTACS

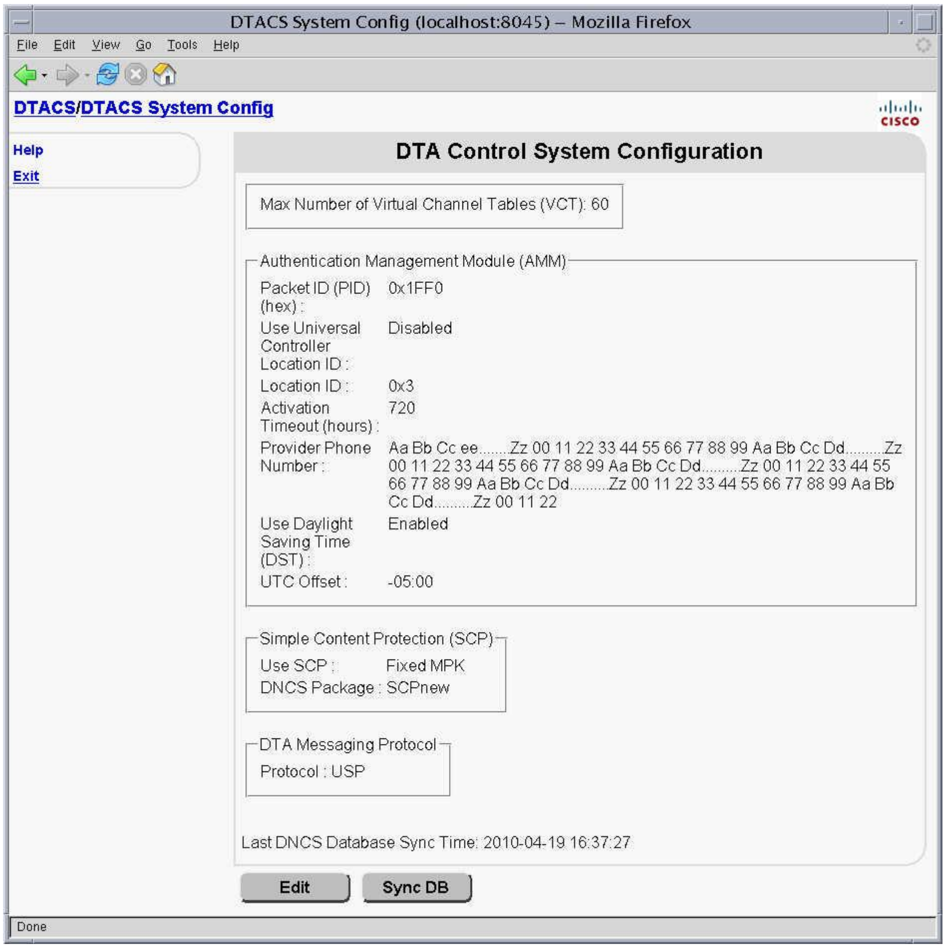
Introduction

This chapter explains how to provision the Digital Transport Adapter Control System.

In This Chapter

Configure the System

To configure the DTA Control System, click the **Sys Config** text on the DTA Control System's main page. The DTA Control System Configuration window appears.


DTACS System Config (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTACS System Config
cisco
Help
Exit
Edit
Sync DB
Done

DTA Control System Configuration

Max Number of Virtual Channel Tables (VCT): 60

Authentication Management Module (AMM)

Packet ID (PID) (hex) :	0x1FF0
Use Universal Controller Location ID :	Disabled
Location ID :	0x3
Activation Timeout (hours) :	720
Provider Phone Number :	Aa Bb Cc ee........Zz 00 11 22 33 44 55 66 77 88 99 Aa Bb Cc Dd.........Zz 00 11 22 33 44 55 66 77 88 99 Aa Bb Cc Dd.........Zz 00 11 22 33 44 55 66 77 88 99 Aa Bb Cc Dd.........Zz 00 11 22 33 44 55 66 77 88 99 Aa Bb Cc Dd.........Zz 00 11 22
Use Daylight Saving Time (DST) :	Enabled
UTC Offset :	-05:00

Simple Content Protection (SCP)

Use SCP :	Fixed MPK
DNCS Package :	SCPnew

DTA Messaging Protocol

Protocol : USP

Last DNCS Database Sync Time: 2010-04-19 16:37:27

Edit a System Configuration

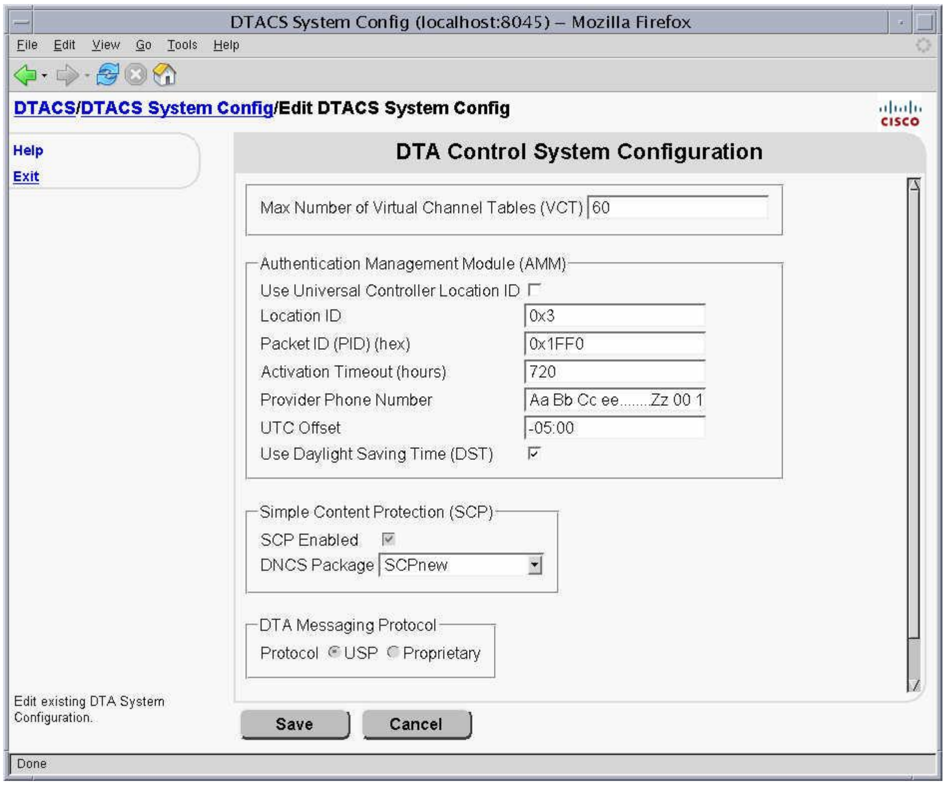
Follow these steps to edit a DTA Control System's configuration.

1 Click **Edit** on the DTA Control System Configuration window.

Results:

- The DTA Control System Configuration window appears with blank fields for text entry

- The 'Edit existing DTA System Configuration' message appears


DTACS System Config (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTACS System Config/Edit DTACS System Config
Help
Exit
Save
Cancel
Done

DTA Control System Configuration

Max Number of Virtual Channel Tables (VCT) 60

Authentication Management Module (AMM)

Use Universal Controller Location ID □

Location ID 0x3

Packet ID (PID) (hex) 0x1FF0

Activation Timeout (hours) 720

Provider Phone Number Aa Bb Cc ee.......Zz 00 1

UTC Offset -05:00

Use Daylight Saving Time (DST) ☑

Simple Content Protection (SCP)

SCP Enabled ☑

DNCS Package SCPnew

DTA Messaging Protocol

Protocol ● USP ○ Proprietary

Edit existing DTA System Configuration.

2 Press the Tab key to go to the field you want to change. The following table describes the fields that can be updated on this page.

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.

Field	Description
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.
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)	Lets you specify whether or not your site uses DST. ■ Enabled (checked) indicates that the system uses DST. ■ Disabled (unchecked) indicates that the system does not use DST.

Field	Description
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.	

3 Click **Save** to save your changes, or click **Cancel** if you want to leave this screen without saving changes.

Sync the Database

Important: Whenever you make changes to the channel map on the DNCS, you should wait until the SAM_UPDATE_TIME has been executed before you sync the database. This will allow for the normal DNCS operation to complete.

1 From the Edit DTACS System Config window, click **Sync DB** to synchronize data in the DNCS database with data in the DTACS database. The DTA Control System Configuration window appears, and the message **The DB Sync request processed successfully** appears in the lower-left corner of the window.

2 Click **Back to Console** to return to the DTACS main page.

Note: You can also click the DTACS text at the top of the window to return to the DTACS main page on any system configuration page.

Set Up SCP

Before you can set up Simple Content Protection (SCP), you must create a package to hold the encrypted segments of the sources on the DNCS. Then you must sync the database so that the new package appears on the DTACS user interface.

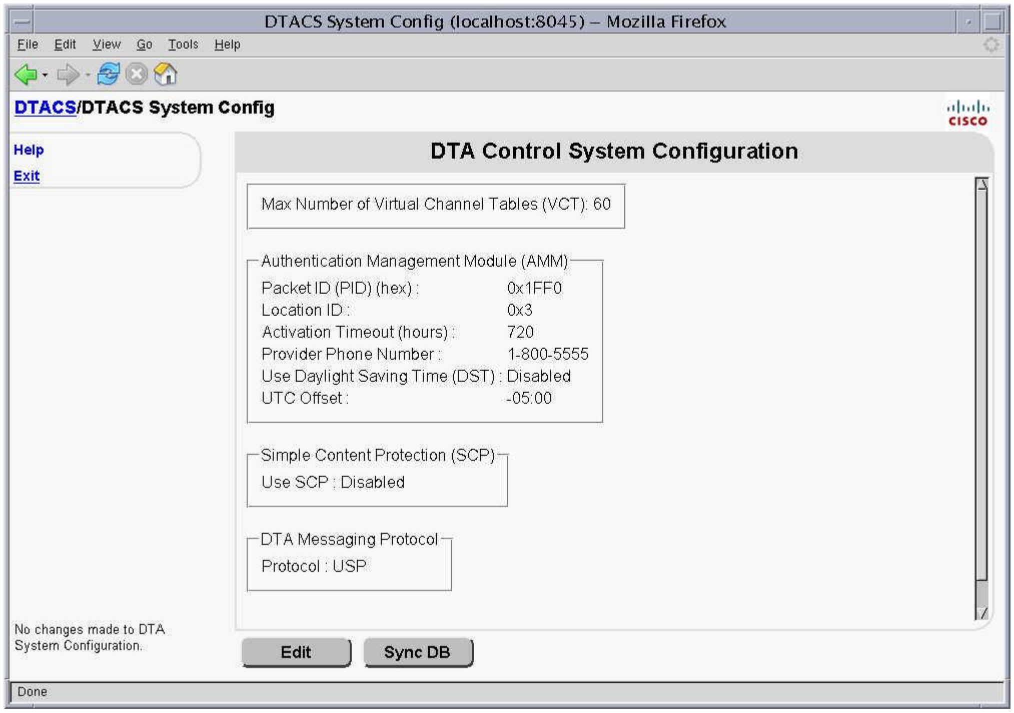
Note: SCP is a feature that Cisco Services must enable. Contact Cisco Services to make sure that this feature has already been set up before you begin.

Follow these steps to set up a package for encrypted sources. If you need help completing any of these tasks, refer to the online help for more details.

1 On the DNCS, create a package called **SCPnew**. Refer to the online help for more details.

2 Add the segments for the sources that are encrypted on the DNCS into the SCPnew package. Refer to the online help for more details.

3 On the DTACS Admin Console, click **Sys Config** to view the DTA Control System Configuration page.



DTACS System Config (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTACS System Config
Help
Exit

DTA Control System Configuration

Max Number of Virtual Channel Tables (VCT): 60

Authentication Management Module (AMM)

Packet ID (PID) (hex) :	0x1FF0
Location ID :	0x3
Activation Timeout (hours) :	720
Provider Phone Number :	1-800-5555
Use Daylight Saving Time (DST) :	Disabled
UTC Offset :	-05:00

Simple Content Protection (SCP)

Use SCP : Disabled

DTA Messaging Protocol

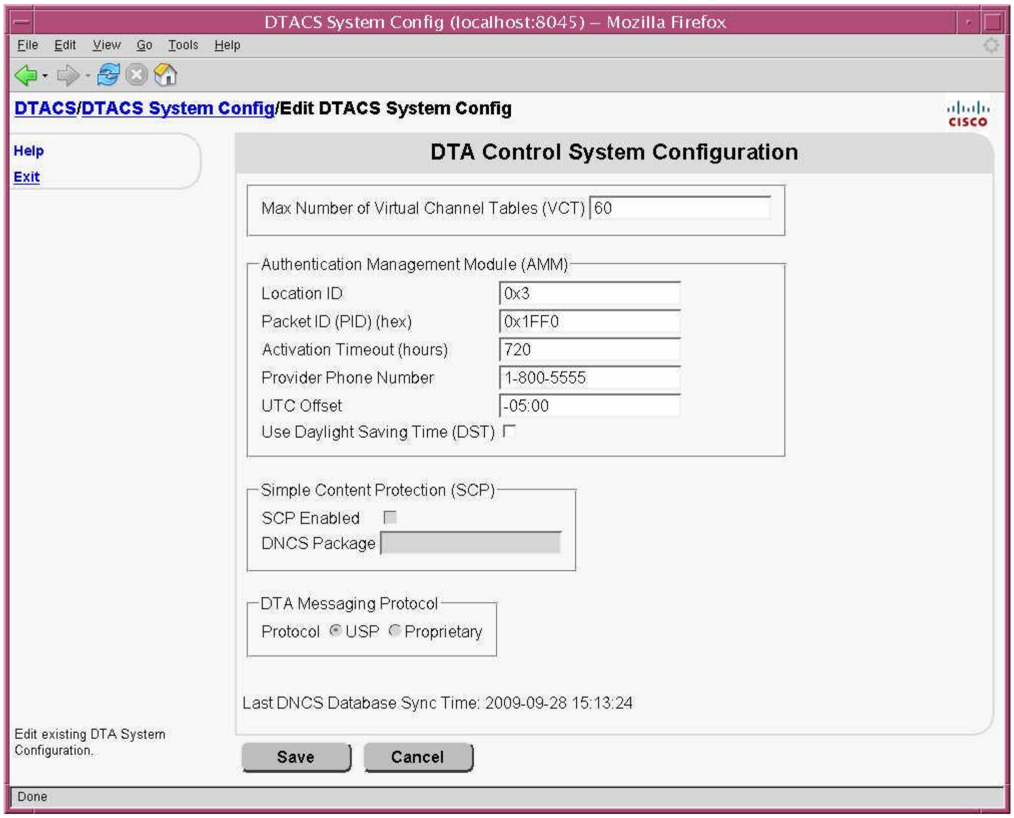
Protocol : USP

No changes made to DTA System Configuration.

4 Click **Sync DB** to sync the database, so that 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.


DTACS System Config (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTACS System Config/Edit DTACS System Config
cisco
Help
Exit
Save
Cancel
Done

DTA Control System Configuration

Max Number of Virtual Channel Tables (VCT) 60

Authentication Management Module (AMM)

Location ID 0x3
Packet ID (PID) (hex) 0x1FF0
Activation Timeout (hours) 720
Provider Phone Number 1-800-5555
UTC Offset -05:00
Use Daylight Saving Time (DST) □

Simple Content Protection (SCP)

SCP Enabled □
DNCS Package

DTA Messaging Protocol

Protocol ● USP ○ Proprietary

Last DNCS Database Sync Time: 2009-09-28 15:13:24

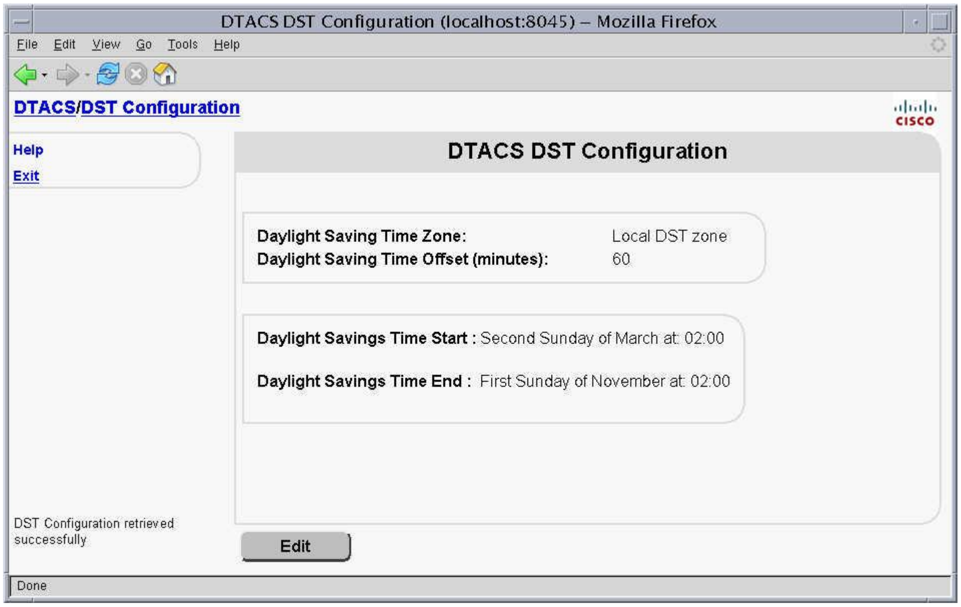
Edit existing DTA System Configuration.

6 In the DNCS Package field, select the **SCPnew** package that you created, and click **Save**. All of the sources in the SCPnew package are now available to DTAs for use.

Configure Daylight Saving Time

Follow these steps to configure Daylight Saving Time (DST) on the DTA Control System. From the Edit DTACS System Config window, select the box beside **Use Daylight Saving Time (DST).**

1 Click **DST Config** on the DTA Control System's main page. The DTACS DST Configuration window appears.



DTACS DST Configuration (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DST Configuration
Help
Exit
Edit
Done

DTACS DST Configuration

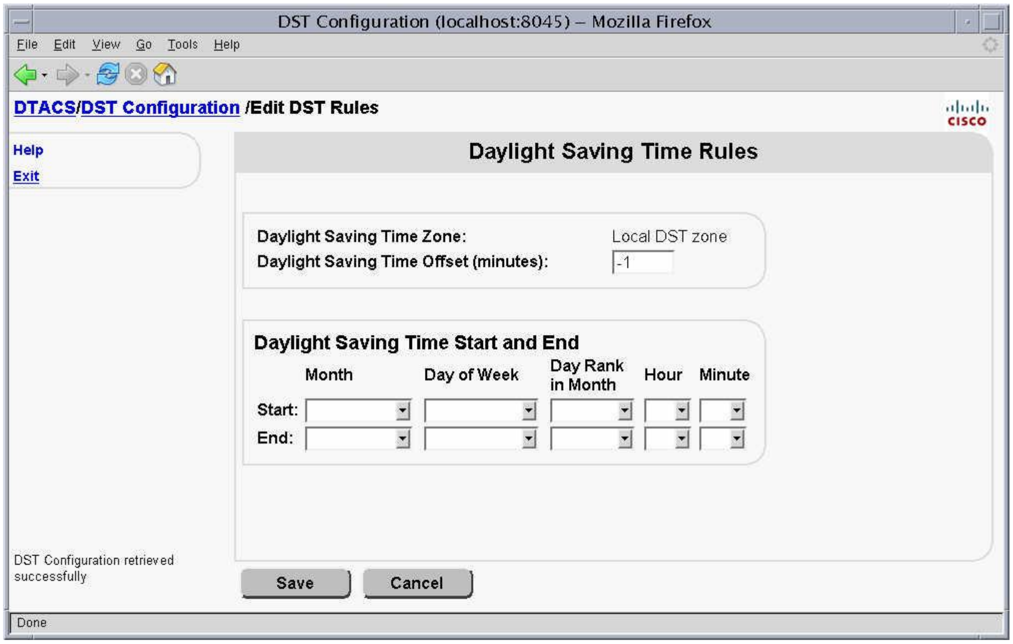
Daylight Saving Time Zone: Local DST zone
Daylight Saving Time Offset (minutes): 60

Daylight Savings Time Start : Second Sunday of March at: 02:00

Daylight Savings Time End : First Sunday of November at: 02:00

DST Configuration retrieved successfully

2 Click **Edit**. The Edit DST Rules window appears.



DST Configuration (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DST Configuration /Edit DST Rules
Help
Exit
Save
Cancel
Done

Daylight Saving Time Rules

Daylight Saving Time Zone: Local DST zone
Daylight Saving Time Offset (minutes): -1

Daylight Saving Time Start and End

	Month	Day of Week	Day Rank in Month	Hour	Minute
Start:					
End:					

DST Configuration retrieved successfully

3 Enter the settings for the DST rules that will apply to your location. The following table lists descriptions for the DST settings.

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 of Week	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, expressed in 24-hour time so that there is no need for a.m., p.m., or any other units of measure. Select any integer from 0 to 23.
Start: Minute	The number of minutes after the Start Hour that the DST rule becomes effective. This value is expressed in 24-hour time so that there is no need for a.m., p.m., or any other units of measure. Select any integer from 0 to 59.
End: Month	The month the DST rule ends.
End: Day of Week	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, expressed in 24-hour time so that there is no need for a.m., p.m., or any other units of measure. Select any integer from 0 to 23.
End: Minute	The number of minutes after the End Hour that the DST rule ends. This value is expressed in 24-hour time so that there is no need for a.m., p.m., or any other units of measure. Select any integer from 0 to 59.

4 Click **Save** to save your settings.

Manage Virtual Channel Tables

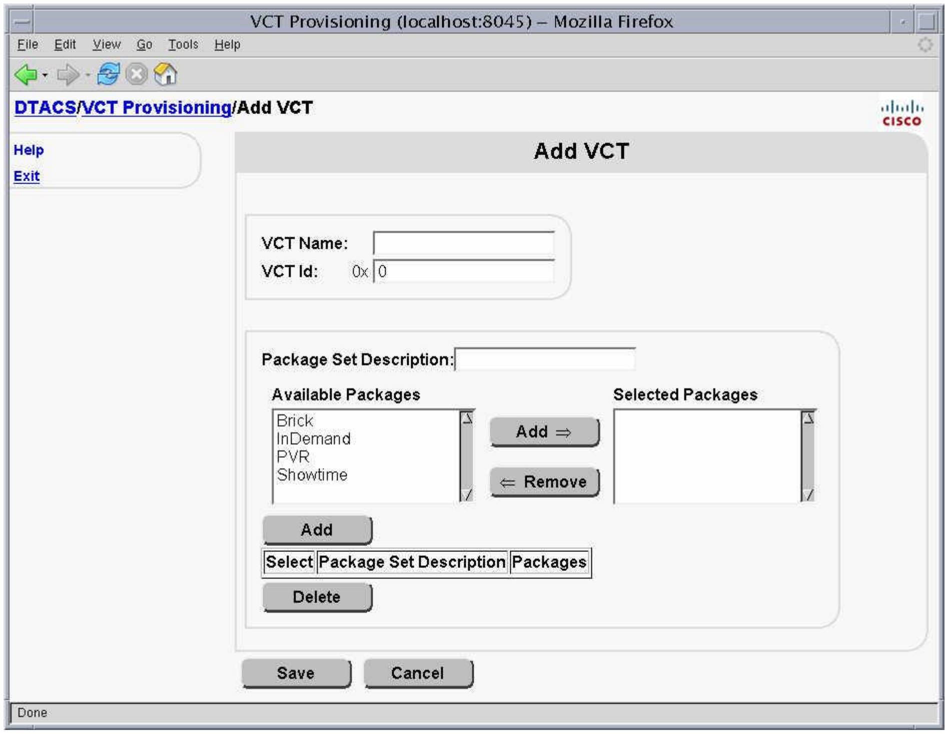
The DTA Control System's web-based user interface provides a way to manage Virtual Channel Tables (VCTs). The DTACS user interface allows you to manage the association of packages to VCTs. You can use this user interface to view, edit, add and delete VCTs.

