CommWorks
a 3Com company

Total Control® 1000 Enhanced Data System

Maintenance Guide
Release 4.5
Part Number 10048391

CommWorks
a 3Com company

Total Control® 1000 Enhanced Data System

Maintenance Guide
Release 4.5
Part Number 10048391

CONTENTS

INDEX

LIST OF TABLES

LIST OF FIGURES

About This Guide

About This Guide includes an overview of this guide, lists guide conventions, related documentation, and product compatibility, and provides contacting CommWorks information.

This guide describes how to maintain and troubleshoot the various components of the CommWorks Total Control® 1000 Enhanced Data System.

This guide is intended for network administrators or engineers who install and configure the Total Control 1000 Enhanced Data System for use with their applications.

Release notes are issued with some products—visit our website at http://totalservice.commworks.com. If the information in the release notes differs from the information in this guide, follow the instructions in the release notes.

Conventions

Table 1 lists notice icons used in this guide.

Table 1 Notice Icon Descriptions

Icon	Notice Type	Description
	Information Note	Information that contains important features or instructions.
	Caution	Information to alert you to potential damage to a program, system, or device.
	Warning	Information to alert you to potential personal injury or fatality. May also alert you to potential electrical hazard.
	ESD	Information to alert you to take proper grounding precautions before handling a product.

Table 2 lists text conventions in this guide.

Table 2 Text Convention Descriptions

Convention	Description
Text represented as a `screen display`	`This typeface` represents displays that appear on your terminal screen, for example: Netlogin:
Text represented as **menu** or **sub-menu names**.	**This typeface** represents all menu and sub-menu names within procedures, for example: On the **File** menu, click **New**.
Text represented by <filename>	This typeface represents a variable. For example: <filename>.

Screen Captures

The screens in this guide may not represent what you see on your monitor; use them only as guidelines.

Related Documentation

The following documents contain additional information about CommWorks Total Control® 1000 components, operations, systems, and procedures that may be referenced in this manual:

Total Control 1000 Enhanced Data System

The following documents relate to the CommWorks Total Control® 1000 Enhanced Data System:

- Total Control 1000 Enhanced Data System *System Overview Guide* - Part Number 10048404
- Total Control 1000 Enhanced Data System *Getting Started Guide* - Part Number 10048403
- Total Control 1000 Enhanced Data System *Operations Guide* - Part Number 10048402
- Total Control 1000 Enhanced Data System *Maintenance Guide* - Part Number 10048391
- Total Control 1000 Enhanced Data System *Trouble Locating and Clearing Guide* - Part Number 10048400
- Total Control 1000 Enhanced Data System *Modem and Span Command Line Reference* - Part Number 10048399
- Total Control 1000 Enhanced Data System *Access Router Card 5.5 Command Line Reference* - Part Number 10048398
- Total Control Manager for Windows and UNIX *Getting Started Guide* - Part Number 10045614
- CommWorks 5115 Common Element Manager *User's Guide* - Part Number 10047652
- CommWorks 5115 Common Element Manager for Total Control 1000 *User Guide* - Part Number 10048397