Add a New VCT

Follow these steps to add new VCT(s).

Note: When you create a new VCT, any sources associated with packages that are included in the BSG channel map are automatically added to the associated VCT. However, if you edit the VCT later to assign new packages, then the sources contained in those packages are *not* automatically added to the VCT. You must add those sources separately.

1 Click **Add** on the VCT Provisioning page. The Add VCT window appears.



2 Type the **VCT Name** you want to use in the VCT Name text box.

3 Type the **VCT Id** you want to use in the VCT Id text box. The field requires you to enter a hex value.

4 Type a **Package Set Description**.

5 Click one or more package names you want to select in the **Available Packages** scrolling list. The package name(s) become highlighted.

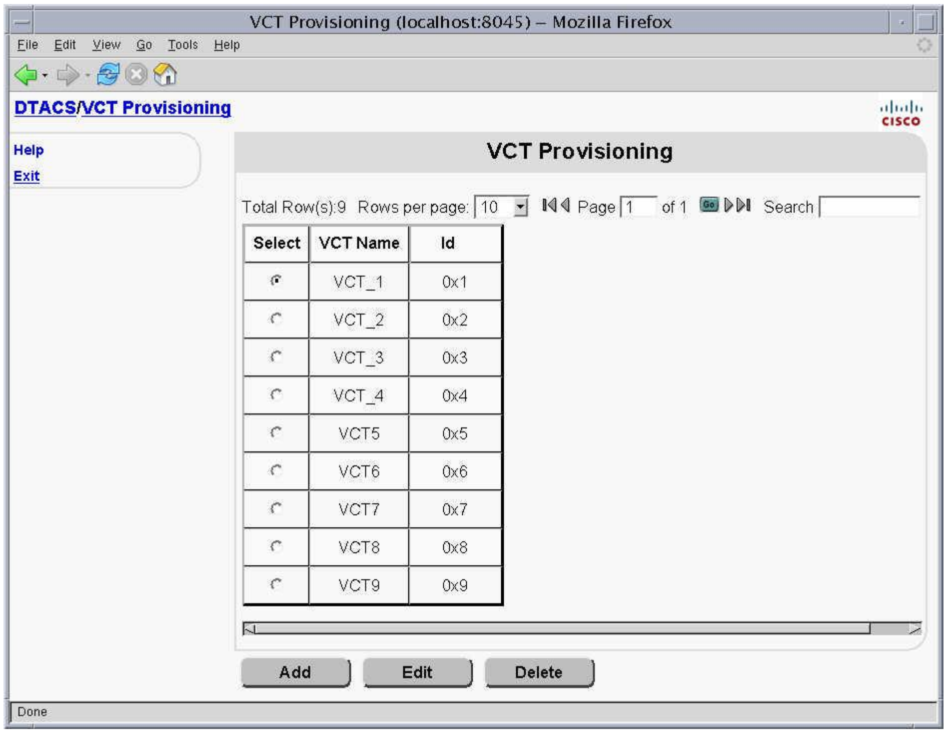
6 Click **Add.** The packages you selected appear in the Selected Packages scrolling list box.

7 Click **Save**. The VCT Provisioning page appears again, and the new VCT name and ID appear in the list.

Edit a VCT

Follow these steps to view and edit VCTs.

1 Click **VCT Provisioning** text on the DTA Control System's main page. The VCT Provisioning window appears.


VCT Provisioning (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/VCT Provisioning
cisco
Help
Exit
VCT Provisioning
Add
Edit
Delete
Done

Total Row(s):9 Rows per page: 10 Page 1 of 1 Search

Select	VCT Name	Id
●	VCT_1	0x1
○	VCT_2	0x2
○	VCT_3	0x3
○	VCT_4	0x4
○	VCT5	0x5
○	VCT6	0x6
○	VCT7	0x7
○	VCT8	0x8
○	VCT9	0x9

Note: You can click **DTACS** at the top of the page to go back to the DTACS main page.

2 Click beside the name of the VCT that you want to edit, and click **Edit**. The Edit VCT window appears, showing information about the selected VCT.

Note: Click **Cancel** if you do not want to make changes. The VCT Provisioning page displays.

3 Type new information in the **VCT Name** text box to change the selected VCT's name.

Note: Once a VCT has been created, you cannot change its VCT ID.

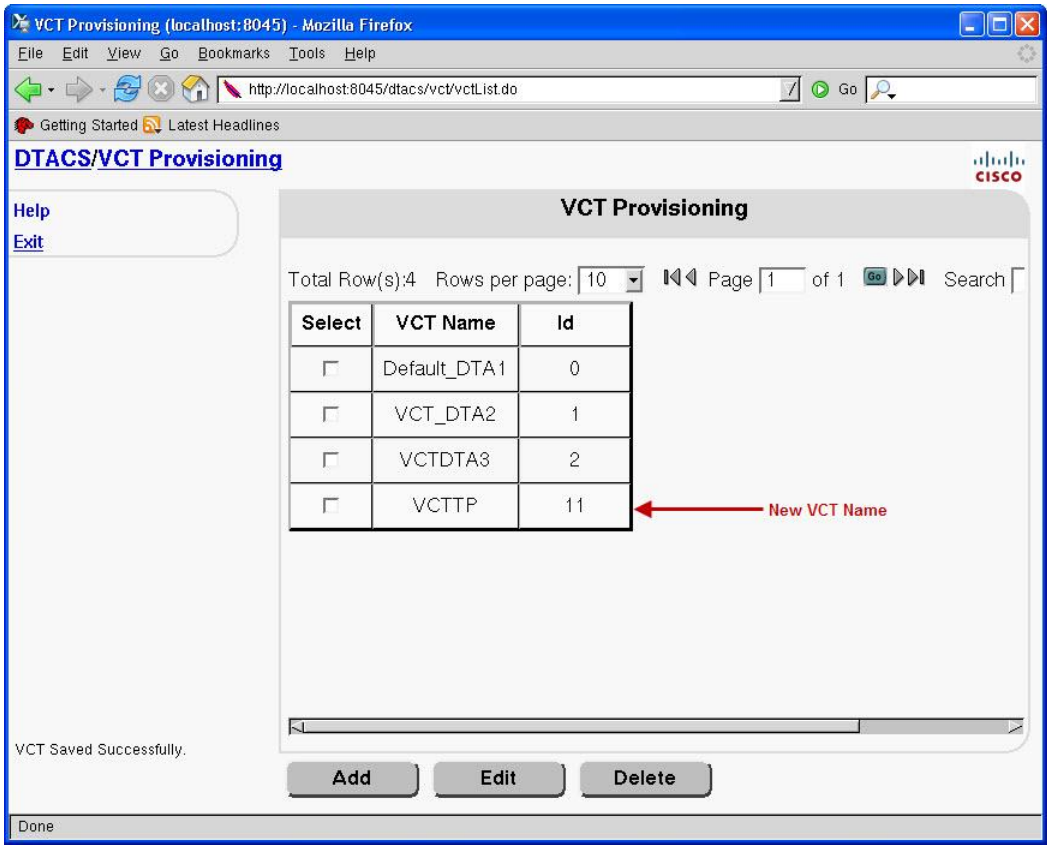
4 Type a **Package Set Description**.

5 Select a Package Set and click **Delete**.

Notes:

- You can select several packages or sources that appear together in the list by clicking the first item you want to select and, while pressing the **Shift** key, click the last item you want to select. The list items you want to add or remove are highlighted.
- You can select more than one package or source that does not appear together in the list by clicking an item in the scrolling list and, while pressing the **Ctrl** key, click additional items in the list. The list items you want to add or remove are highlighted.

6 Click **Save** to save your changes. The VCT Provisioning page displays. If you changed the VCT Name or VCT Id, the new information appears on the page.


VCT Provisioning (localhost:8045) - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8045/dtacs/vct/vctList.do
Go
Getting Started
Latest Headlines
DTACS/VCT Provisioning
Help
Exit
VCT Provisioning
Search
New VCT Name
Add
Edit
Delete
Done

Total Row(s):4 Rows per page: 10 Page 1 of 1

Select	VCT Name	Id
□	Default_DTA1	0
□	VCT_DTA2	1
□	VCTDTA3	2
□	VCTTP	11

VCT Saved Successfully.

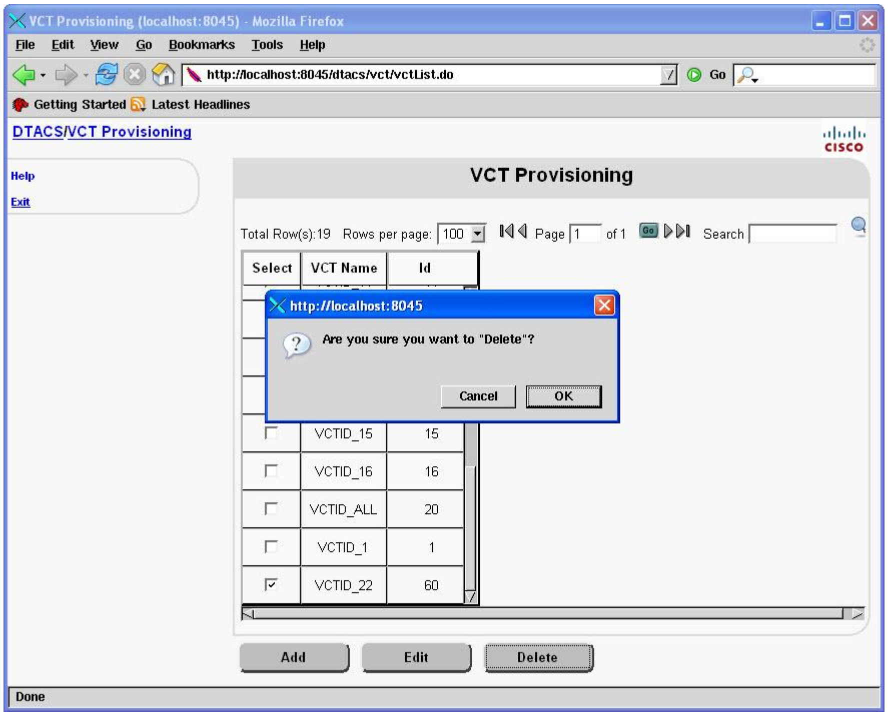
Note: If you changed packages or sources associated with a VCT, you must click Edit to verify the changes.

Delete a VCT

Follow these steps to delete a VCT.

Note: You cannot delete a VCT that is being used by any DTA.

1 Click the check box next to the VCT you want you want to delete on the VCT Provisioning page. A check mark appears in the check box.



VCT Provisioning (localhost:8045) - Mozilla Firefox

http://localhost:8045/dtacs/vct/vctList.do

DTACS/VCT Provisioning

VCT Provisioning

Total Row(s):19 Rows per page: 100 Page 1 of 1 Search

Select	VCT Name	Id
□	VCTID_15	15
□	VCTID_16	16
□	VCTID_ALL	20
□	VCTID_1	1
☑	VCTID_22	60

http://localhost:8045

Are you sure you want to "Delete"?

2 Click **Delete**. The 'Are you sure you want to delete' confirmation message appears.

3 Click **OK**. A message appears in the lower-left corner, indicating that the VCT was deleted successfully.

4 Click **DTACS** at the top of the page to return to the DTACS main page.

Provisioning a Broadcast Service Group

A Broadcast Service Group (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. This section contains the procedures necessary to provision a BSG.

Note: BSG provisioning is also known as QAM localization.

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.

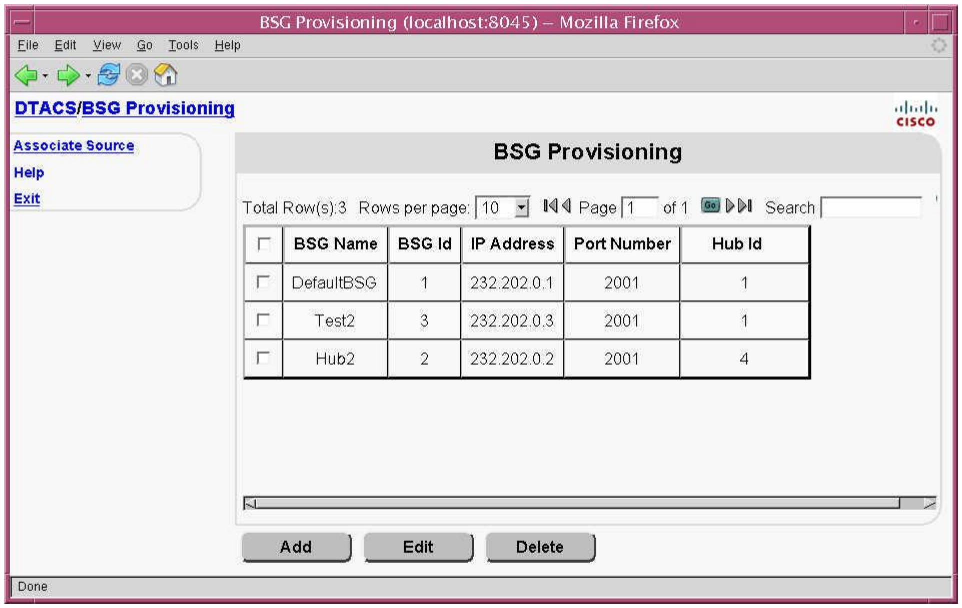
- **Billing System:** The billing system associates a rate code with a specific service package. The service package is passed to the DTACS, which uses the package to define a set of services (channel lineups) for DTA client devices. However, service packages and their associated channel lineup information 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.

Note: The channel map of a BSG is determined by the channel map of the DNCS Hub ID that is associated with the BSG.

Add a BSG

Follow these instructions to add a BSG to the DTACS.

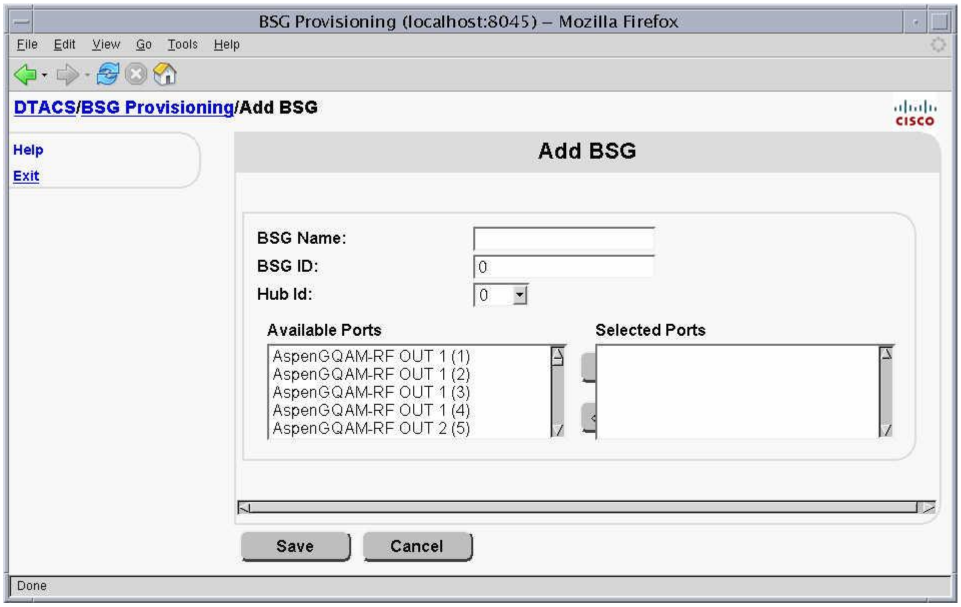
1 In the Network Elements section of the main page, click **BSG Provisioning**. The BSG Provisioning window opens, listing all the BSGs available in the DTACS.


BSG Provisioning (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/BSG Provisioning
cisco
Associate Source
Help
Exit
Total Row(s):3 Rows per page: 10 Page 1 of 1 Search
Add
Edit
Delete
Done

BSG Provisioning

□	BSG Name	BSG Id	IP Address	Port Number	Hub Id
□	DefaultBSG	1	232.202.0.1	2001	1
□	Test2	3	232.202.0.3	2001	1
□	Hub2	2	232.202.0.2	2001	4

2 Click **Add**. The Add BSG window opens.


BSG Provisioning (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/BSG Provisioning/Add BSG
cisco
Help
Exit
Save
Cancel
Done

Add BSG

BSG Name:
BSG ID: 0
Hub Id: 0

Available Ports
AspenGQAM-RF OUT 1 (1)
AspenGQAM-RF OUT 1 (2)
AspenGQAM-RF OUT 1 (3)
AspenGQAM-RF OUT 1 (4)
AspenGQAM-RF OUT 2 (5)

Selected Ports

3 Enter information as described in ***BSG Settings*** (on page 96).

4 Click **Save**; then click **OK** to confirm.

5 Your next step is to associate sources with the BSG. Go to ***Associate Sources With a BSG*** (on page 96).

BSG Settings

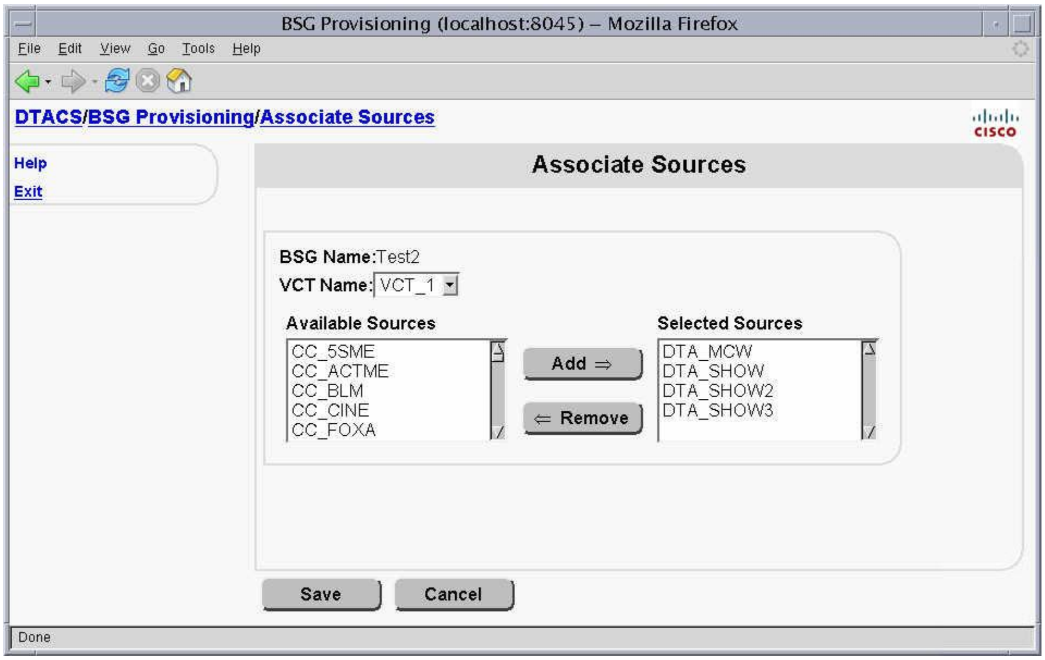
Use the following fields when you manage BSGs in the DTACS.

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.

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.


BSG Provisioning (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/BSG Provisioning/Associate Sources
Help
Exit
Associate Sources
Add ⇒
⇐ Remove
Save
Cancel
Done

BSG Name: Test2

VCT Name: VCT_1

Available Sources: CC_5SME, CC_ACTME, CC_BLM, CC_CINE, CC_FOXA

Selected Sources: DTA_MCW, DTA_SHOW, DTA_SHOW2, DTA_SHOW3

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**.

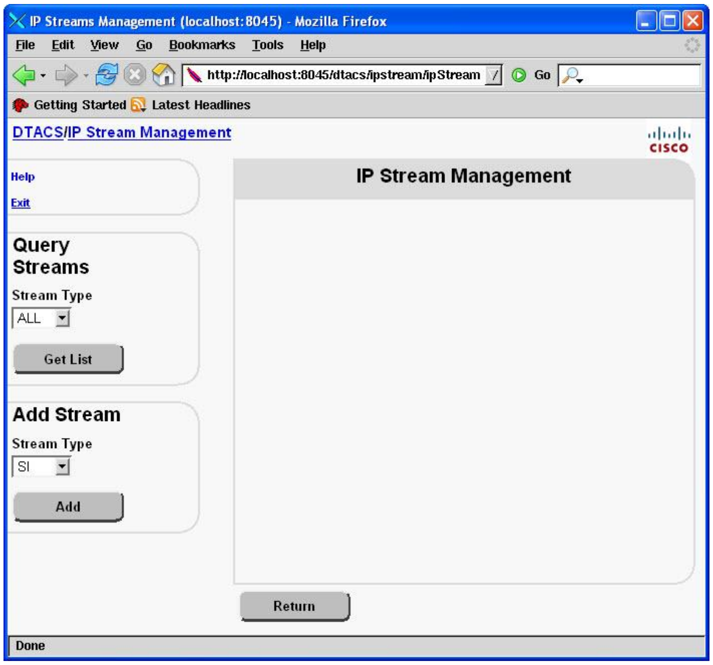
6 Your next step is to provision a new SI IP stream associated with the BSG. Go to ***Setting Up IP Streams*** (on page 98).

Setting Up IP Streams

Add IP Streams

Follow these steps to add IP Streams.

1 Click **IP Stream Management** on the DTA Control System's main page. The IP Stream Management window appears.


IP Streams Management (localhost:8045) - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8045/dtacs/ipstream/ipStream
Go
Getting Started Latest Headlines
DTACS/IP Stream Management
cisco
Help
Exit
Query Streams
Stream Type
ALL
Get List
Add Stream
Stream Type
SI
Add
IP Stream Management
Return
Done

Note: You can click **Return** to go back to DTA Control System's main page.

2 Click the drop-down arrow in the Add Stream section of the window and select the type of IP streams you want to add:

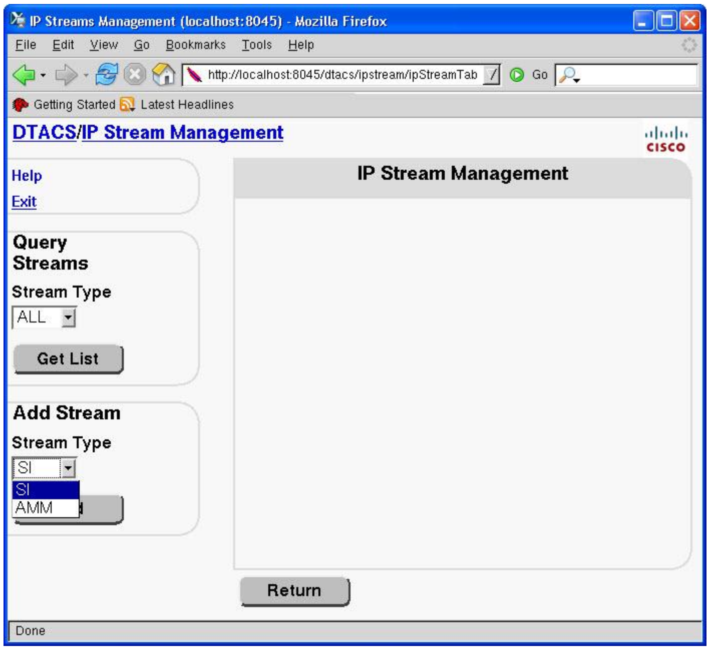
- System Information Message (SI)
- Activation Management Message (AMM)

Note: All of the AMM data messages are sent to every DTA. Therefore, you only need to add one AMM stream.

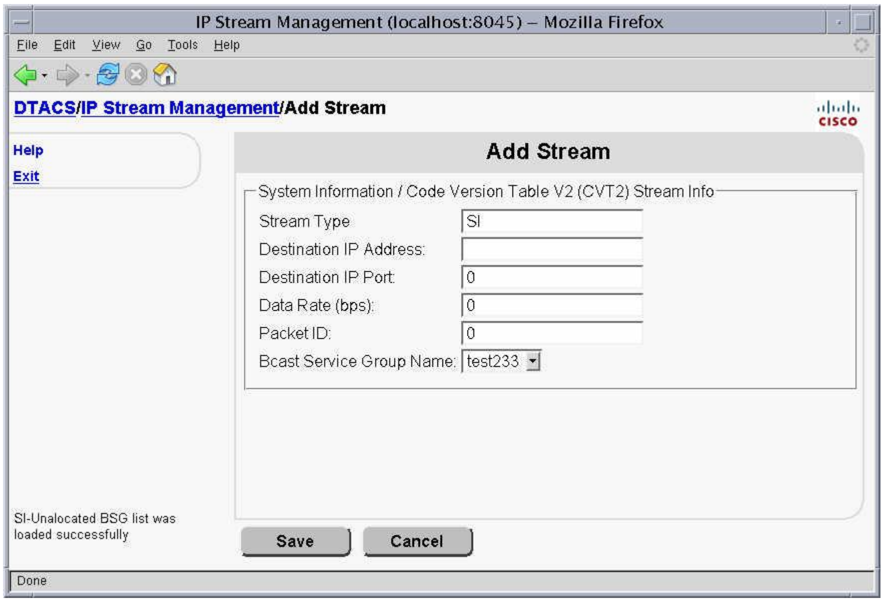
3 Move the cursor over the drop-down list entries. List items are highlighted when the cursor points to them.

4 Select **SI,** or the list item you want to select, from the list of stream types. The selection is highlighted.

5 Click **SI** or the list item you want to select. The selected list item (SI) appears in the Stream Type list box.


IP Streams Management (localhost:8045) - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8045/dtacs/ipstream/ipStreamTab
Go
Getting Started Latest Headlines
DTACS/IP Stream Management
Help
Exit
Query Streams
Stream Type
ALL
Get List
Add Stream
Stream Type
SI
SI
AMM
IP Stream Management
Return
Done

6 Click **Add**. The Add Stream window shows configuration information for the stream type you selected.


IP Stream Management (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/IP Stream Management/Add Stream
Help
Exit
Add Stream
Save
Cancel
Done

System Information / Code Version Table V2 (CVT2) Stream Info

Stream Type	SI
Destination IP Address:	
Destination IP Port:	0
Data Rate (bps):	0
Packet ID:	0
Bcast Service Group Name:	test233

SI-Unalocated BSG list was loaded successfully

7 Press the Tab key to go to the fields you want to add. The following table describes the fields that can be added on this page.

Note: You cannot change the Stream Type on the Add Stream page.

Field Name	Definition
Stream Type	Type of IP Stream. Valid values are AMM or SI.

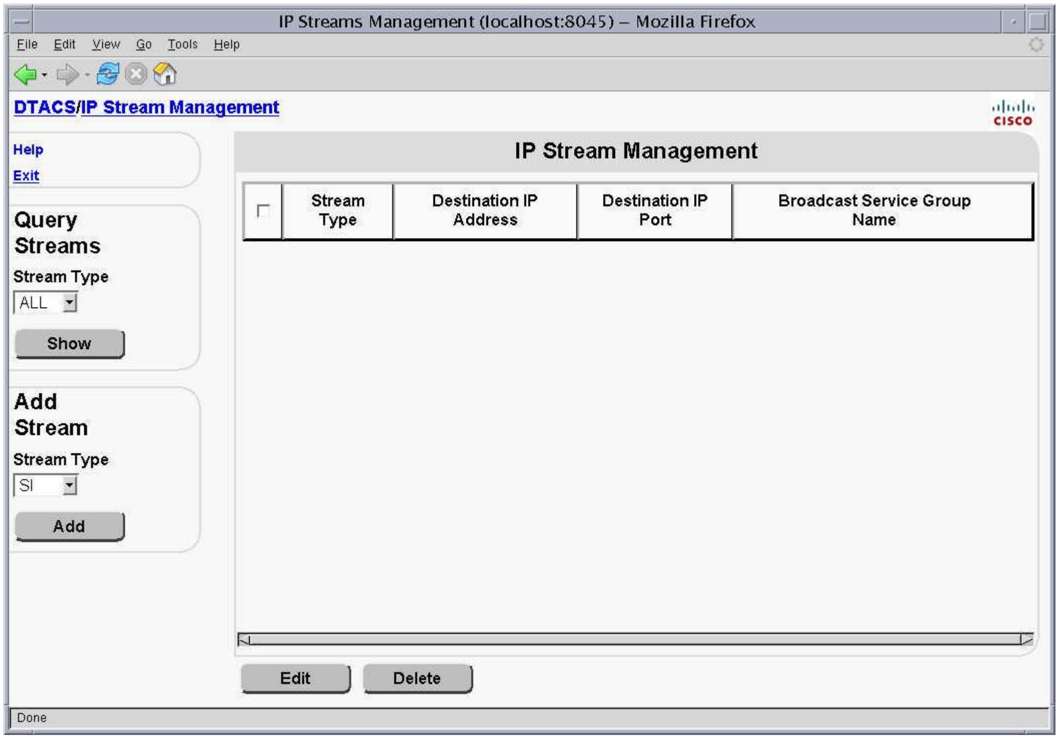
Field Name	Definition
Stream Type	Type of IP Stream. Valid values are AMM or SI.
Destination IP Address	The IP Address associated with this stream type.
Destination IP Port	The network port associated with the stream type.
Data Rate	The rate at which data can be transmitted when using this type of stream. This value depends on a number of variables, such as the number of DTAs and the amount of SI data. However, starting default values may be something like 20000 bps for SI or 10000 bps for AMM.
Packet ID	The pre-defined packet identifier associated with this type of data.
Bcast Service Group Name	The name of the BSG associated with this stream.

8 Click **Save** to save your changes, or click **Cancel** if you want to leave this screen without saving changes.

Query IP Streams

Follow these steps to select and query IP streams.

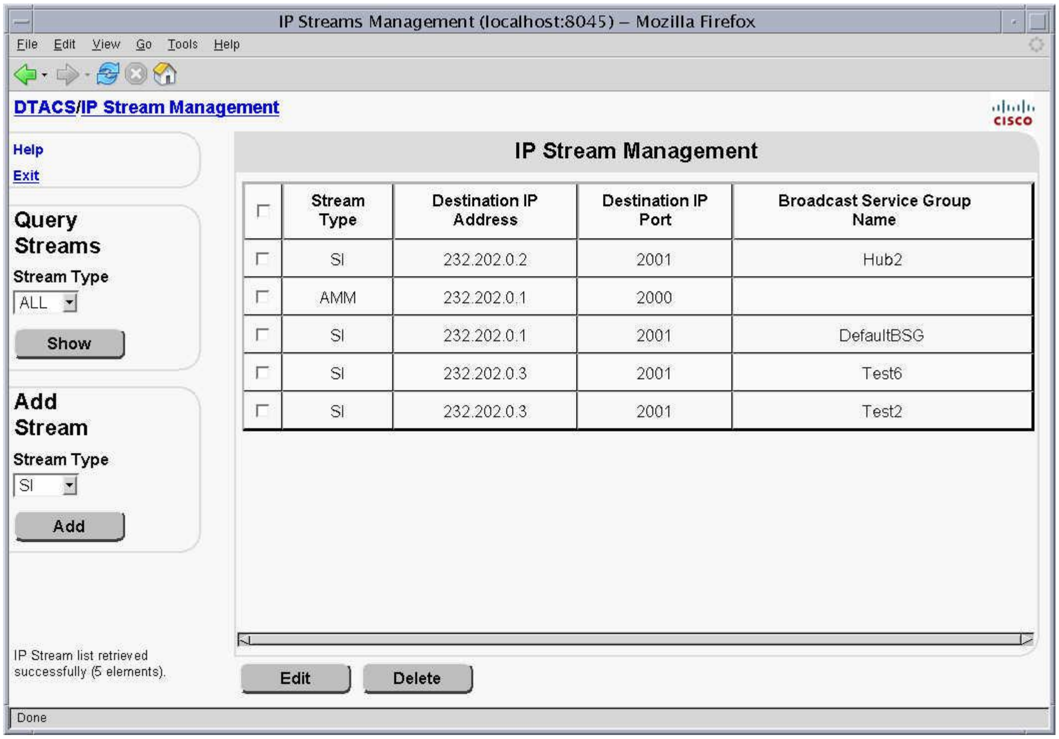
1 Click **IP Stream Management** on the DTA Control System's main page. The IP Stream Management window appears.



Note: You can click **DTACS** to go back to DTACS main page.

2 Click the drop-down arrow in the Query Streams section of the window and select the types of IP streams you want to view. You can view all streams together, or you can choose to view only SI streams or only AMM streams.

3 Click **Show** to view the IP Streams List.


IP Streams Management (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/IP Stream Management
cisco
Help
Exit
Query Streams
Stream Type
ALL
Show
Add Stream
Stream Type
SI
Add
IP Stream Management
Edit
Delete
Done

□	Stream Type	Destination IP Address	Destination IP Port	Broadcast Service Group Name
□	SI	232.202.0.2	2001	Hub2
□	AMM	232.202.0.1	2000	
□	SI	232.202.0.1	2001	DefaultBSG
□	SI	232.202.0.3	2001	Test6
□	SI	232.202.0.3	2001	Test2

IP Stream list retrieved successfully (5 elements).

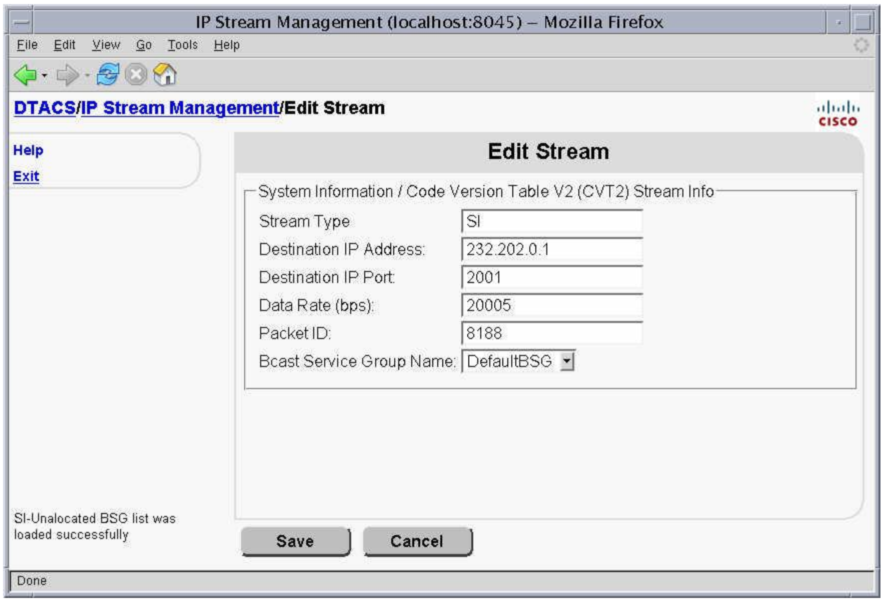
Note: You cannot change the data on this page. If you want to change IP stream data, you must click the **Edit** button.

Edit an IP Stream Type

Follow these steps to edit a stream type's information.

1 From the IP Streams List page, select the row you want to edit, and click **Edit**. The Edit Stream window appears.

Note: You can only edit one row of data at a time.


IP Stream Management (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/IP Stream Management/Edit Stream
Help
Exit
Save
Cancel
Done

Edit Stream

System Information / Code Version Table V2 (CVT2) Stream Info

Stream Type	SI
Destination IP Address:	232.202.0.1
Destination IP Port:	2001
Data Rate (bps):	20005
Packet ID:	8188
Bcast Service Group Name:	DefaultBSG

SI-Unalocated BSG list was loaded successfully

2 Press the Tab key to go to the field you want to update. The following table describes the fields that can be updated on this page.

Field Name	Definition
Stream Type	Type of IP Stream. Valid values are AMM or SI.
Destination IP Address	The IP Address associated with this stream type
Destination IP Port	The network port associated with the stream type
Data Rate	The rate at which data can be transmitted when using this type of stream
Packet ID	The pre-defined packet identifier associated with this type of data
Bcast Service Group Name	The name of the BSG associated with this stream.

3 Click **Save** to save your changes, or click **Cancel** if you want to leave this screen without saving changes.

Delete an IP Stream

1 Click the check box next to the Stream Type you want you want to delete on the IP Streams List page. A check mark appears in the check box.

2 Click **Delete**. The IP Streams List page appears and the IP Stream you selected is not listed in the streams list.

Note: If you want to delete all IP Streams, click the check box in the first row of the stream list and then click Delete.

Setting Up 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, rather than using TSRs to pass the data through the entire transport stream.

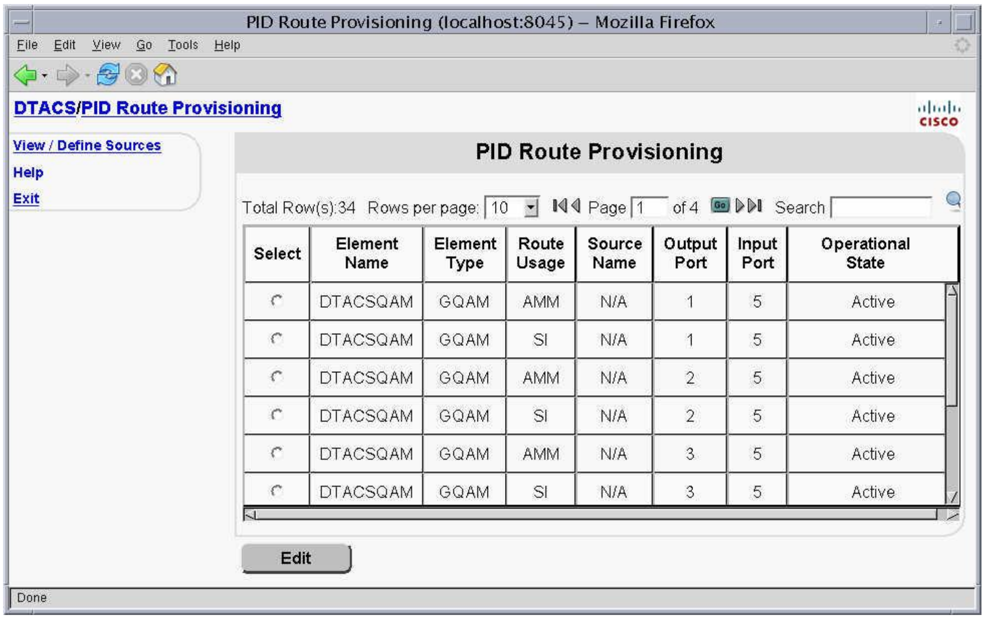
Using passthru PID routes allows the data to flow through the QAM on carriers that contain DTA-related content. When you provision passthru PID routes for BSG-associated QAM carriers with active content, the DTACS sets up additional PID routes (AMM, SI/CVT with user-defined PID route sources) on those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

In order to set up a passthru PID route, you must first create the PID route source and then add a PID to that route.

Create a PassThru PID Route

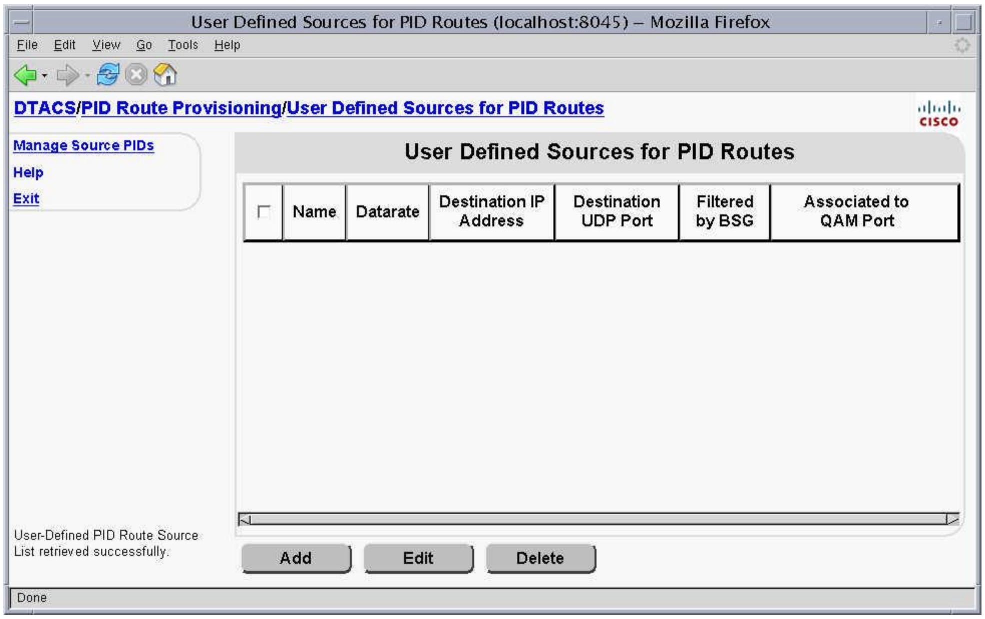
Follow these instructions to add a passthru PID source to a PID route in the DTACS.

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


PID Route Provisioning (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/PID Route Provisioning
View / Define Sources
Help
Exit
PID Route Provisioning
Total Row(s):34 Rows per page: 10 Page 1 of 4 Search
Edit
Done

Select	Element Name	Element Type	Route Usage	Source Name	Output Port	Input Port	Operational State
○	DTACSQAM	GQAM	AMM	N/A	1	5	Active
○	DTACSQAM	GQAM	SI	N/A	1	5	Active
○	DTACSQAM	GQAM	AMM	N/A	2	5	Active
○	DTACSQAM	GQAM	SI	N/A	2	5	Active
○	DTACSQAM	GQAM	AMM	N/A	3	5	Active
○	DTACSQAM	GQAM	SI	N/A	3	5	Active

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


User Defined Sources for PID Routes (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
Manage Source PIDs
Help
Exit
Add
Edit
Delete
Done

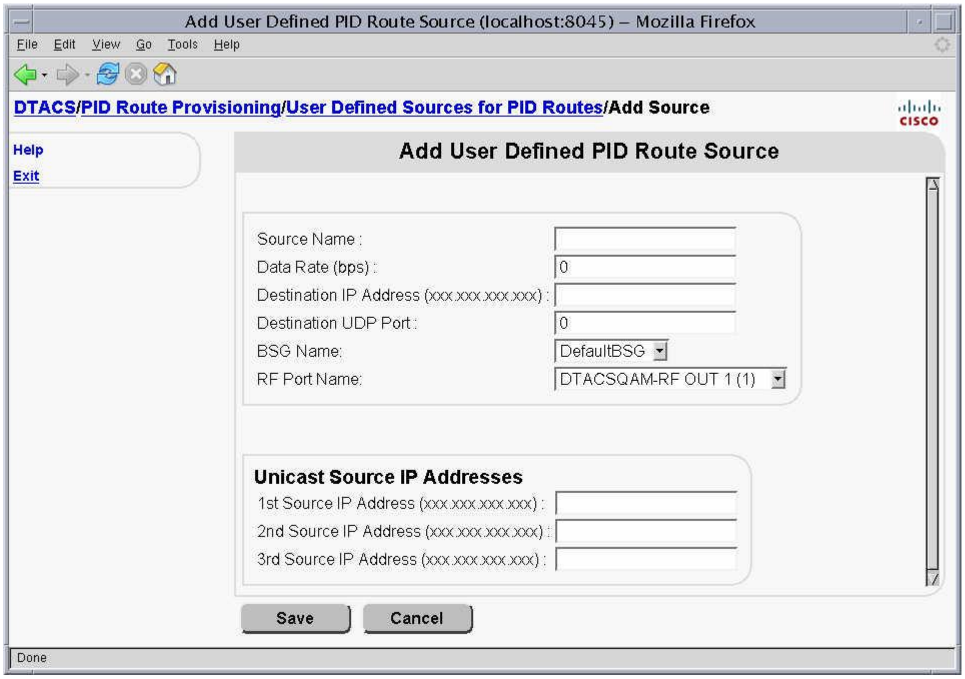
DTACS/PID Route Provisioning/User Defined Sources for PID Routes

User Defined Sources for PID Routes

□	Name	Datarate	Destination IP Address	Destination UDP Port	Filtered by BSG	Associated to QAM Port

User-Defined PID Route Source List retrieved successfully.