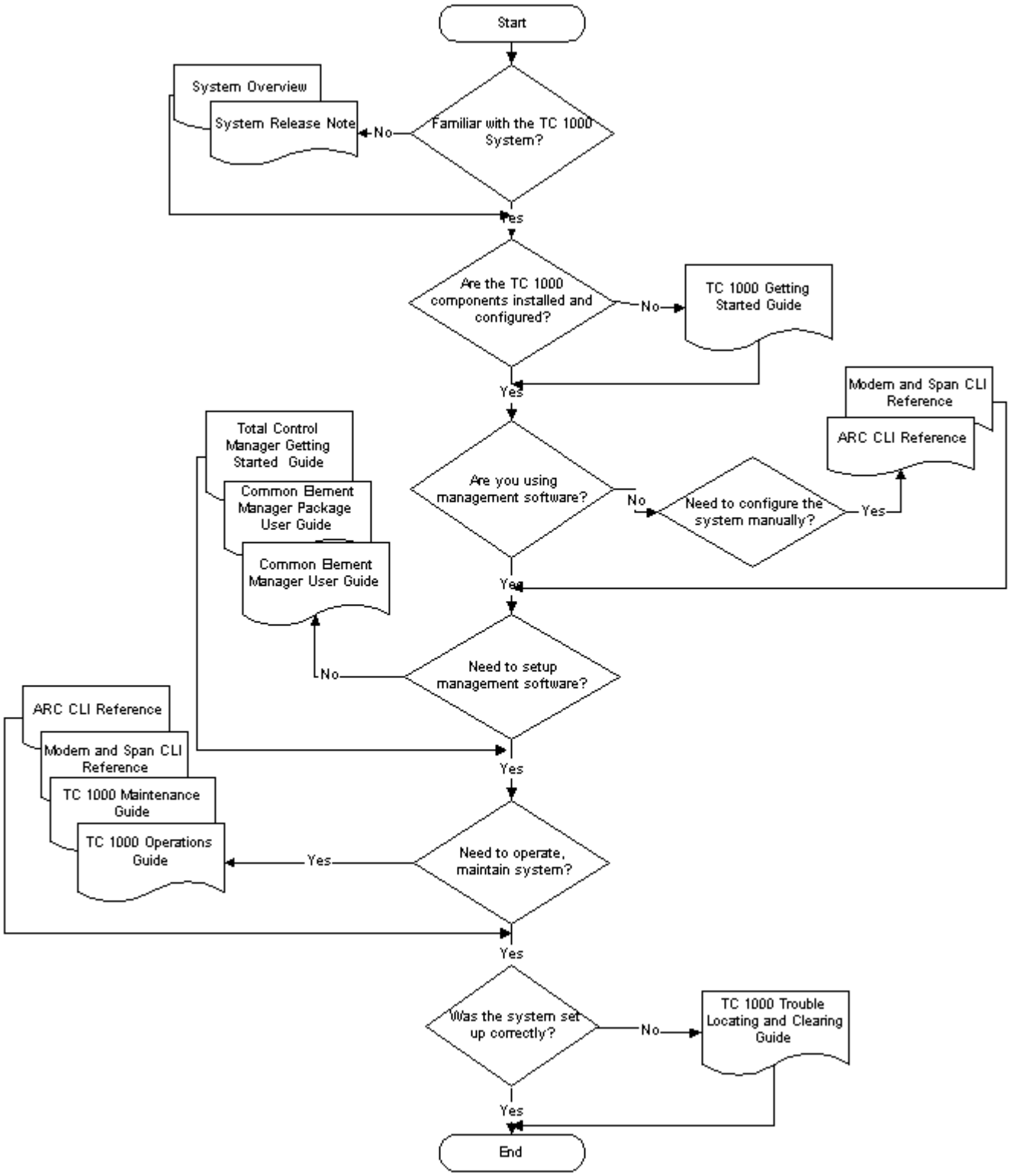
Total Control HiPer System

Some documents from the Total Control MultiService Access Platform (the HiPer system) also relate to the Total Control 1000 Enhanced Data System.

- HiPer ARC Network Application Card *Getting Started Guide* - Part Number 10031739
- PCI Dual 10/100Base-T Ethernet Network Interface Card *Getting Started Guide* - Part Number 1.024.1330-02
- PCI Dual V.35 10/100 Ethernet PCI Network Interface Card *Getting Started Guide* - Part Number 1.024.1959-01
- Quad T1/E1 10/100 Ethernet PCI Network Interface Card *Getting Started Guide* - Part Number 1.024.1973-00
- Dual DS3 Asynchronous Transfer Mode Network Interface Card *Getting Started Guide* - Part Number 10030485
- Dual E3 Asynchronous Transfer Mode Network Interface Card *Getting Started Guide* - Part Number 10031642
- HiPer DSP Network Application Card *Getting Started Guide* - Part Number 10030920
- HiPer DSP T1/E1 Network Interface Card *Getting Started Guide* - Part Number 1.024.1310-02
- HiPer NMC Network Application Card *Getting Started Guide* - Part Number 10030486
- 10/100 Ethernet Aux I/O Network Application Card *Getting Started Guide* - Part Number 1.024.1309-01

Use the following documentation map to help you install and configure your Total Control 1000 system.

Figure 1 Documentation Map



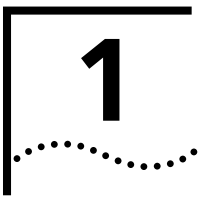
Contacting Customer Service

For information about customer service, including support, training, code releases and updates, contracts, and documentation, visit our website at http://totalservice.commworks.com.

Refer to the Documentation CD-ROM for information about product warranty.

Before contacting technical support, have this information available:

- Contract number
- Problem description
  - Symptoms
  - Known causes
- Product information
  - Software and hardware versions
  - Serial numbers



Downloading Software

This section includes how to download new application software and BIOS code to your CommWorks Total Control® 1000 Enhanced Data Systems components. This chapter includes:

Overview

Software Download-2 (SDL-2) is a utility to download software to a Network Application Card (NAC) in a Total Control 1000 chassis locally through the console port or remotely across a Local Area Network (LAN) or Wide Area Network (WAN).