3 Click **Add**. The Add User Defined PID Route Source window opens.


Add User Defined PID Route Source (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
Help
Exit
Save
Cancel
Done

DTACS/PID Route Provisioning/User Defined Sources for PID Routes/Add Source

Add User Defined PID Route Source

Source Name :
Data Rate (bps) : 0
Destination IP Address (xxx.xxx.xxx.xxx) :
Destination UDP Port : 0
BSG Name: DefaultBSG
RF Port Name: DTACSQAM-RF OUT 1 (1)

Unicast Source IP Addresses

1st Source IP Address (xxx.xxx.xxx.xxx) :
2nd Source IP Address (xxx.xxx.xxx.xxx) :
3rd Source IP Address (xxx.xxx.xxx.xxx) :

4 Complete the fields on this screen as follows:

Field	Description
Source Name	Enter the name of the source you are adding.
Data Rate (bps)	Enter the data rate for the source (in bps).
Destination IP Address	Enter the destination IP address for the source.

Field	Description
Destination UDP Port	Enter the destination UDP port for the source (from 1 to 65535).
BSG Name	Select the BSG associated with this source from the drop-down list.
RF Port Name	Select the output RF port (QAM carrier) associated with this source from the drop-down list.
Unicast Source IP Addresses	
1st Source IP Address	Enter the source's first unicast IP address, 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 source's second unicast IP address, if applicable.
3rd Source IP Address	Enter the source's third unicast IP address, if applicable.

5 Click **Save**. The DTACS creates the user-defined source for PID routes that you entered.

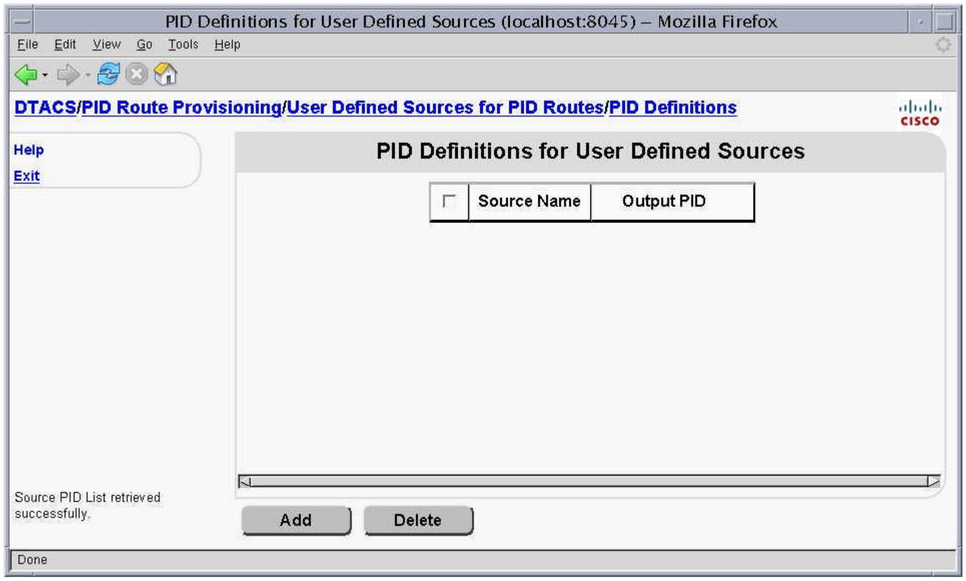
Add a PassThru PID Definition to a User-Defined Source

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.



PID Definitions for User Defined Sources (localhost:8045) – Mozilla Firefox

DTACS/PID Route Provisioning/User Defined Sources for PID Routes/PID Definitions

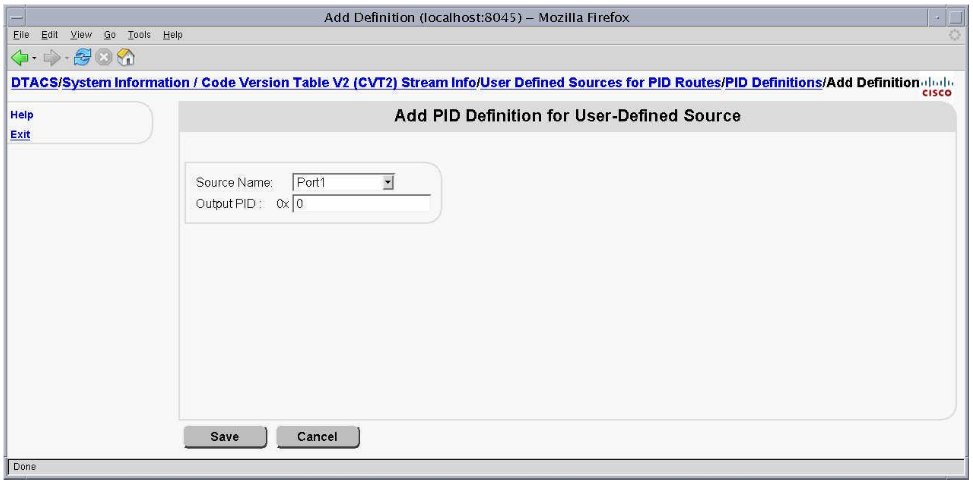
PID Definitions for User Defined Sources

☐	Source Name	Output PID

Source PID List retrieved successfully.

Done

4 Click **Add**. The Add PID Definition for User-Defined Source window opens.



Add Definition (localhost:8045) – Mozilla Firefox

DTACS/System Information / Code Version Table V2 (CVT2) Stream Info/User Defined Sources for PID Routes/PID Definitions/Add Definition

Add PID Definition for User-Defined Source

Source Name: Port1

Output PID : 0x 0

Done

5 Select the **Source Name** from the drop-down list.

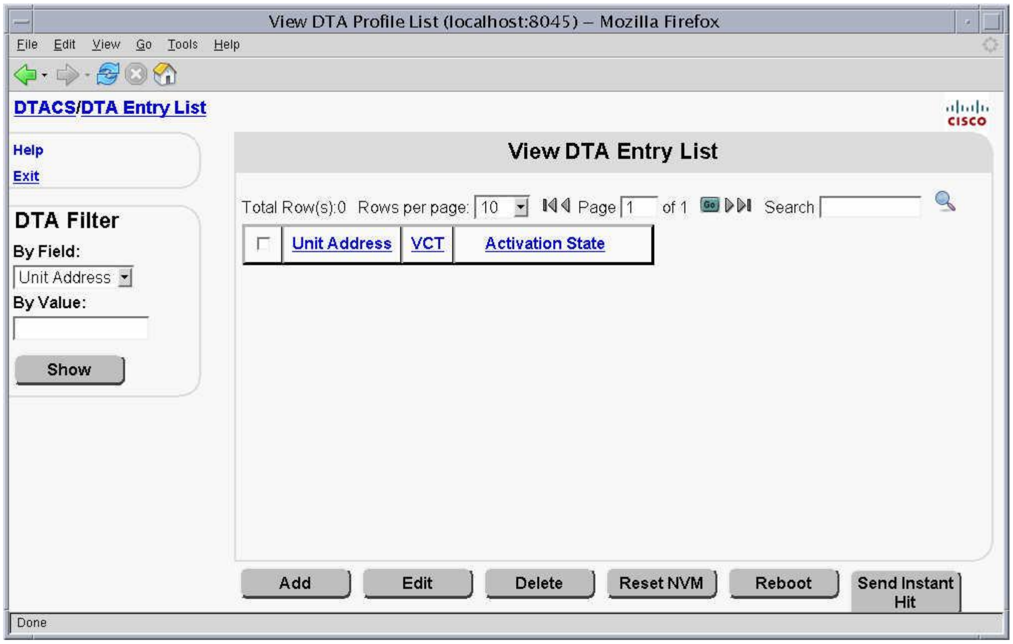
6 Enter an **Output PID**.

7 Click **Save**. The DTACS creates the PID definition for the source you selected. It also creates PID routes for the PID definitions for user-defined sources on carriers that contain DTA content.

Set Up DTAs

View DTA Information

To select a DTA and view DTA information, click **DTA Management** text on the DTA Control System's main page. The DTA Management window appears.


View DTA Profile List (localhost:8045) – Mozilla Firefox

DTACS/DTA Entry List

View DTA Entry List

DTA Filter

By Field: Unit Address

By Value:

Total Row(s):0 Rows per page: 10 Page 1 of 1 Search

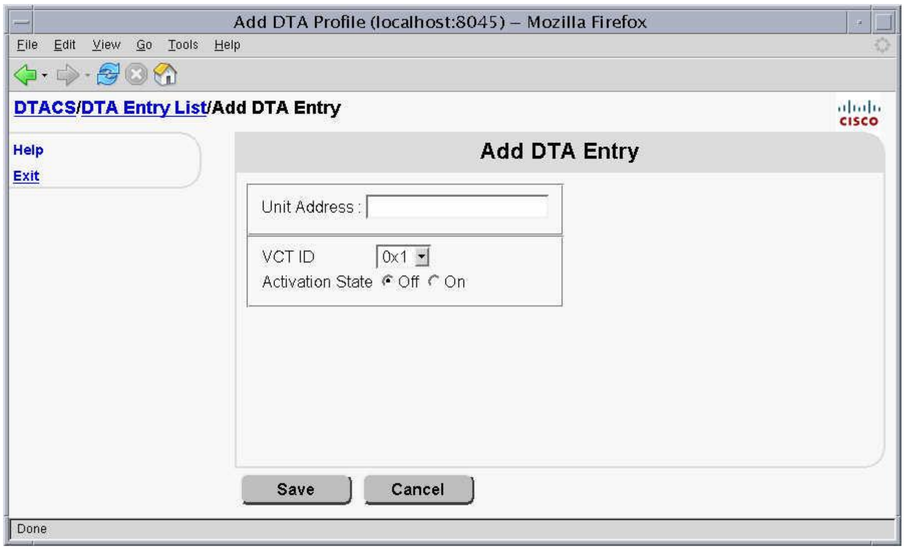
☐	Unit Address	VCT	Activation State

Done

Add a DTA

Follow these steps to add a DTA.

1 Click **Add**. The Add DTA Entry window displays.



Add DTA Profile (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTA Entry List/Add DTA Entry
cisco
Help
Exit
Add DTA Entry
Save
Cancel
Done

Unit Address :

VCT ID 0x1

Activation State ● Off ○ On

2 Press the Tab key to go to the field you want to add. The following table describes the fields that can be added on this page.

Field Name	Definition
Unit Address	The DTA's Unit Address. This value must start with 12:BE.
VCT ID	The ID of the Version Code Table associated with this DTA.
Activation State	Indicates whether the DTA is activated. Select either Off or On.

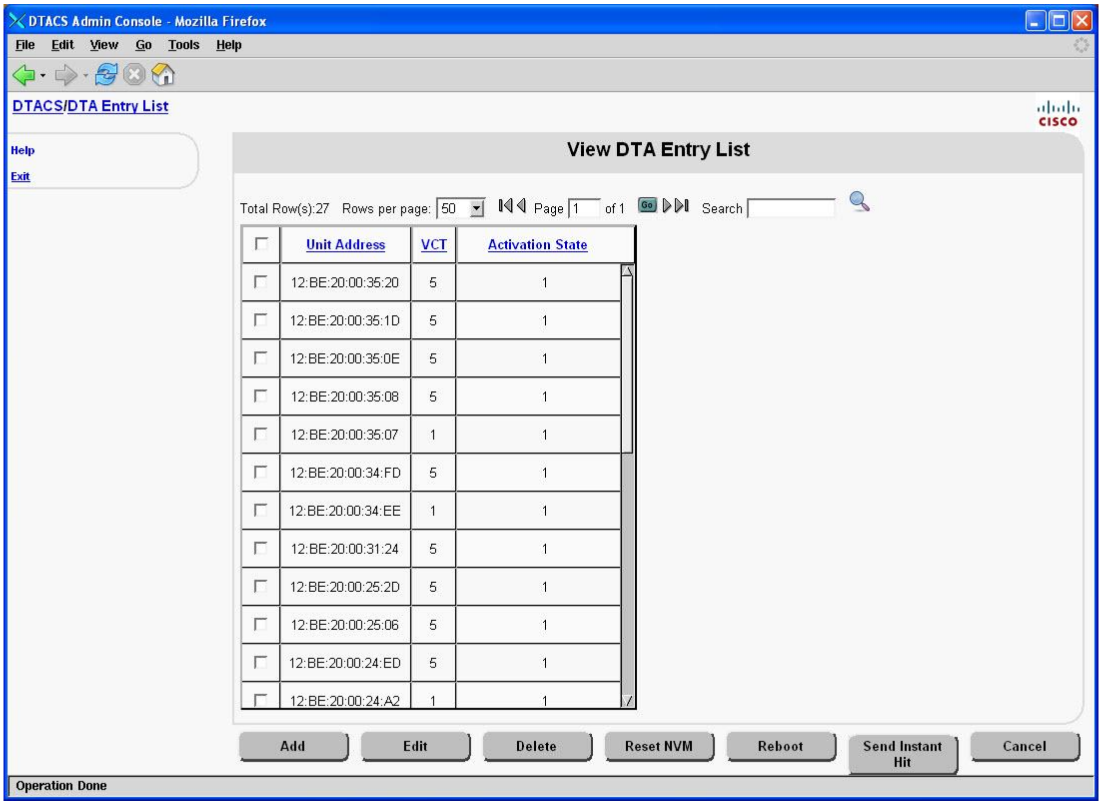
3 Click **Save.** The View DTA List Entry window appears and the new DTA is listed.

4 Click **DTA Management** at the top of the window to the return to the DTA Management page.

Edit a DTA

Follow these steps to edit a DTA.

1 From the DTA Management page, type a value in the **By Value:** text box and click **Show**. The View DTA Entry List appears, showing entries that match the value you entered.

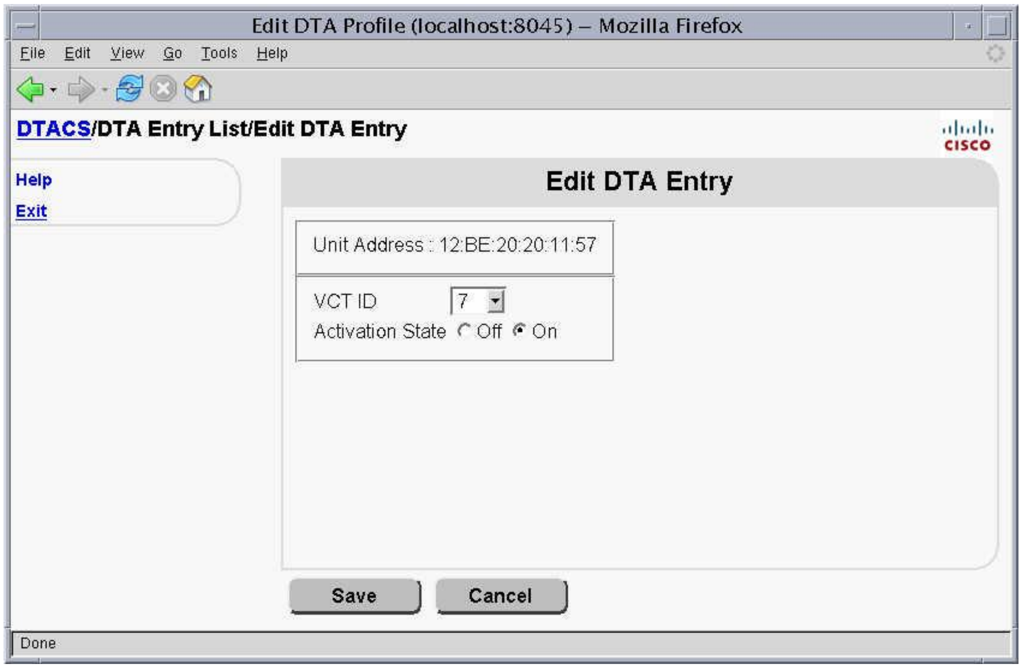


Total Row(s):27 Rows per page: 50 Page 1 of 1 Search

□	Unit Address	VCT	Activation State
□	12:BE:20:00:35:20	5	1
□	12:BE:20:00:35:1D	5	1
□	12:BE:20:00:35:0E	5	1
□	12:BE:20:00:35:08	5	1
□	12:BE:20:00:35:07	1	1
□	12:BE:20:00:34:FD	5	1
□	12:BE:20:00:34:EE	1	1
□	12:BE:20:00:31:24	5	1
□	12:BE:20:00:25:2D	5	1
□	12:BE:20:00:25:06	5	1
□	12:BE:20:00:24:ED	5	1
□	12:BE:20:00:24:A2	1	1

2 Click the check box beside a DTA entry to select a DTA from the list. A check mark appears in the check box.

3 Click **Edit**. The Edit DTA Entry window appears.



Edit DTA Profile (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTA Entry List/Edit DTA Entry
cisco
Help
Exit
Edit DTA Entry
Save
Cancel
Done

Unit Address : 12:BE:20:20:11:57

VCT ID 7

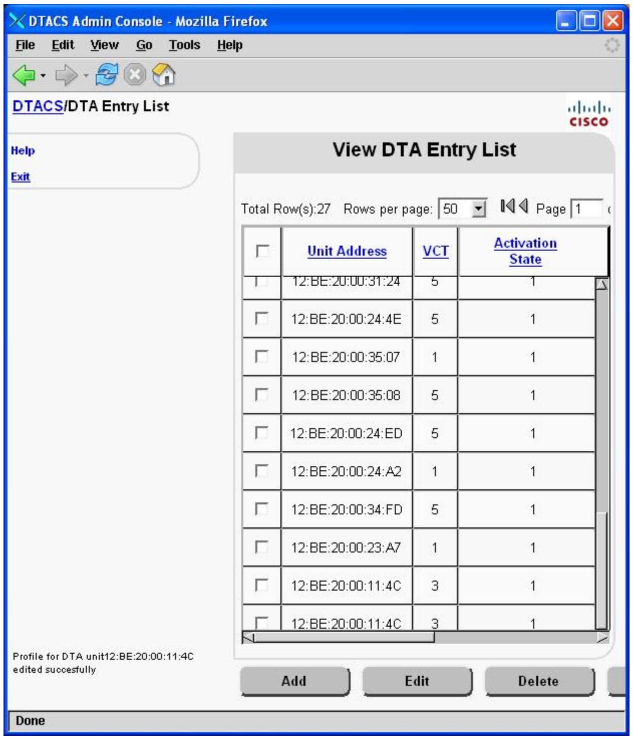
Activation State ○ Off ● On

Note: Click **Cancel** if you do not want to make changes.

4 Go to the field you want to update. The following table describes the fields that can be updated on this page.

Field Name	Definition
Unit Address	The DTA's Unit Address. You cannot change this field.
VCT ID	The ID of the Version Code Table associated with this DTA.
Activation State	Indicates whether the DTA is activated. Select either Off or On.

5 Click **Save.**



DTACS Admin Console - Mozilla Firefox
File Edit View Go Tools Help
DTACS/DTA Entry List
Help
Exit
View DTA Entry List
Add
Edit
Delete
Done

Total Row(s):27 Rows per page: 50 Page 1

□	Unit Address	VCT	Activation State
□	12:BE:20:00:31:24	5	1
□	12:BE:20:00:24:4E	5	1
□	12:BE:20:00:35:07	1	1
□	12:BE:20:00:35:08	5	1
□	12:BE:20:00:24:ED	5	1
□	12:BE:20:00:24:A2	1	1
□	12:BE:20:00:34:FD	5	1
□	12:BE:20:00:23:A7	1	1
□	12:BE:20:00:11:4C	3	1
□	12:BE:20:00:11:4C	3	1

Profile for DTA unit12:BE:20:00:11:4C edited succesfully

Results:

- The DTA Entry List window appears.
- The DTA whose information you edited appears in the list.
- The 'Profile for client unit [UNIT ID] updated successfully' message appears.

Note: Substitute the Unit ID for the selected DTA for [UNIT ID] in the confirmation message.

Delete a DTA

1 Click the check box next to the DTA you want you want to delete on the View DTA Entry List page. A check mark appears in the check box.

2 Click **Delete**. The 'Are you sure you want to delete profile(s)?' message appears.

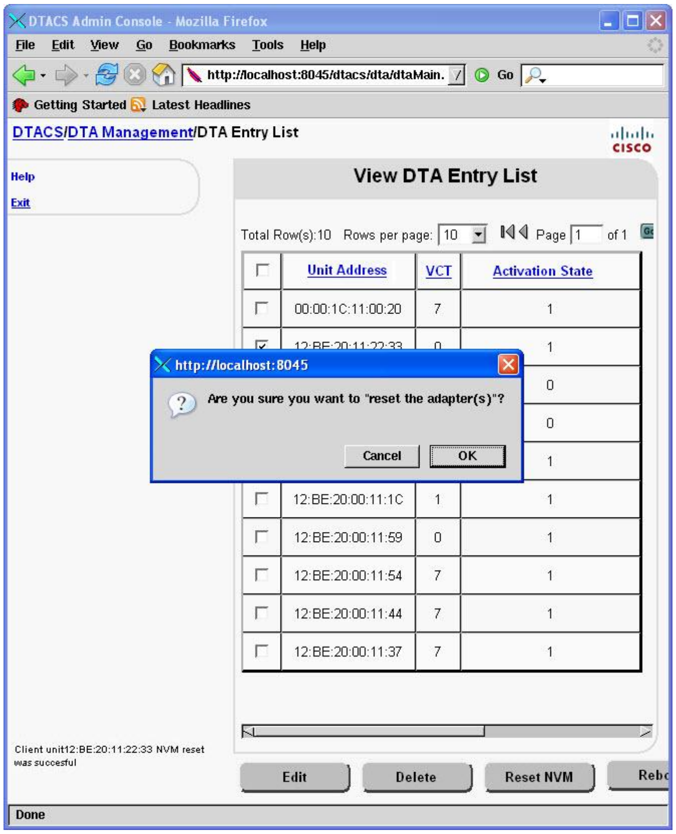
3 Click **OK** to delete the DTA. The View DTA Entry List window appears and the DTA is no longer listed.

Note: If you click **Cancel,** the View DTA Entry List window appears and the DTA appears in the list.

Reset NVM

1 Click the check box next to the DTA you want you want to reset on the View DTA Entry List page. A check mark appears in the check box.

2 Click **Reset NVM.** The 'Are you sure you want to reset the adapter(s)' message appears.


DTACS Admin Console - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8045/dtacs/dta/dtaMain.
Go
Getting Started Latest Headlines
DTACS/DTA Management/DTA Entry List
Help
Exit
http://localhost:8045
Cancel
OK
Edit
Delete
Reset NVM
Rebc
Done

View DTA Entry List

Total Row(s):10 Rows per page: 10 Page 1 of 1

□	Unit Address	VCT	Activation State
□	00:00:1C:11:00:20	7	1
☑	12:BE:20:11:22:33	0	1
[illegible]	[illegible]	[illegible]	0
[illegible]	[illegible]	[illegible]	0
[illegible]	[illegible]	[illegible]	1
□	12:BE:20:00:11:1C	1	1
□	12:BE:20:00:11:59	0	1
□	12:BE:20:00:11:54	7	1
□	12:BE:20:00:11:44	7	1
□	12:BE:20:00:11:37	7	1

Are you sure you want to "reset the adapter(s)"?

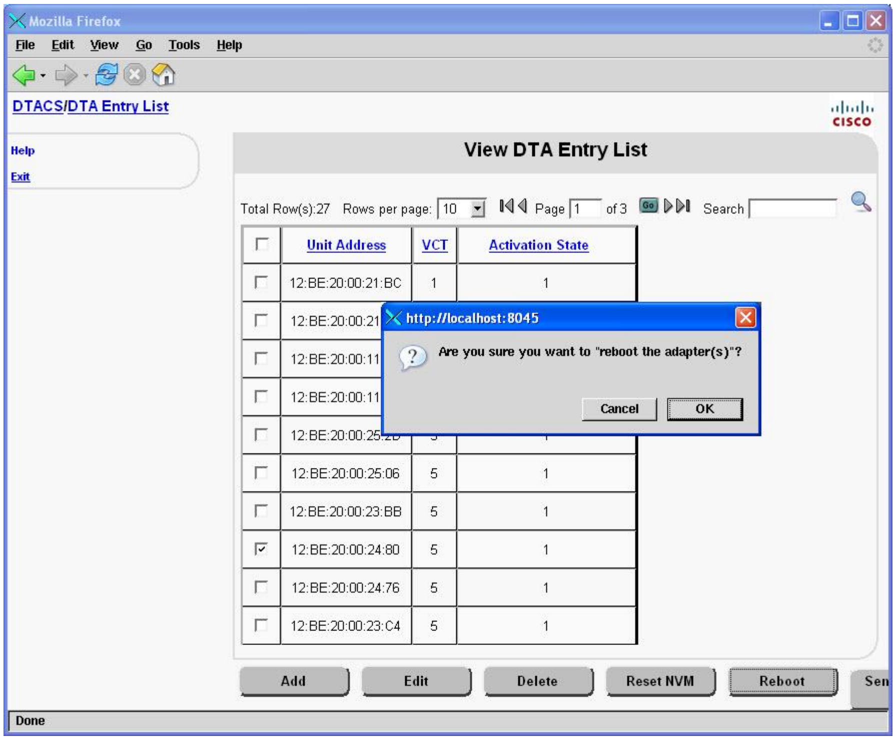
Client unit12:BE:20:11:22:33 NVM reset was succesful

3 Click **OK**. The 'Client unit [UNIT ID] NVM reset was successful' confirmation message appears on the View DTA Entry List page.

Reboot a DTA

1 Click the check box next to the DTA you want you want to reboot on the View DTA Entry List page. A check mark appears in the check box.

2 Click **Reboot**. The ' Are you sure you want to reboot the adapter(s)?' confirmation message appears.



View DTA Entry List

Total Row(s):27 Rows per page: 10 Page 1 of 3 Search

□	Unit Address	VCT	Activation State
□	12:BE:20:00:21:BC	1	1
□	12:BE:20:00:21		
□	12:BE:20:00:11		
□	12:BE:20:00:11		
□	12:BE:20:00:25:2D	5	1
□	12:BE:20:00:25:06	5	1
□	12:BE:20:00:23:BB	5	1
☑	12:BE:20:00:24:80	5	1
□	12:BE:20:00:24:76	5	1
□	12:BE:20:00:23:C4	5	1

http://localhost:8045

Are you sure you want to "reboot the adapter(s)"?

Cancel OK

3 Click **OK**. The 'Client unit [UNIT ID] reboot was successful' message appears on the View DTA Entry List page.

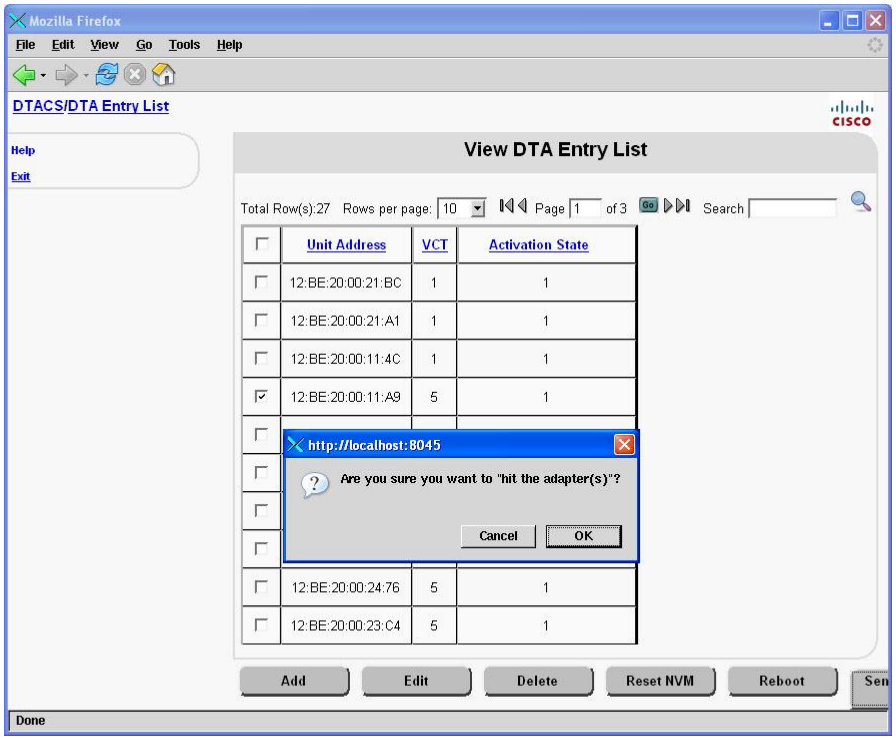
Send an Instant Hit

Follow these steps to send an instant hit to one or more DTAs.

1 From the View DTA Entry List screen, select the DTAs that should receive the instant hit.

Important: If you select the check box at the top of the screen, the system only selects the DTAs that are visible on the screen. It does *not* select any DTAs that may exist on other screens.

2 Click **Send Instant Hit**. The 'Are you sure you want to hit the adapter(s)?' message appears.



View DTA Entry List

Total Row(s):27 Rows per page: 10 Page 1 of 3 Search

□	Unit Address	VCT	Activation State
□	12:BE:20:00:21:BC	1	1
□	12:BE:20:00:21:A1	1	1
□	12:BE:20:00:11:4C	1	1
☑	12:BE:20:00:11:A9	5	1
□			
□			
□			
□			
□	12:BE:20:00:24:76	5	1
□	12:BE:20:00:23:C4	5	1

http://localhost:8045

Are you sure you want to "hit the adapter(s)"?

Cancel OK

3 Click **OK** to send the hit. The 'Client unit [UNIT ID] hit was successful' confirmation message appears on the View DTA Entry List page.

Common Download

Configure the Carousel

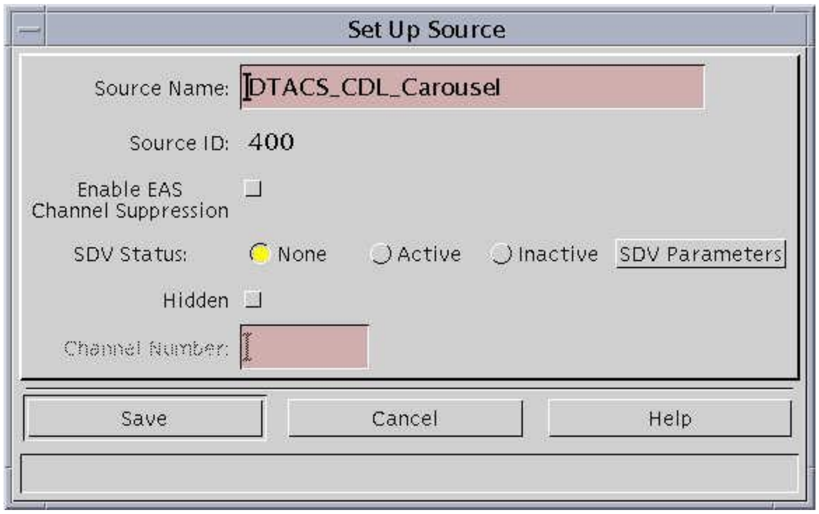
Follow these steps to configure Common Download on the DNCS and DTACS Servers.

Important:

- Refer to the DTACS Online Help for detailed information to complete these configuration tasks.
- Refer to *Recommendations for Data Carousel Rate Management Technical Bulletin* (part number 716377) for guidelines on managing inband and out-of-band data carousel rates.

1 On DNCS Source List UI, create a New Source for the DTACS Carousel (dataPump).

Example: Name = DTACS CDL Carousel, Source ID = user specified Source ID number (i.e., 310).



Set Up Source

Source Name: DTACS_CDL_Carousel

Source ID: 400

Enable EAS Channel Suppression ☐

SDV Status: ● None ○ Active ○ Inactive

Hidden ☐

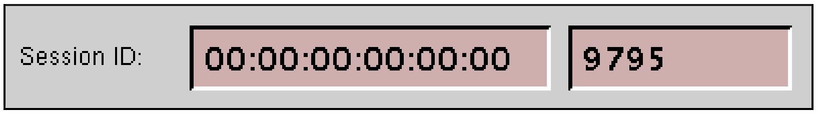
Channel Number:

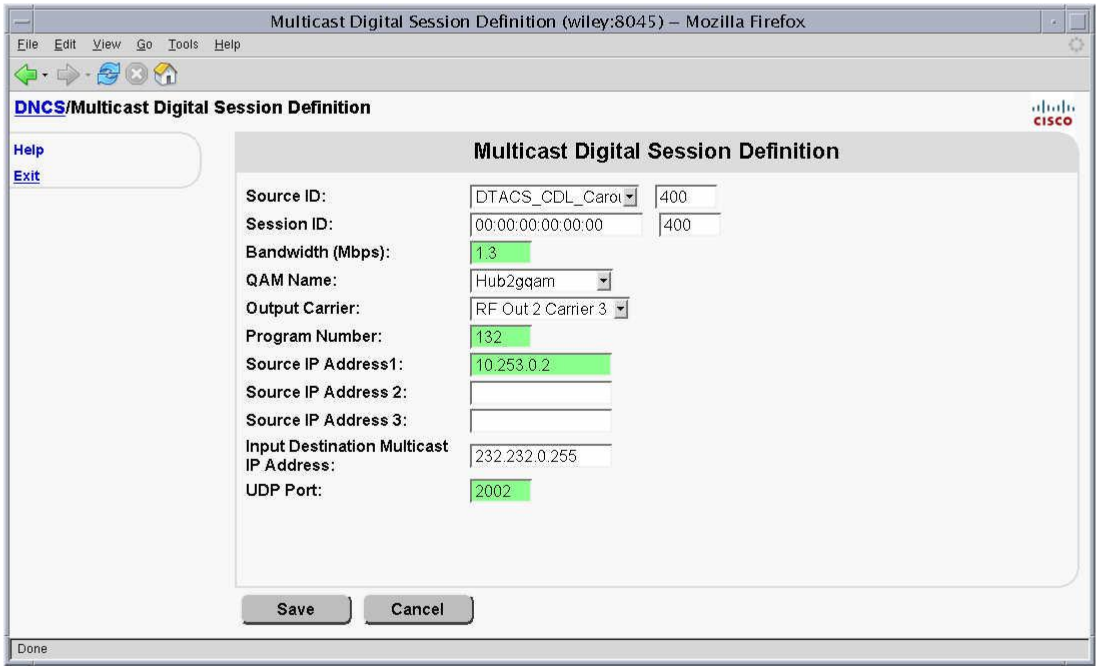
2 Select a DTA GQAM and one of its outputs, which has sufficient bandwidth for modulating the DTA images out to the DTAs.

Notes:

- If a DTA GQAM has not been defined on this system, or if another GQAM is needed because of bandwidth issues, then create a new DTA GQAM using the DNCS QAM List for support of the DTACS dataPump's session.
- This example describes a DTA CDL Carousel configuration with a multicast session. A unicast session may be used, but the unicast session setup is not shown at this time.

3 On the DNCS, create a new source definition for the DTACS Carousel's source (shown above).

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:  Session ID: 00:00:00:00:00:00 9795
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).

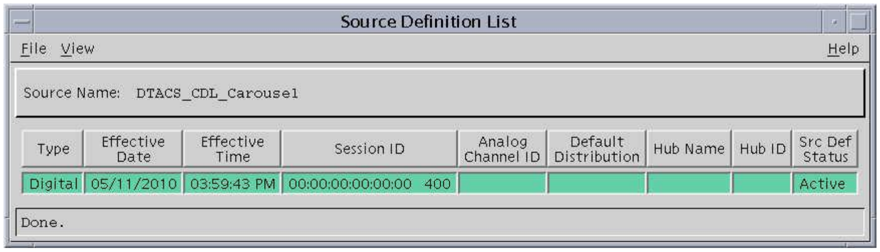

Multicast Digital Session Definition (wiley:8045) – Mozilla Firefox
File Edit View Go Tools Help
Help
Exit
Save
Cancel
Done

DNCS/Multicast Digital Session Definition

Multicast Digital Session Definition

Source ID:	DTACS_CDL_Carou	400
Session ID:	00:00:00:00:00:00	400
Bandwidth (Mbps):	1.3	
QAM Name:	Hub2gqam	
Output Carrier:	RF Out 2 Carrier 3	
Program Number:	132	
Source IP Address1:	10.253.0.2	
Source IP Address 2:		
Source IP Address 3:		
Input Destination Multicast IP Address:	232.232.0.255	
UDP Port:	2002	

4 Save the session. The Source Definition List screen should show the session as active.



Source Name: DTACS_CDL_Carousel

Type	Effective Date	Effective Time	Session ID	Analog Channel ID	Default Distribution	Hub Name	Hub ID	Src Def Status
Digital	05/11/2010	03:59:43 PM	00:00:00:00:00:00 400					Active

5 From the DTACS System Configuration screen, click **Sync DB** to sync the DTACS and DNCS databases.

6 Log in to the DTACS and assume the dtacs role; then type **mkdir /dvs/dtacs/dtacsFiles/images** to create the images directory on the DTACS Server. Users will store the DTA code files (or "DTA images") in this directory.

```
boris:/dvs/dtacs/dtacsFiles> ls -l
drwxrwxr-x   2 dtacs    dtacs        512 Jun 29 15:55 images
```

7 Make sure that the image files are on the DNCS, then use **scp** to copy the files from the DNCS directory to the DTACS.

Example: `scp/tmp/DTA1x.x.x.xxxx_xx_X.p.simg jsmith@dtacs:/tmp`

Note: You cannot complete this step as dtacs or root user role, and you cannot copy the files directly into the /dvs/dtacs/dtacsFiles/images directory.

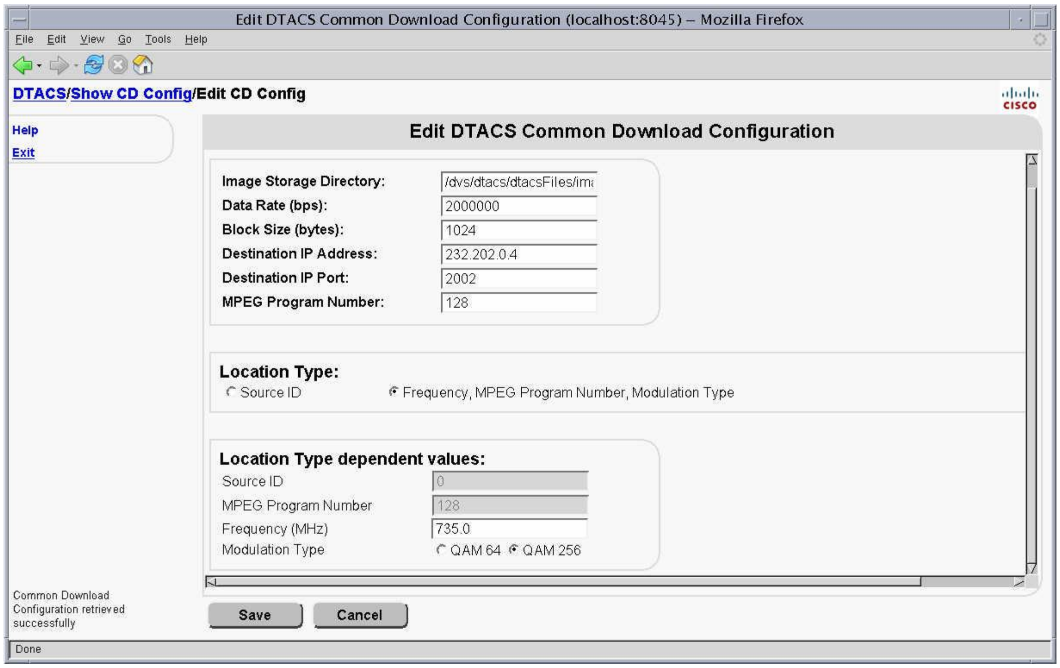
8 On the DTACS, as the dtacs user, use **cp** to copy the files into the /dvs/dtacs/dtacsFiles/images directory.

Example:

```
cp
/tmp/DTA1.x.x.xxxx_xx_X.p.simg /dvs/dtacs/dtacsFiles/images/DTA1.x.x.xxxx_xx_
X.p.simg
```

9 Click **Edit** on the DTACS Common Download Configuration screen and define the following parameters:

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 1,000,000 and 2,000,000 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


Edit DTACS Common Download Configuration (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/Show CD Config/Edit CD Config
Help
Exit
Save
Cancel
Done

Edit DTACS Common Download Configuration

Image Storage Directory: /dvs/dtacs/dtacsFiles/ima

Data Rate (bps): 2000000

Block Size (bytes): 1024

Destination IP Address: 232.202.0.4

Destination IP Port: 2002

MPEG Program Number: 128

Location Type:

○ Source ID ● Frequency, MPEG Program Number, Modulation Type

Location Type dependent values:

Source ID: 0

MPEG Program Number: 128

Frequency (MHz): 735.0

Modulation Type: ○ QAM 64 ● QAM 256

Common Download Configuration retrieved successfully

10 Define the following parameters on the DTACS DTA Image Association screen. Use one of the DTA images copied to the /dvs/dtacs/dtacsFiles/images directory):

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 **0x223a**.
Hardware ID	Select the correct hardware ID for the DTAs that will receive this image. **Example:** For DTA30s, select **0x643**.
Download Command	Select **Immediate**. **Note:** This field only displays when you are adding or editing an image association.

Notes:

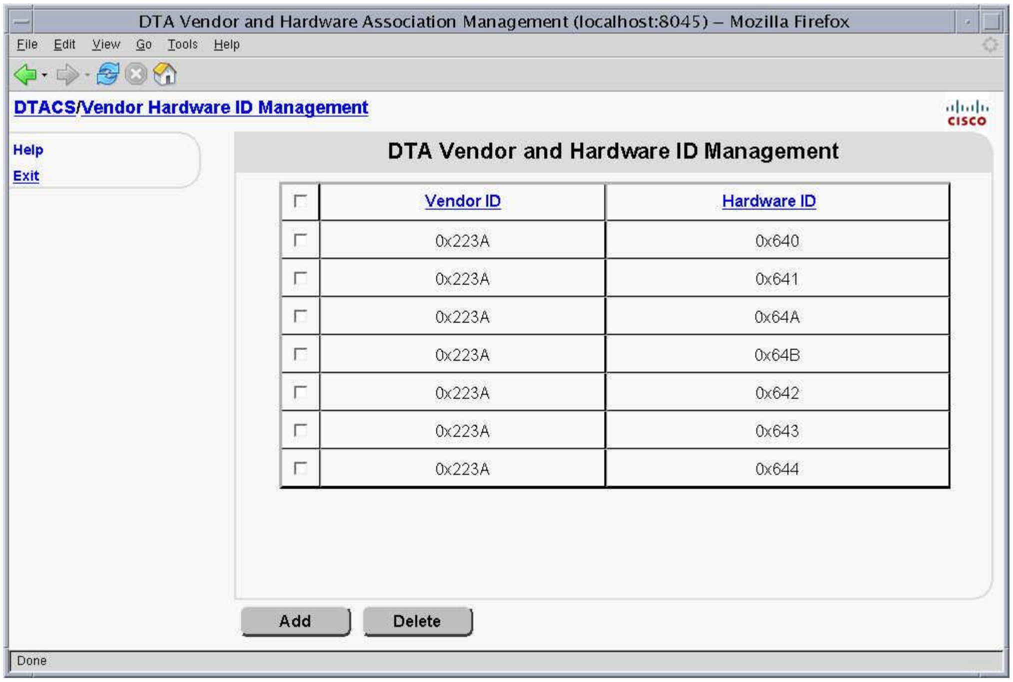
- Saving this Image Association should create a CVT file in the /dvs/dtacs/pub directory on the DTACS Server. The DTACS server should send this CVT information out every minute on the SI IP Stream to all the DTACS PID Routes that are active. Sending the CVT every minute is the default setting for the dtacsCvtMgr. This default is set using the variable CVT_REPEAT_RATE in /dvs/dtacs/etc/cvtMgr.cfg.

- The dataPump's session should appear active on the GQAM's output as seen on the GQAM's LCD.
- If you define a Source ID Location Type when you configure the carousel, then the DTAs must have a VCT assigned to them, and the source must be active on the DNCS. With these conditions met and a code image loaded on the carousel, all VCTs will have a hidden channel for the Image Carousel source. The hidden channel is shown on the DTA's Virtual Channel Map Diag Screen, and the source is placed in all active VCTs.
- Do not manually add this source to a VCT.

Add a New Vendor and Hardware ID

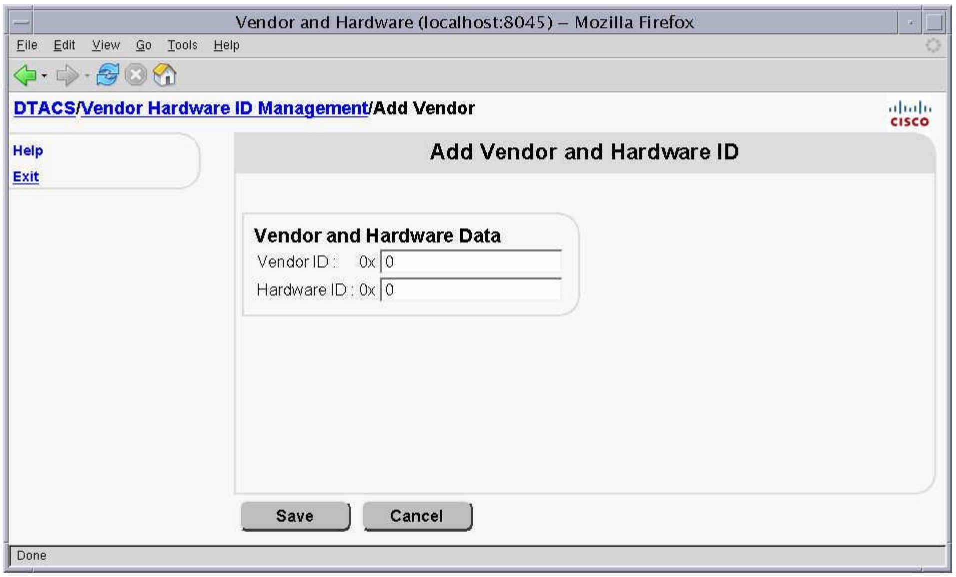
Follow these steps to add a new vendor and hardware ID to the system.