Only use SDL-2 when downloading to NACs. All other software downloads use SDL-1 (PCSDL).

Figure 2 shows the SDL process.

Figure 2 Software Download-2 Process Overview

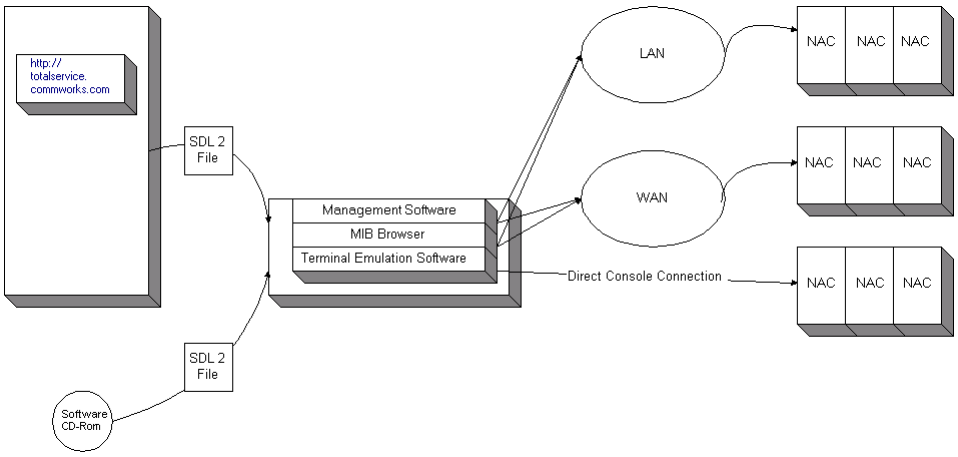


Table 3 displays the methods you can use to complete an SDL-2.

Table 3 SDL-2 Download Options

SDL-2 Method	Use
SNMP or common element manager	Download across a LAN or WAN to the network management card using TFTP protocol through a MIB browser or common element manager. The file then transfers automatically to the NAC using SNMP.
Z-Modem download	Console port download using Z-Modem protocol directly from the host PC to the NAC.

When using common element manager, the "Software Download Complete" message indicates the download is complete.

Z-Modem Download

The typical Z-Modem download is a Z-Modem file transfer from the host PC to the target NAC. Use a terminal emulator package that supports Z-Modem. Upon the completion of the Z-Modem transfer, a result message displays regarding the success or failure of the file transfer. Successful transfer does not necessarily mean that the entire process completed successfully, since the device may be done with the file transfer, but it still could encounter an error programming Non-volatile Random Access Memory (NVRAM).

After the NAC is finished processing the download file, it waits about five seconds, and an ASCII result string is sent to the serial port. This string displays on the emulator screen.

If the SDL-2 agent aborts the download operation, the final ASCII result message displays after the five-second delay.

Downloading Software through Common Element Manager

Common element manager can transfer software across a LAN or WAN to a chassis NAC.

Before You Start

Connect the management station to the network management card Network Interface Card (NIC) through a LAN, WAN, or SLIP connection.

You may also need to configure the network management card SLIP port. Refer to the Network Management Card Getting Started Guide *for more information.*

Checking the Software Version

Follow these steps to check the currently-installed version of software:

1. From the common element manager explorer, click the specific card or server component.
2. In the **Identification** tab, verify the **Version**.

Installing Software

To install code for the selected element, use the **Software** command. You can also set the current code version as a baseline so that you can reinstall it. Which code is available is determined by placing software files in the appropriate directory. The software options are as follows:

- Install baseline—downloads and installs the baseline software.
- Install current—downloads and installs the current software.
- Install planned—downloads and installs the planned software. Use planned software during the Upgrading a Card operation.
- Set baseline to current—sets the baseline software to the currently installed version of software.

Before upgrading the software, you may want to set the currently installed software as the baseline. This allows you to revert to the currently installed software if needed. Refer to Setting the Baseline to Current.

Setting the Baseline to Current

To set the currently installed software as the baseline software:

1. From the common element manager explorer, right-click the component you want to set as the software baseline.
2. From the pop-up menu, select **Software**.
3. Select **Set Baseline to Current**.

   A dialog box appears and common element manager sets the current software as the baseline software.
4. Click **Close**.