1 Click **Vendor and Hardware ID** in the Common Download area of the DTACS main page. The DTA Vendor and Hardware ID Management screen appears.


DTA Vendor and Hardware Association Management (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/Vendor Hardware ID Management
Help
Exit
DTA Vendor and Hardware ID Management
Add
Delete
Done

□	Vendor ID	Hardware ID
□	0x223A	0x640
□	0x223A	0x641
□	0x223A	0x64A
□	0x223A	0x64B
□	0x223A	0x642
□	0x223A	0x643
□	0x223A	0x644

2 Click **Add**. The Add Vendor and Hardware ID screen appears.


Vendor and Hardware (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/Vendor Hardware ID Management/Add Vendor
Help
Exit
Save
Cancel
Done

Add Vendor and Hardware ID

Vendor and Hardware Data

Vendor ID : 0x 0

Hardware ID : 0x 0

3 Type the vendor ID and hardware ID for the hardware you are adding, and click **Save**.

Note: The vendor ID for Cisco is 0x223a, and the hardware ID for DTA30s is 0x643.

4 Repeat steps 2 and 3 if you need to add another vendor and hardware ID.

Manage Image Associations

The following sections explain how to add, edit and delete image associations on the DTACS Server.

Note: Before you begin, the vendor and hardware ID must be added to the system. See ***Add a New Vendor and Hardware ID*** (on page 120) if you need to add a vendor or hardware ID.

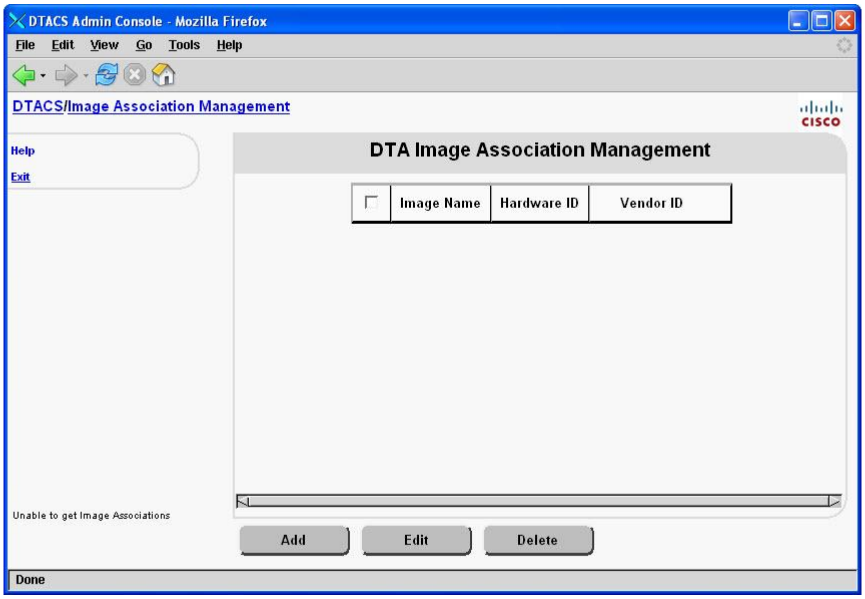
Add an Image Association

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

1 On the DTACS main window, click the DTACS tab.

2 Click the **Provisioning** tab.

3 Click **Image Association**. The DTA Image Association Mangement window opens.


DTACS Admin Console - Mozilla Firefox
File Edit View Go Tools Help
DTACS/Image Association Management
Help
Exit
DTA Image Association Management
Image Name
Hardware ID
Vendor ID
Add
Edit
Delete
Done

Unable to get Image Associations

4 Click **Add**. The Add DTA Image Association window opens.

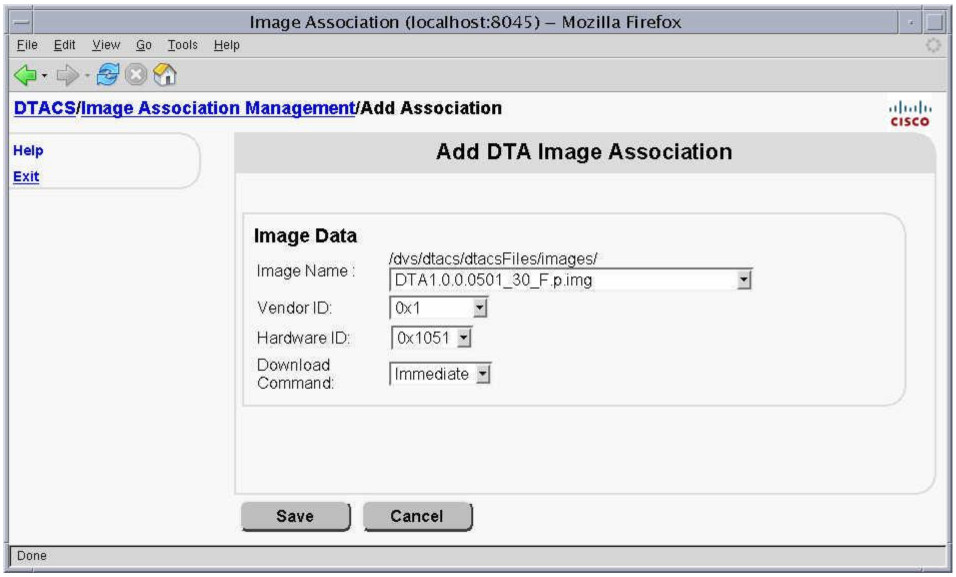


Image Association (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/Image Association Management/Add Association
Help
Exit
Add DTA Image Association
Image Data
Save
Cancel
Done

Image Name :	/dvs/dtacs/dtacsFiles/images/ DTA1.0.0.0501_30_F.p.img
Vendor ID:	0x1
Hardware ID:	0x1051
Download Command:	Immediate

5 Complete the fields on the screen as shown in the following table:

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 you can edit after you create the association.
Vendor ID	Select the distributor of the image file from the drop-down list. **Example:** Cisco is 0x223a.

Field	Description
Hardware ID	Select the correct hardware ID for the DTAs that will receive this image. **Example:** For DTA30s, select 0x643.
Download Command	Select Immediate.

6 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 0 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.
- Do not add this source manually to a VCT.

7 Click **Exit** to close the DTA Image Mangement 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 Management**. 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.

Delete an Image Association

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

1. Click **Image Management**. The DTA Image Association Management window opens.
2. Select the image association(s) 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.

Manage CVTs

The DTACS web-based user interface provides a way to provision Code Version Table (CVT) entries. You can use the DTACS web-based user interface to add, query, edit, and delete CVTs.

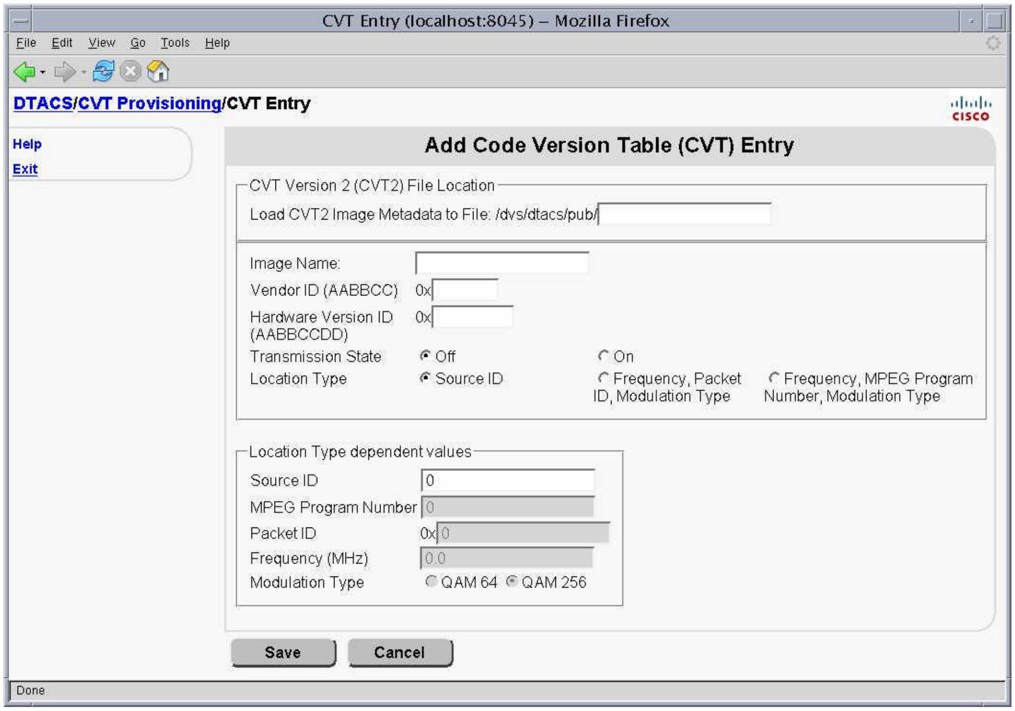
Add a CVT

Follow these steps to add a CVT entry.

1 Click **Add**.

Results:

- The Add Code Version Table (CVT) Entry window appears.
- Configuration fields for a new CVT entry appear on the Add CVT page.
- The 'Create a new CVT entry' message appears.
- The **Save** and **Cancel** buttons appear on the bottom of the window.


CVT Entry (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
Help
Exit
Save
Cancel
Done

DTACS/CVT Provisioning/CVT Entry

Add Code Version Table (CVT) Entry

CVT Version 2 (CVT2) File Location

Load CVT2 Image Metadata to File: /dvs/dtacs/pub/

Image Name:

Vendor ID (AABBCC) 0x

Hardware Version ID (AABBCCDD) 0x

Transmission State ● Off ○ On

Location Type ● Source ID ○ Frequency, Packet ID, Modulation Type ○ Frequency, MPEG Program Number, Modulation Type

Location Type dependent values

Source ID 0

MPEG Program Number 0

Packet ID 0x 0

Frequency (MHz) 0.0

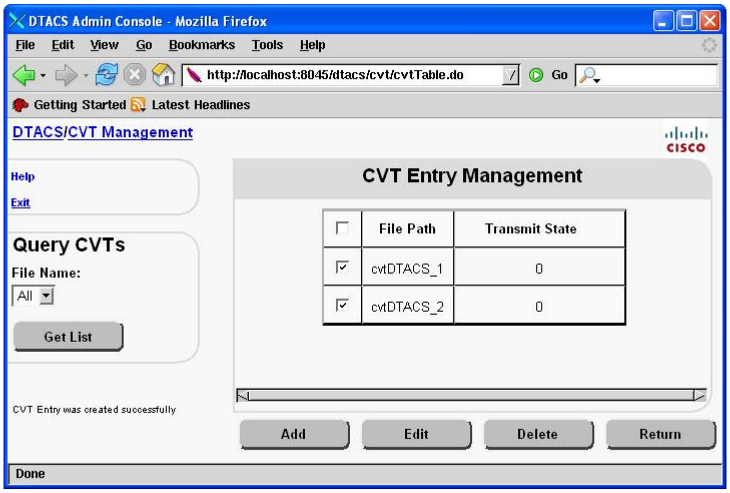
Modulation Type ○ QAM 64 ● QAM 256

2 Press the Tab key to go to the fields you want to add. The following table describes the fields that can be added on this page.

Note: Any changes made to this screen do *not* affect CVTs that were created by the Image Association page.

Configuration Field	Description
Load CVT2 Image Metadata to File	The unique name of the CVT entry you are creating. This name will appear in the File Path column on the CVT Management window.
Image Name	The name of an 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 either Off or On.
Location Type	Specifies the location of the download code. Select one of three options: ■ Source ID ■ Frequency, Packet ID, Modulation Type ■ Frequency, MPEG Program Number, Modulation Type
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.
Frequency	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 either QAM64 or QAM256.

3 Click **Save** if you want to save your changes. The IP Streams List appears and the 'CVT Entry was created successfully' message appears.



CVT Entry Management

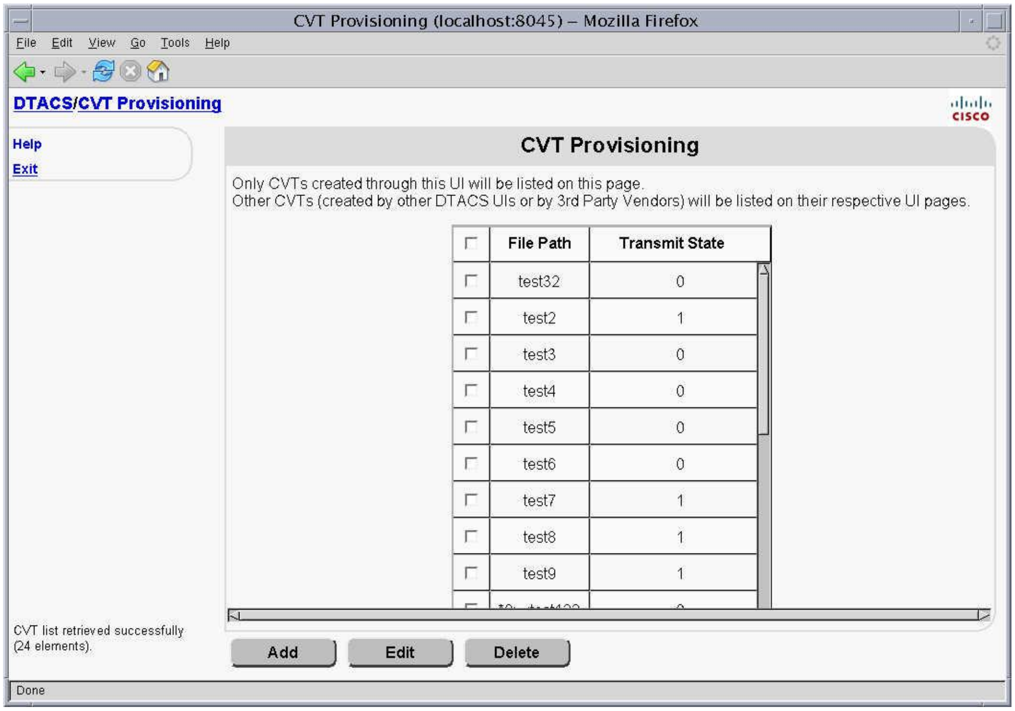
□	File Path	Transmit State
☑	cvtDTACS_1	0
☑	cvtDTACS_2	0

CVT Entry was created successfully

Query a CVT

Follow these steps to select and query CVT entries.

1 Click **CVT Provisioning** text on the DTA Control System's main page. The CVT Entry Management window appears.


CVT Provisioning (localhost:8045) – Mozilla Firefox
File Edit View Go Tools Help
DTACS/CVT Provisioning
cisco
Help
Exit
Add
Edit
Delete
Done

CVT Provisioning

Only CVTs created through this UI will be listed on this page.
Other CVTs (created by other DTACS UIs or by 3rd Party Vendors) will be listed on their respective UI pages.

□	File Path	Transmit State
□	test32	0
□	test2	1
□	test3	0
□	test4	0
□	test5	0
□	test6	0
□	test7	1
□	test8	1
□	test9	1

CVT list retrieved successfully (24 elements).

Note: You can click **Return** to go back to DTACS main page.

2 Click **Show**. The IP Stream Table window displays all of the items that meet the selected criteria.

Edit a CVT

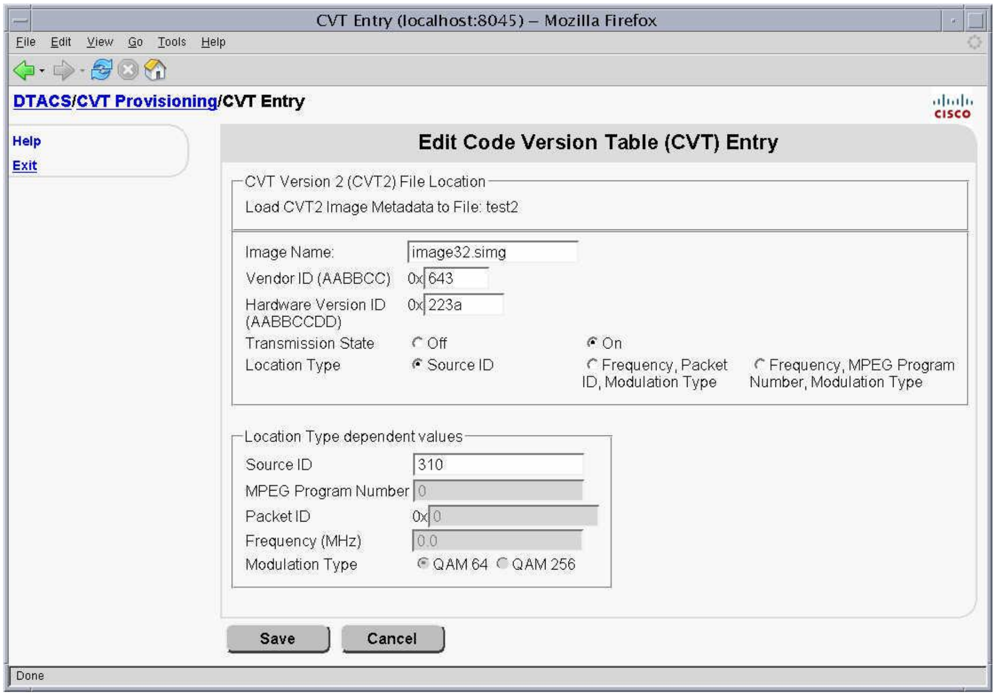
Follow these steps to edit a CVT entry's information.

Note: If the Location ID Type=0, then the source will be added to all active VCTs.

1 Select a row on the IP Streams List page.

2 Click **Edit**. The Edit Code Version Table (CVT) Entry window and the 'Edit a CVT Entry' message appear.

3 Press the tab key to go to the field you want to update.


CVT Entry (localhost:8045) – Mozilla Firefox
File
Edit
View
Go
Tools
Help
DTACS/CVT Provisioning/CVT Entry
cisco
Help
Exit
Save
Cancel
Done

Edit Code Version Table (CVT) Entry

CVT Version 2 (CVT2) File Location

Load CVT2 Image Metadata to File: test2

Image Name: image32.simg

Vendor ID (AABBCC) 0x 643

Hardware Version ID (AABBCCDD) 0x 223a

Transmission State ○ Off ● On

Location Type ● Source ID ○ Frequency, Packet ID, Modulation Type ○ Frequency, MPEG Program Number, Modulation Type

Location Type dependent values

Source ID 310

MPEG Program Number 0

Packet ID 0x 0

Frequency (MHz) 0.0

Modulation Type ● QAM 64 ○ QAM 256

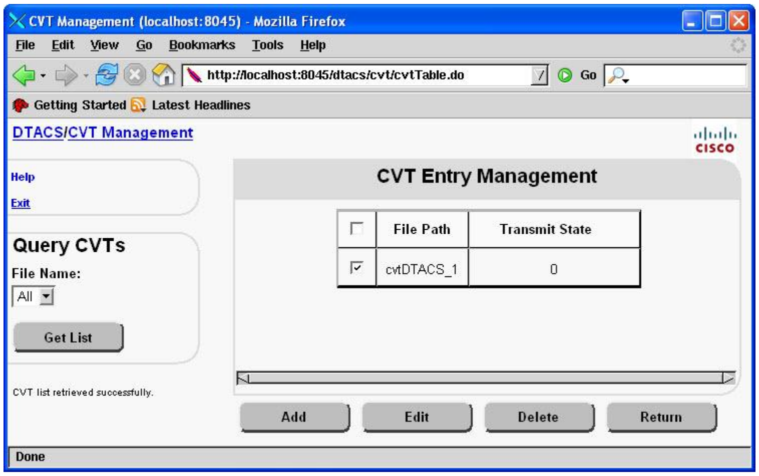
4 Click **Save** to save your changes.

Delete a CVT

Follow these steps to delete a CVT entry.

1 Click the check box next to the CVT entry you want you want to delete on the CVT Entry Management List page. A check mark appears in the check box.

2 Click **Delete**. The CVT Entry Management List page appears and the IP Stream you selected is not listed in the streams list.


CVT Management (localhost:8045) - Mozilla Firefox
File Edit View Go Bookmarks Tools Help
http://localhost:8045/dtacs/cvt/cvtTable.do
Go
Getting Started
Latest Headlines
DTACS/CVT Management
Help
Exit
Get List
Add
Edit
Delete
Return
Done

Query CVTs

File Name: All

CVT list retrieved successfully.

CVT Entry Management

□	File Path	Transmit State
☑	cvtDTACS_1	0

3 Click the **DTACS** text at the top of the window to return to the DTACS main page.

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 similar to 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 DNCS 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 steps 13 and 14.

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

Customer Information

If You Have Questions

If you have technical questions, call Cisco Services for assistance. Follow the menu options to speak with a service engineer.

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

A

Managing DTACS User Accounts

This appendix contains procedures for managing user accounts on the DTACS Server. The appendix includes descriptions of user accounts, password expiration rules and role-based access control.

In This Appendix

DTACS Security

Administrative Users

Administrative users (admins) are the only users who can assume the dtacs role. Users who do not have administrative privileges cannot access the DTACS WUI. The following sections include information about managing all types of users.

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

We have implemented role-based access control as part of the DTACS operating system. Role-based access control allows system admins to assign control of parts of the system to specific users. System admins can also limit system access to specific users.

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

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

	Files		Commands	Database		
Role/Account	**Read**	**Write**	**Execute**	**Read**	**Write**	**Alter**
Root	Y	Y	Y	Y	Y	Y
DTACS Role	Y	Y	Y	Y	Y	Y
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 WUI 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 Server using “dtacs” and the dtacs role password.
- DTACS now uses SFTP instead of FTP, because SFTP is a more secure method of transferring data.

For more detailed information about security enhancements, refer to *IBDS Security Enhancements Instructions* (part number 4027701).

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

User Accounts

This section describes how to create and delete user accounts.

Create a User Account

1. Open an xterm window on the DTACS Server.
2. Log into the DTACS Server as **root**.
3. Type **/dvs/dtacs/etc/create_users** and press **Enter**. The Choose Type of User to Add menu appears.

   ```
   --------------------------
   Choose Type of User to Add
   --------------------------
   1: Add Regular User (has no DNCS/RNCS privileges)
   2: Add Operator (has DNCS/RNCS read privileges)
   3: Add Administrator (has DNCS/RNCS read & write privileges)
   Please enter choice or 'Q' to exit:
   ```

4. Select the user type for the account you want to add.
5. Type the name of the new user account and press **Enter**. The user name must be between 6 and 8 alphanumeric characters and cannot contain special characters. The **Do you wish to continue adding this user (Y/N)?** message appears.
6. Type **y** (for yes) and press **Enter**.
7. Type the **password** for the user and press **Enter**.
8. Type the **password** for the user again and press **Enter**. The create_users program exits.

Delete a User 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.

Important: Even when you delete a user, the user's name still exists in the password history file. We recommend that you **do not edit this file.**

If you delete a user, then add the same user again, the user's old password history remains in effect and the password history file contains the user's last five passwords. The user cannot change their password to one of the five passwords in the password history file.

Database Access

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

- root user: DBA, connect, resources
- dtacs role: Connect and select, insert, update and delete tables
- dtacsSSH: Connect and select tables
- public: No access

Follow these steps to see a list of users and their access privileges.

1. Open an xterm window on the DTACS Server.
2. Log into the DTACS Server as a **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**.

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

Log On

Follow this procedure to log into the CDE at the DTACS Server terminal.

1. At the DTACS Server terminal, type your **user name** and press **Enter**.
2. At the prompt, type your **password** and press **Enter**. A DTACS Server prompt should appear on the screen.
3. Before you execute any DTACS Server commands (such as dtacsStart or dtacsStop), type **sux - dtacs** and press **Enter**.
4. Before you launch any DTACS Server user interface windows (such as the Administrative Console), type the following commands:

   export DISPLAY= : 0.0 and press **Enter**

   xhost + and press **Enter**

You can only have one active session for SSH, SFTP, and CDE sessions for any user name.

Note: This does not apply to the dtacs role or to the root user.

This restriction can be changed for a user by modifying the project file entry for that user.

Override Session Limitations on DTACS

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]

   Notes:

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

Session Security Enhancements

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.

Important: Whenever you change an environment variable in .profile, you must then source the file. Type **. /export/home/dtacs/.profile** and press **Enter**. (Be sure to type a space between the first . and /.) Then run the dtacsStop and dtacsStart commands.

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 lines to the .profile file:

   export TIMEOUT=[seconds]
   export TMOUT=[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**, add the following lines:
  export TIMEOUT=300
  export TMOUT=300
- To enter a session locking time of **15 minutes**, add the following lines:
  export TIMEOUT=900
  export TMOUT=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.

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.

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.

Changing a User Account Password

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: Users can change their 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: Users can change their own account password. 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: Users can change their own account password. 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.

Change the Password Expiration Period

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

Important:

- New users added to the server 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.

Change a User Password Expiration Period

Use this procedure to change the password expiration period for an individual user account.

1 Open an xterm window on the DTACS.

2 Log into the DTACS Server as **root**.

3 Type **passwd -r files -x [days] [username]** and press **Enter**.

Notes:

- Type the number of days before a user password expired for **[days]**.
- Type the username for **[username]**.
- Do not type the brackets **[ ]** in the command.

4 Verify the expiration period by typing **passwd -s [username]** and press **Enter.**

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

```
dtacs     PS             09/02/09              91       14

user      pw_status      date          MIN     MAX      WARN
```

- The **date** (09/02/08) is the date the password was set by the user (dtacs).
- The **MIN** (blank) is the minimum number of days before a user is allowed to change the password. We recommend that you leave this field blank.
- The **MAX** (91) is the number of days after the date that the password is valid.
- The **WARN** (14) is the number of days before the password expires that a warning banner is displayed.
- Type **exit** and press **Enter** to close the xterm window.

Disable the Password Expiration Period

You can disable the password expiration period that is applied when creating new users or when changing passwords or for an individual user.

Important:

- New users added to the server 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.

Disable the Password Expiration Period for the System

Use this procedure to *disable 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 **–1** (negative one).
7. Locate the following line in the passwd file:

   export WARNWEEKS=2
8. Change the warning period to **–1** (negative one).
9. Save the passwd file and close the text editor.
10. In the xterm window, type **source . ./passwd** and press **Enter**. The system will use the updated passwd file.
11. Type **exit** and press **Enter** to close the xterm window.

Important: Existing users' individual expiration periods remain in force until the user's password is changed (either by an administrator or by the user).

Disable the Password Expiration Period for a User

Use this procedure to *disable the password expiration period for an individual user account*. We recommend that you follow this procedure for the following user accounts at a minimum:

- root
- dtacs
- informix
- dtacsSSH
- dtacsftp
- easftp

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.

B

Troubleshooting the DTACS Server

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

In This Appendix

Correcting Java Errors in Firefox

These procedures may be used to help resolve Firefox exceptions that may occur when using a local machine's Firefox browser to connect to the remote DTACS (for example when using a Firefox browser on a PC to establish a UI connection to the remote DTACS server). These procedures do not apply when the DTACS Firefox browser is exported to a remote machine.

Follow these steps to correct Java errors in Firefox:

1. Clear the Firefox Browser Cache
2. If the issues are not resolved, stop and re-start the Tomcat process.

Clearing the Firefox Browser Cache

With the Firefox browser open on the local machine, perform the following steps in the browser.

Note: The browser does not need to be connected to the DTACS while performing these steps.

If you are using **Firefox Vers 3.6**:

1. Select **Tools** > **Clear Recent History.**
2. In the **Time range to clear** drop-down box, select **Everything.**
3. In the **Details** area, clear the check box beside every item *except* **Cache.**
4. Click **Clear Now**.
5. Close the Firefox browser and re-open it to establish a new connection to the DTACS UIs.

If you are using **Firefox Vers 3.0**:

1. Select **Tools** > **Clear Private Data.**
2. Clear the check box beside every item *except* Cache.
3. Click **Clear Private Data Now**.
4. Close the Firefox browser and re-open it to establish a new connection to the DTACS UIs.

Stopping the Tomcat Process

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

1. Select **File > Exit** from the File menu on the DTACS WUI to close the Firefox browser connection to the DTACS.
2. Open an xterm connection to the DTACS and type `su - root` to change to the root userid.

3 Type the password for the root user at the password prompt.

4 Type `svcadm disable apache-tomcat` and press **Enter** to stop the Tomcat process.

5 Type `svcs -a | grep apache-tomcat` and press **Enter** to monitor the state of apache-tomcat. When the state changes to disabled, then proceed with starting apache-tomcat.

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 At the prompt, type `pwd` and press **Enter** to verify that you are in the webui work directory. The directory name appears at the system prompt.

3 At the root prompt, type `rm -rf*` and press **Enter** to remove all files from the webui work directory.

Starting the Tomcat Process

1 Log into the DTACS as root user.

2 Type `svcadm enable apache-tomcat` and press **Enter** to start the Tomcat process.

3 Type `svcs -a | grep apache-tomcat` and press **Enter** to monitor the state of apache-tomcat. When the state changes to online, then proceed to the next step.

4 Type `exit` and press **Enter** to stop using the root userid. The system prompt displays.

5 Launch the Firefox browser and connect to the DTACS UI.

If Firefox issues still exist, then call Cisco Services for assistance in resolving the error.

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.

C

Backup and Restore the DTACS File System and Database

This appendix contains procedures to back up data on the DTACS Server to tape media. This stored information can be used to restore the DTACS Server if the system suffers an outage.

In This Appendix

Back Up the DTACS File System

Consider the following points about a backup of the DTACS server file system.

System Shutdown No Longer Required for File System Backups

System operators do not have to shut down their system in order to back up the DTACS server file system.

Important: Even though you are not required to shut down the system components, we recommend that you schedule your file system backups for periods of lowest system activity.

Recommended Frequency

We recommend that you perform a complete system backup at least once a month, just prior to upgrading to new system software, and immediately after the upgrade.

Filesystem Backup Script Options

The script that backs up the file system is called backupFileSystems. You can run the backupFileSystems script with the following options:

- **-l** - Local-tape-drive. Specifies the tape drive to use on the local host computer.

  (for example - /dev/rmt/0h)

- **-r** - Remote-tape-drive. Specifies a tape drive on a remote host computer.

  (for example - sparky:/dev/rmt/0h or 192.168.1.10:/dev/rmt/0h)

- **-B** - Backup directory. Specifies the directory to which the backup of the file system will be saved.

  The backup directory must be on an NFS-mounted filesystem.

- **-v** - verbose. Verbose output.
- **-t** - tape label. Backup tape label. This must be a unique string with no spaces.
- **-h** - help. Provides a brief description of the valid options.

Backing Up the DTACS File System

1 Insert the DVD labeled **DTACS Maintenance DVD** into the DVD drive of the DTACS server.

2 Type **df -n** and press **Enter**. A list of mounted file systems appears.

Note: The presence of /cdrom in the output confirms that the system correctly mounted the DVD.

3 Label a blank tape with the following information:

[DTACS Server] File System Backup [Date]
[Site Name]
[Software Version]
DTACS Maintenance DVD x.x.x

4 Log in as **root** user.

5 Insert the blank tape into the tape drive of the DTACS server and wait for the green light to stop flashing.

6 Type **/cdrom/cdrom0/s3/backup_restore/backupFileSystems -v** and press **Enter**. The system backs up the DTACS file system, ejects the tape, and displays a message when the backup is complete.

7 When the backup is complete, remove the tape and store it in a safe place.

8 Type **eject cdrom** and then press **Enter**.

Back Up the DTACS Database

This section provides procedures for backing up the DTACS database to tape.

Database Backup Script Options

The script that backs up the databases is called backupDatabase. You can run the backupDatabase script with the following options:

- **-b** - Blocks. Specifies the block size of the tape device to which the database backup is written.

  Note: If -b is not specified, the system uses a default tape block size appropriate for your tape drive. If the system is unable to determine your tape drive, the system uses 32.

- **-s** - Size. Specifies the size of the tape device to which the database backup is written.

  If -s is not specified, the system uses a default tape size appropriate for your tape drive. If the system is unable to determine your tape drive, the system uses 8000000.

- **-l** - Local-tape-drive. Specifies the tape drive to use on the local host computer. (for example - /dev/rmt/0h)
- **-r** - Remote-tape-drive. Specifies a tape drive on a remote host computer. (for example - sparky: /dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- **-c** - check-database. Checks the integrity of the databases. (Does not fix if errors are found.)
- **-n** - non-interactive. Non-interactive, useful when running from cron.
- **-v** - verbose. Verbose output.
- **-h** - help. Provides a brief description of the valid options.

Restore the DTACS File System

Consider the following points about the restoration of the DTACS file system.

Prerequisite

You need the following items:

- The tape from your most recent file system backup.
- An external eSATA/USB DVD-RRW drive, provided by Cisco (Addonics model AEPDRRWUE).
- A DTACS DVD, provided by Cisco. The DVD should be labeled DVD release 1.2.0.4/App release 1.2.0.7.
- A laptop with all required cables and connectors to access the iLOM/System console through the serial port.

Important: Be sure your tapes are write-protected before you use them to restore the system.

File System Restore Script Options

The script that restores the DTACS file system is called restoreFileSystems. You can run the restoreFileSystems script with the following options:

- **-l** - Local-tape-drive. Specifies the tape drive to use on the local host computer.

  (for example - /dev/rmt/0h)
- **-r** - Remote-tape-drive. Specifies a tape drive on a remote host computer.

  (for example - sparky:/dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- **-B** - Backup directory. Specifies the directory that contains the backup from which the file system will be restored. The backup directory must be on an NFS-mounted filesystem.
- **-v** - verbose. Verbose output.
- **-i** - interactive. Runs the restoration script in interactive mode.
- **-h** - help. Provides a brief description of the valid options.

Note: The -l, -r, and -B options are mutually exclusive of one another; only one of them can be used.

Shutdown the DTACS Server

These steps must be performed during maintenance window.

1 Open an xterm window.

2 As **dtacs** user, type **dtacsStop** and press **Enter**. The DTACS processes are stopped.

Note: Eject any existing DVD media from the internal SATA DVD drive that's currently mounted by the OS. From the root shell prompt, type **eject** and press **Enter**.

3 Type **sux – root** and press **Enter** to change to the root user.

Note: When prompted for the password, enter the root password.

4 Type **eeprom auto-boot?** and press **Enter** to check the auto-boot OBP settings for the system.

5 Is auto-boot set to false?

- If **yes**, continue with step 6.
- If **no**, type **eeprom auto-boot?=false** and press **Enter**.

6 Type **init 5** and press **Enter** to shut down the DTACS server gracefully and power off the system.

Connect the External DVD Drive

Important: Be sure that the system is powered off before following these instructions.

1 Pull the front panel of the DTACS server downward to expose the internal DVD drive.

2 On the left side of the internal DVD drive, you will see a metal clip holding it into place. Pull the clip to the left and gently pull the DVD drive out.

Note: You only have to pull it out a few inches to sever the connection.

3 Plug the external DVDROM into USB (port 0) port on the back of the system.

Note: Make sure you have the USB & power adaptor plugged into the back of the DVD drive.

4 Insert the DTACS 1.2.0.4 DVD into the DVD drive

5 Use the Serial Management Connection to access the iLOM console of the system. From the iLOM login screen on your computer, log into the iLOM using the default login credentials. The iLOM prompt -> appears on your screen.

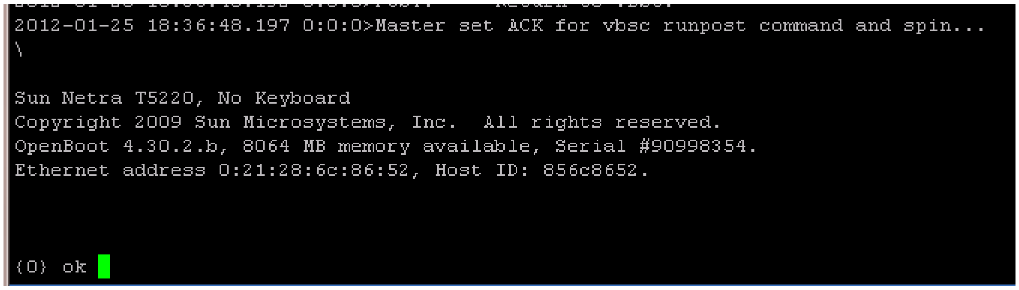
6 At the iLOM prompt (->) type the following commands and press Enter to set the input and output ports to "virtual-console":

set /HOST/bootmode script="setenv input-device=virtual-console"

set /HOST/bootmode script="setenv output-device=virtual-console"

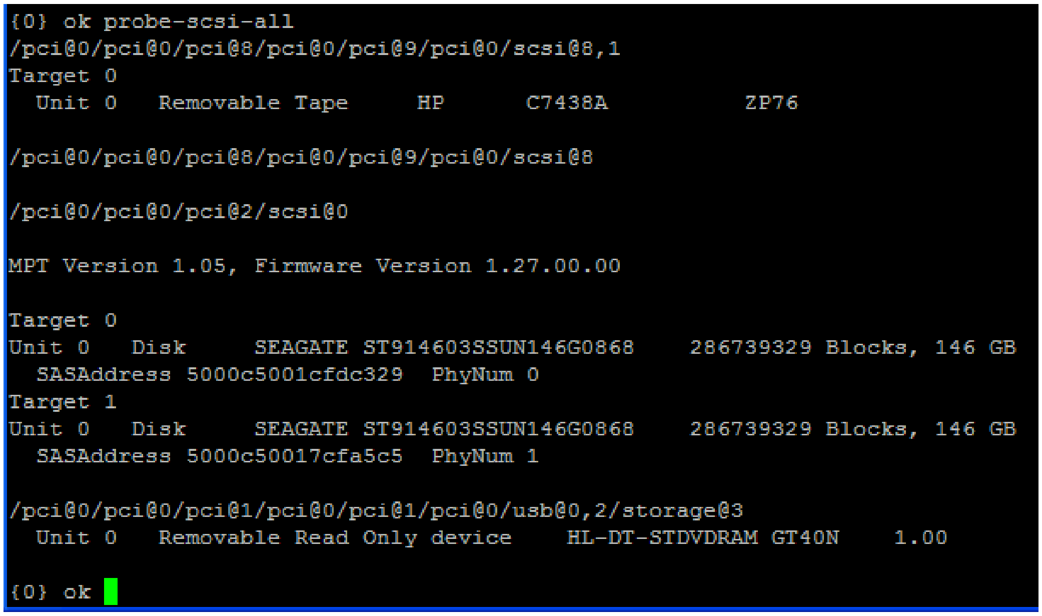
7 Type **start /SYS** and press **Enter** to power on the system.

8 Type **start /SP/console –f** and press **Enter** to start the console. When the POST test finishes, the ok prompt appears as shown below.



```
2012-01-25 18:36:48.197 0:0:0>Master set ACK for vbsc runpost command and spin...
\

Sun Netra T5220, No Keyboard
Copyright 2009 Sun Microsystems, Inc.  All rights reserved.
OpenBoot 4.30.2.b, 8064 MB memory available, Serial #90998354.
Ethernet address 0:21:28:6c:86:52, Host ID: 856c8652.



{0} ok
```

9 Type **probe-scsi-all** and press **Enter** to discover the physical address of the USB DVDROM. In the following example, the last device path listed maps to the external USB DVD drive attached to the system (/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3).



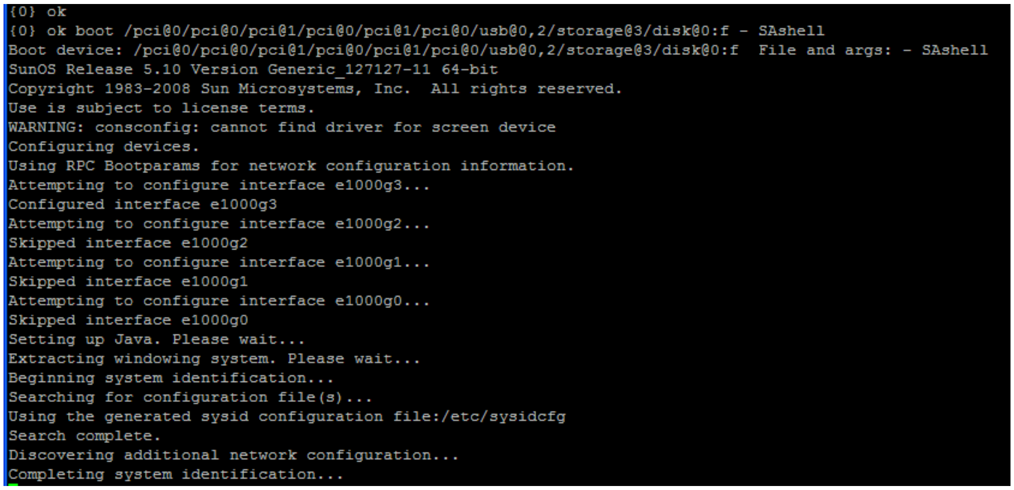
```
{0} ok probe-scsi-all
/pci@0/pci@0/pci@8/pci@0/pci@9/pci@0/scsi@8,1
Target 0
  Unit 0   Removable Tape     HP      C7438A          ZP76

/pci@0/pci@0/pci@8/pci@0/pci@9/pci@0/scsi@8

/pci@0/pci@0/pci@2/scsi@0

MPT Version 1.05, Firmware Version 1.27.00.00

Target 0
Unit 0   Disk     SEAGATE ST914603SSUN146G0868    286739329 Blocks, 146 GB
  SASAddress 5000c5001cfdc329  PhyNum 0
Target 1
Unit 0   Disk     SEAGATE ST914603SSUN146G0868    286739329 Blocks, 146 GB
  SASAddress 5000c50017cfa5c5  PhyNum 1

/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3
  Unit 0   Removable Read Only device    HL-DT-STDVDRAM GT40N    1.00

{0} ok
```

10 Type **boot <physical device path for the DVD>/disk@0:f – SAshell** at the ok prompt and press **Enter** to boot the system in SAshell mode. In the example shown, you would type:

Example: boot /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3/disk@0:f - SAshell

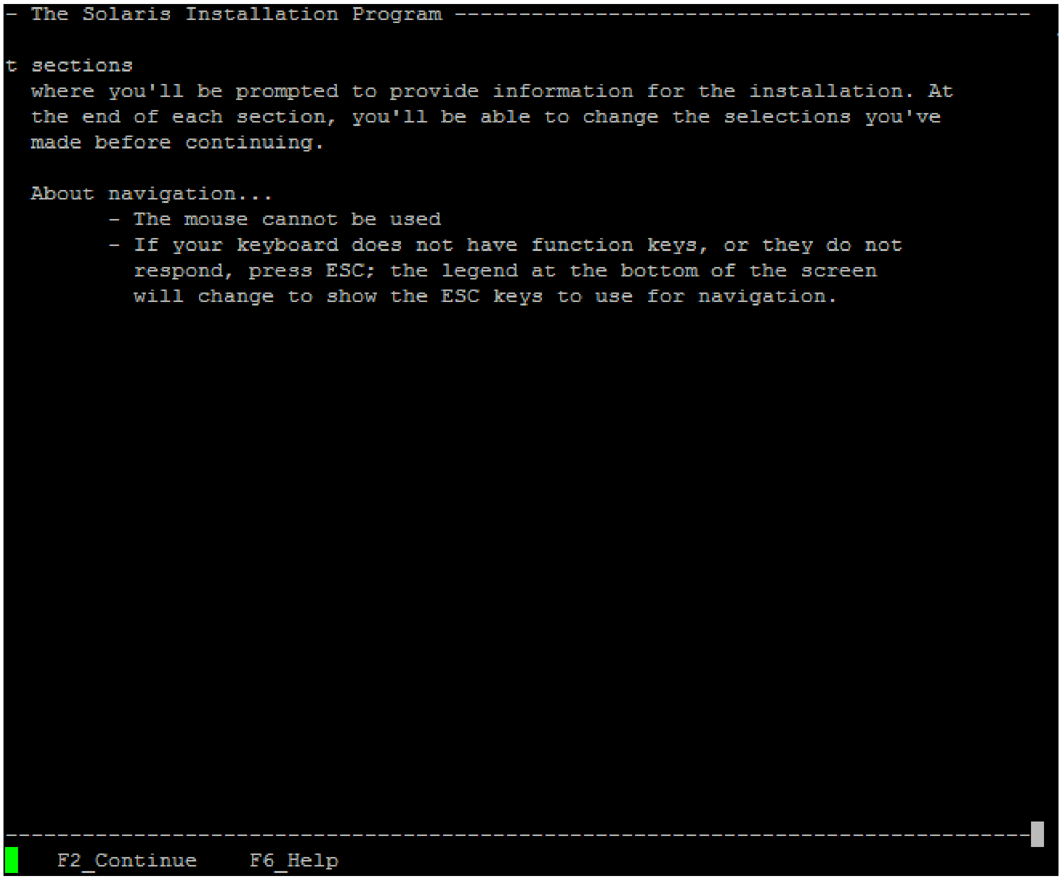
Important:

- Be sure to type a space before and after the – character in this command.
- Do **not** press Enter until you have typed the entire command to the end (SAshell). The command may wrap around to the next line, as shown in the following example.

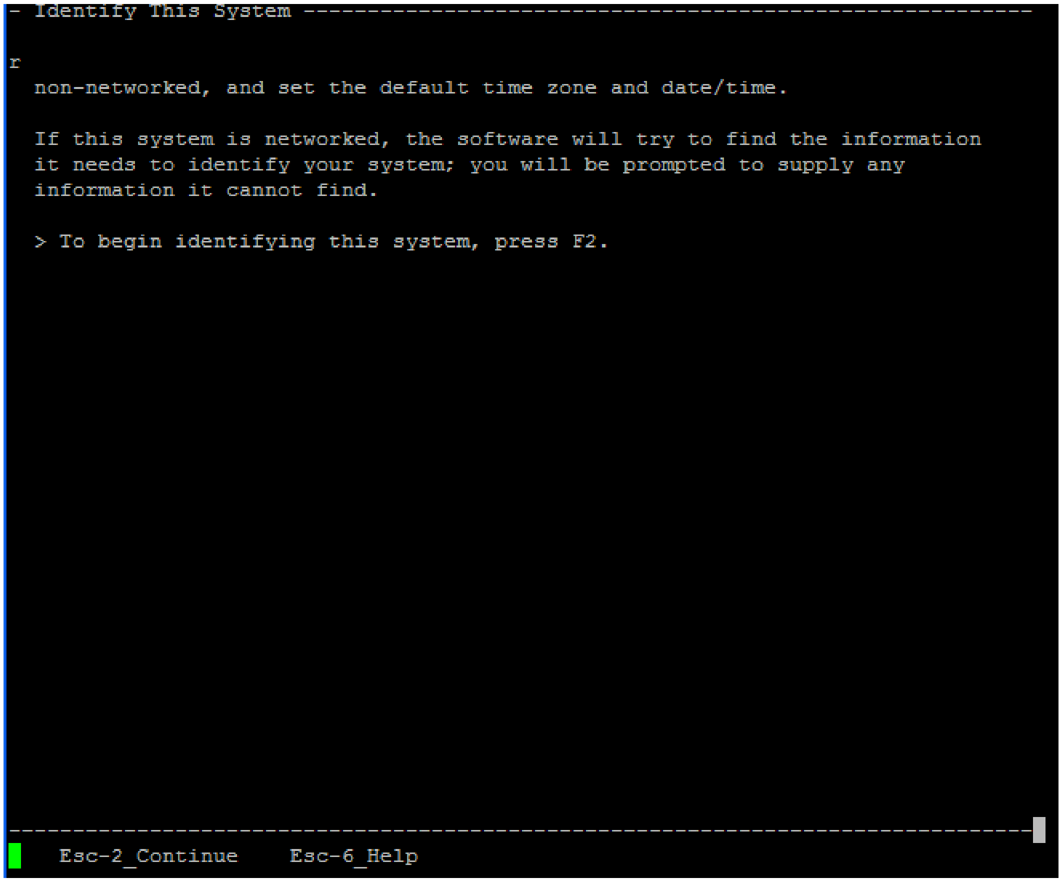


```
{0} ok
{0} ok boot /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3/disk@0:f - SAshell
Boot device: /pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3/disk@0:f  File and args: - SAshell
SunOS Release 5.10 Version Generic_127127-11 64-bit
Copyright 1983-2008 Sun Microsystems, Inc.  All rights reserved.
Use is subject to license terms.
WARNING: consconfig: cannot find driver for screen device
Configuring devices.
Using RPC Bootparams for network configuration information.
Attempting to configure interface e1000g3...
Configured interface e1000g3
Attempting to configure interface e1000g2...
Skipped interface e1000g2
Attempting to configure interface e1000g1...
Skipped interface e1000g1
Attempting to configure interface e1000g0...
Skipped interface e1000g0
Setting up Java. Please wait...
Extracting windowing system. Please wait...
Beginning system identification...
Searching for configuration file(s)...
Using the generated sysid configuration file:/etc/sysidcfg
Search complete.
Discovering additional network configuration...
Completing system identification...
```

11 Follow the on-screen prompts to complete the system identification configuration. Because your keyboard does not have function keys, you will use the **Esc** key followed by the number **2** key to proceed, as explained on-screen.

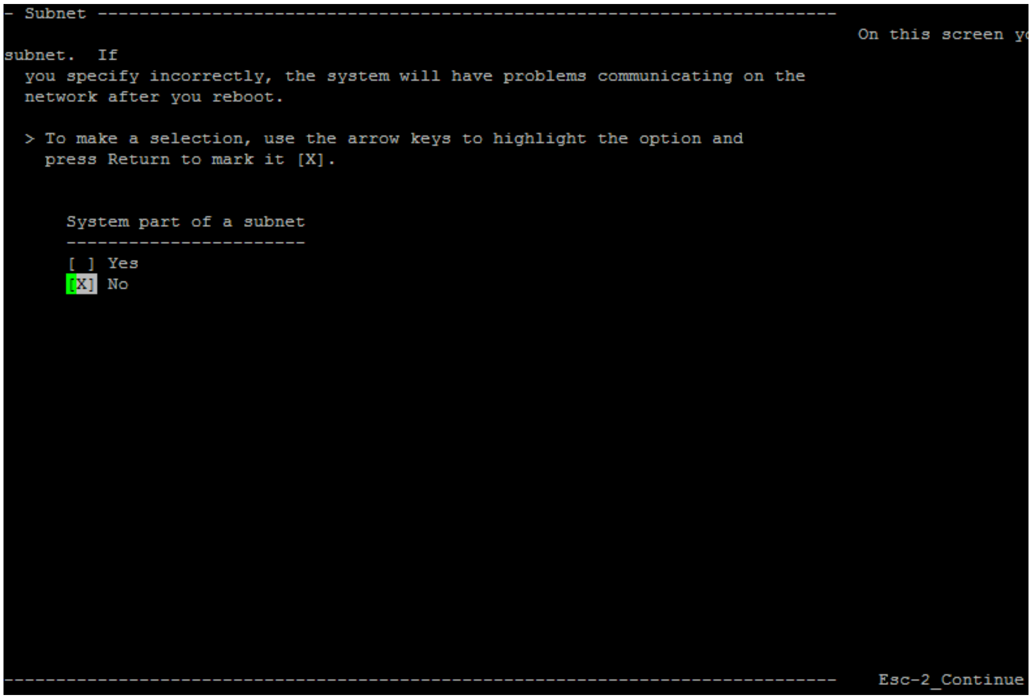


```
- The Solaris Installation Program -------------------------------------------

t sections
  where you'll be prompted to provide information for the installation. At
  the end of each section, you'll be able to change the selections you've
  made before continuing.

  About navigation...
        - The mouse cannot be used
        - If your keyboard does not have function keys, or they do not
          respond, press ESC; the legend at the bottom of the screen
          will change to show the ESC keys to use for navigation.

-------------------------------------------------------------------------------
    F2_Continue    F6_Help
```



```
- Identify This System -----------------------------------------------------------

r
  non-networked, and set the default time zone and date/time.

  If this system is networked, the software will try to find the information
  it needs to identify your system; you will be prompted to supply any
  information it cannot find.

  > To begin identifying this system, press F2.

--------------------------------------------------------------------------------
    Esc-2_Continue    Esc-6_Help
```

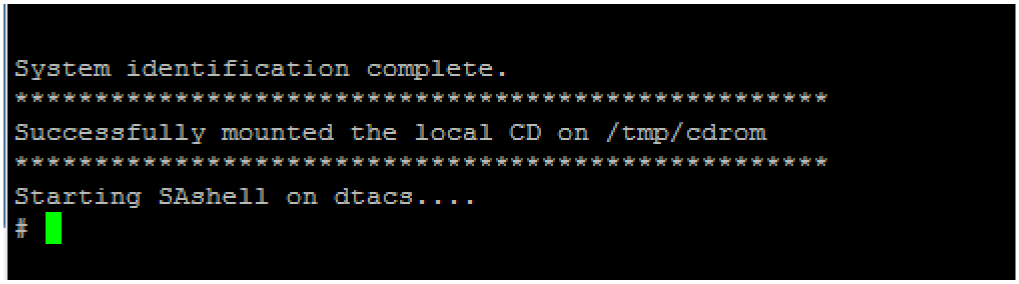
12 Use the down arrow key to move the selection to **No**, and press the SPACE bar key to select it. Press **Esc** and then type **2** to proceed.



```
- Subnet -----------------------------------------------------------------------
                                                                    On this screen y
subnet.  If
  you specify incorrectly, the system will have problems communicating on the
  network after you reboot.

  > To make a selection, use the arrow keys to highlight the option and
    press Return to mark it [X].


      System part of a subnet
      -----------------------
      [ ] Yes
      [X] No

--------------------------------------------------------------------------------    Esc-2_Continue
```

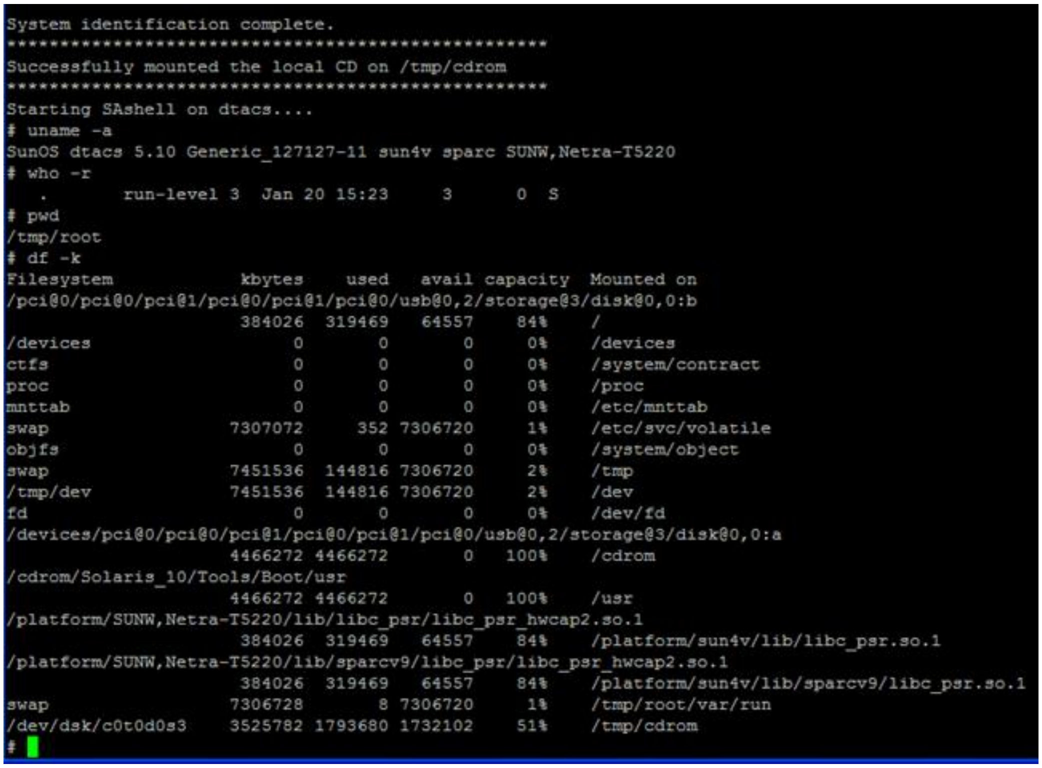
13 A prompt appears, asking you to confirm the selection you just made. Press **Esc** and then type **2** to proceed.

The system completes the system identification process and drops to SAShell mode as shown below.



```
System identification complete.
***************************************************
Successfully mounted the local CD on /tmp/cdrom
***************************************************
Starting SAshell on dtacs....
#
```

The following screenshot shows further information regarding the system and filesystem mounted after it completes booting to SAshell mode/prompt.



```
System identification complete.
***************************************************
Successfully mounted the local CD on /tmp/cdrom
***************************************************
Starting SAshell on dtacs....
# uname -a
SunOS dtacs 5.10 Generic_127127-11 sun4v sparc SUNW,Netra-T5220
# who -r
   .       run-level 3  Jan 20 15:23     3      0  S
# pwd
/tmp/root
# df -k
Filesystem            kbytes    used   avail capacity  Mounted on
/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3/disk@0,0:b
                       384026  319469   64557    84%    /
/devices                    0       0       0     0%    /devices
ctfs                        0       0       0     0%    /system/contract
proc                        0       0       0     0%    /proc
mnttab                      0       0       0     0%    /etc/mnttab
swap                  7307072     352 7306720     1%    /etc/svc/volatile
objfs                       0       0       0     0%    /system/object
swap                  7451536  144816 7306720     2%    /tmp
/tmp/dev              7451536  144816 7306720     2%    /dev
fd                          0       0       0     0%    /dev/fd
/devices/pci@0/pci@0/pci@1/pci@0/pci@1/pci@0/usb@0,2/storage@3/disk@0,0:a
                      4466272 4466272       0   100%    /cdrom
/cdrom/Solaris_10/Tools/Boot/usr
                      4466272 4466272       0   100%    /usr
/platform/SUNW,Netra-T5220/lib/libc_psr/libc_psr_hwcap2.so.1
                       384026  319469   64557    84%    /platform/sun4v/lib/libc_psr.so.1
/platform/SUNW,Netra-T5220/lib/sparcv9/libc_psr/libc_psr_hwcap2.so.1
                       384026  319469   64557    84%    /platform/sun4v/lib/sparcv9/libc_psr.so.1
swap                  7306728       8 7306720     1%    /tmp/root/var/run
/dev/dsk/c0t0d0s3     3525782 1793680 1732102    51%    /tmp/cdrom
#
```

File System Restore Script Options

The script that restores the DTACS file system is called restoreFileSystems. You can run the restoreFileSystems script with the following options:

- **-l** - Local-tape-drive. Specifies the tape drive to use on the local host computer.

  (for example - /dev/rmt/0h)
- **-r** - Remote-tape-drive. Specifies a tape drive on a remote host computer.

  (for example - sparky:/dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- **-B** - Backup directory. Specifies the directory that contains the backup from which the file system will be restored. The backup directory must be on an NFS-mounted filesystem.
- **-v** - verbose. Verbose output.
- **-i** - interactive. Runs the restoration script in interactive mode.
- **-h** - help. Provides a brief description of the valid options.

Note: The -l, -r, and -B options are mutually exclusive of one another; only one of them can be used.

Restoring the DTACS File System

1. Insert the backup tape in the tape drive.
2. Type **/tmp/cdrom/backup_restore/restoreFileSystems -v** and press **Enter**. The system restores the DTACS file system and displays a message when the restoration completes.
3. Type **shutdown -y -g0 -i6** and press **Enter**. The DTACS server reboots.
4. Log in as an admin user.
5. Type **pkginfo –l SAIdtacs** and press **Enter** to verify that the correct version of DTACS was restored:
   - If the correct version was restored, continue at step 6.
   - If the correct version was not restored, verify the tape used was correct. Go back to ***Shutdown the DTACS Server*** (on page 162) and repeat these steps.
6. Follow the procedures in ***Restore the DTACS Database*** (on page 170) to restore the DTACS database. After restoring the database, return to step 7 in this procedure.
7. Type **cd /etc/rc2.d** and press **Enter** to change the directory to /etc/rc2.d.
8. Type **mv _S98informix S98informix** and press **Enter** to move the Informix start up script back into place.
9. Type **eject cdrom** and press **Enter**. The system ejects the DVD.

10 Type **eeprom auto-boot?=true** and press **Enter** at the root shell prompt.

11 Type **touch /reconfigure** and press **Enter** to perform reconfiguration boot.

12 Type **shutdown -y –g0 –i5** and press **Enter** to gracefully shut down the OS and power off the system.

Note: Type **# .** to get iLOM prompt ->.

13 Disconnect the external USB DVDROM drive from the system and reinsert the internal SATA DVDROM drive that was disconnected earlier.

14 If you are using a monitor and keyboard, type the following commands and press **Enter** after each line to return them to their earlier settings.

set /HOST/bootmode script="setenv input-device=keyboard"

set /HOST/bootmode script="setenv output-device=screen"

15 At the iLOM prompt ->, type **start /SYS** and press **Enter** to power on the system.

16 Type **start /SP/console –f** and press **Enter** to access the system console to view POST messages and system boot.

17 At the OS login window (GUI, through monitor or CLI, through an iLOM serial), log as root (administrator) user.

Note: Use the GUI window if your monitor is connected to DTACS server, or use the CLI login if you are accessing the DTACS server console using your laptop through iLOM serial.

18 Switch to **dtacs** user (sux - dtacs), type **dtacsStart** and press **Enter**. The DTACS processes are started.

Important: Be sure that the DTACS server is fully functional and ready to run before you proceed.

19 Type **/cdrom/cdrom0/s3/backup_restore/mirrState -a** and press **Enter**. The system warns you that the submirrors for controller 2 will be attached.

20 Type **y** and press **Enter** to proceed. The system enables the disk mirroring functions on the DTACS server.

Note: This could take up to an hour to complete.

Restore the DTACS Database

This section contains information that guides you through the process of restoring the DTACS database.

Database Restore Script Options

The script that restores the databases is called restoreDatabase. You can run the restoreDatabase script with the following options:

- **-l** - Local-tape-drive. Specifies the tape drive to use on the local host.

  (for example - /dev/rmt/0h)
- **-r** - Remote-tape-drive. Specifies a tape drive on a remote host.

  (for example - sparky: /dev/rmt/0h or 192.168.1.10: /dev/rmt/0h)
- **-c** - check-database. Checks the integrity of the databases. (Does not fix if errors are found.)
- **-v** - verbose. Verbose output.
- **-p** - physical-restore. Performs only a physical restoration of the database and does not restore the logical logs.
- **-i** - interactive. Runs the restoration in interactive mode.
- **-h** - help. Provides a brief description of the valid options.

Restoring the DTACS Database

Complete the following steps to restore the DTACS databases.

Note: You need the tape from your most recent database backup in order to restore the DTACS database.

Important: Be sure your tape is write-protected before you use it to restore the database.

1. As **dtacs** user (sux - dtacs), type **dtacsStop** and press **Enter**. The DTACS processes are stopped.
2. If necessary, open an xterm window on the DNCS.
3. As root user, type **. /dvs/dtacs/bin/dtacsSetup** and press **Enter**. The system established the root user environment.

   Important: Be sure to type the dot, followed by a space, prior to typing /dvs.
4. Insert the DTACS Maintenance DVD into the DVD drive of the DTACS server.
5. Type **/export/home/informix/bin/formatDbSpace.sh** and press **Enter** to format the database partitions.

Note: Contact Cisco support if you see any errors or failures in formatting the database partitions.

6 Insert your most recent copy of the DTACS database backup tape into the tape drive of the DTACS and wait for the green light on the tape drive to stop flashing.

7 Type **/cdrom/cdrom0/s3/backup_restore/restoreDatabase -v** and press **Enter**. The **Is there more than 1 tape in this backup? [Y/N]** message appears.

8 Type **n** and press **Enter**. The system displays a message about ensuring that the backup tape is in the drive.

9 Press **Enter**. The system restores the database.

10 When the **Successfully restored the database message** appears, remove the tape and store it in a safe place.

11 Did you restore the database on the DTACS server?

- If **yes**, return to step 7 in ***Restoring the DTACS File System*** (on page 168).
- If **no**, contact Cisco support for further assistance.

D

DTACS Rollback Procedure

The DTACS rollback procedures are intended for field service engineers who encounter problems while upgrading an existing DTACS system. Prior to executing the DTACS rollback procedures, contact Cisco Services at 1-866-787-3866.

In This Appendix

Which Rollback Procedure Should I Use?

Three rollback procedures exist for rolling back the DTACS upgrade. Read the following choices to help you decide which rollback procedure to use.

- If you need to roll back a major upgrade, and you *have not* already run the procedure under ***Attach Mirrors After a DVD Live Upgrade*** (on page 79), then use the procedure under ***Activate the Old System Release*** (on page 175) to roll back.

  Note: It should take you about 10 minutes to roll back the T5220 or T5440 DTACS server using this procedure.

- If you need to roll back a major upgrade, and you *have* already run the procedure under ***Attach Mirrors After a DVD Live Upgrade*** (on page 79), then use the procedures to restore the DTACS file system and database in Backup and Restore the DTACS File System and Database.

  Note: It may take as long an hour to roll back the T5220 or T5440 DTACS server.

- If you need to roll back a package install, then use the procedures in ***Roll Back a CD Install*** (on page 176).

Activate the Old System Release

Restoring the Old System Release

Follow this procedure to restore the system software that was in place prior to the unsuccessful upgrade to DTACS.

1. Write down the version of the system release are you trying to restore:

   ____

2. If necessary, as dtacs user (sux - dtacs), type **dtacsStop** and press **Enter** to stop DTACS processes.
3. As root user, type **eeprom boot-device=disk:a** and press **Enter**. The system resets the default boot device to the original disk.
4. Type **shutdown -y -g0 -i6** and press **Enter**. The system reboots and activates the old software.

   Important: Do not use the reboot or halt command to reboot the server.

5. Did the DTACS server reboot without error?
   - If **yes**, go to step 6.
   - If **no**, contact Cisco Services.
6. Log on to the CDE of the DTACS server as admin user.
7. As dtacs user, type **dtacsStart** and press **Enter**. The DTACS processes are started.
8. Change to root user.
9. Type **/cdrom/cdrom/s3/sai/scripts/attach_mirrors** and press **Enter**. The mirrors begin to attach.

Roll Back a CD Install

1. Insert the d1.1.0.4 DVD and log in as a root user.
2. Type **cdrom/cdrom0/s3/backup_restore/make_d700_bootable** and press **Enter**.
3. When the system prompts you to reboot, type **y** and press **Enter**.
4. Log in as a root user.
5. Type **/cdrom/cdrom0/s3/backup_restore/make_d500_bootable** and press **Enter**.
6. When the system prompts you to reboot, type **y** and press **Enter**.
7. Log in again.
8. Type **pkginfo -l SAIdtacs** to verify you are back to the original DTACS version.
9. Type **dtacsStart** and press **Enter** to restart the DTACS processes.
10. Monitor DTACS to make sure that it is up are running normally. Then, do the following to sync the mirrors:
    - **a** Remove the d.1.2.0.1 CD and re-insert the d1.1.0.4 maintenance DVD.
    - **b** Type **/cdrom/cdrom0/backup_restore/mirrState -a** and press **Enter** to sync the mirrors.

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

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

Product and service availability are subject to change without notice.

September 2012 Printed in United States of America Part Number 78-4036705-01 Rev D