Upgrading a Component

Follow these steps to upgrade a component.

1. Place code into the 'software_upgrade' directory of your common element manager server.

   For example, <main_dir>/CEM/software_upgrade.

2. From the common element manager explorer, select the component you want to upgrade.
3. From the **Properties** tab, select the **Software** tab.
4. Double-click the **Planned** field and select the appropriate code version from the drop-down menu.
5. Click **Save all**.
6. Right-click the component you want to upgrade.
7. From the pop-up menu, select **Software**.
8. Select **Install planned**.

   A dialog appears and displays the progress of the installation; common element manager marks the component with a lock icon. After the download is complete, the **Working** icon changes to a **Finished** icon.

9. Click **OK**.

When upgrading a card, common element manager reboots the cards; when upgrading a server component, common element manger restarts the service and services related to the component you are upgrading.

Restoring the Baseline

If you set a software version as the baseline (refer to Setting the Baseline to Current), you can revert to that version of software by restoring the baseline.

Follow these steps to restore the baseline software.

1. From the common element manager explorer, right-click the card or server component you want to restore to the baseline software.
2. From the pop-up menu, select **Software**.
3. Select **Install Baseline**.

   A dialog box appears and common element manager installs the baseline software.

4. Click **Close**.

Access Router Card Software Downloads

You can download new code to access router cards by using the *Zmodem* protocol using the Windows terminal emulator *HyperTerminal*. This method requires a direct Console connection and reboots the access router card.

The steps to download new code are:

1. Reboot and wait for the prompt.
2. At the boot prompt, enter AT{Z} and then right click.
3. Click **Send File...** and select **Send File**
4. Specify a name in the **Filename:** field and click **Send**.

- *AT{Z}* command. Issuing the AT{Z} command at the initial boot prompt will also download files but is tricky considering the 5-second timeframe. This method requires a direct Console connection and automatically reboots the access router card.
- *AT{Z[F]}* command. Issuing the AT{Z[F]} command is similar to the AT{Z} command except for the additional function of formatting your FLASH memory. This method requires a direct Console connection and automatically reboots the access router card.

TELNETd Access Port

The Telnetd Access Port identifies the specific TCP port number for incoming Telnet sessions. The default is **23**, Telnet's common port number.

You can change this access port number; the range is 1 to 65535.

Ports 10000 through 10100 are reserved for an internal filter used for host device port security. Use the following command to change the *existing* Telnetd network service:

```
set network service telnetd server_type telnetd socket
<number>
```

Some administrators consider using port 23 for remote administration a security risk since anybody can get a login prompt simply by telnetting to the system. This allows a potential unauthorized user to seize control of the access router card.

Changing to a non-standard port adds protection by making a potential vandal guess which port the system is listening to. Alternatively, you can disable Telnet administration altogether by setting this parameter to ***0*** *or issuing the* ***disable network service telnetd*** *command.*

Discarding and Renaming Files

There are several **delete** commands you can use to discard various files.

- Delete configuration—discards all configuration files, reboots the system and restores system configuration to factory defaults
- Delete file—removes a file from the FLASH file system
- Delete filter—pulls a filter entry from the filter table and discards it from FLASH memory
- Rename file—copies files within the FLASH file system. Use the command:

```
rename file <input_file> <output_file>
```

DSP Multispan Card Software Downloads

Terminal emulation software can download software through the console port.

Unless otherwise specified, all references to the DSP multispan card also apply to the HiPer DSP card.

DSP multispan and DS-3 cards must use the auxiliary port.

Use this SDL-2 procedure when installing code to the NAC through the console port. The SDL-2 utility allows downloading of software to a NAC through a serial link, both locally and remotely.

Before You Begin

Before downloading software:

What You Will Need

To send the new code to the NAC from the console port, requires a standard terminal program that can send files using the Z-Modem protocol.

You also need a computer with a serial port capable of link rates up to 115200 bps, and a null modem cable with RJ-45 and RS-232 on each end.

1. Checking the Software Version:
   - For DSP Multispan, from the console interface, type **`ATI7`** at a modem prompt to display product configuration. For SDH STM-0 and DS-3, from the console interface, type **`version`** at a modem prompt to display product configuration
   - To determine the version of software, view the date and revision of the Boot Block, Board Manager, ACP, and DSP multispan.
2. Preparing to Download Software:
   - Set your terminal program to 115200 bps, 8 bits per character, no parity, one stop bit, and hardware flow control on.

DSP multispan link port speeds are fixed and cannot be changed. Although either port can be used, CommWorks recommends using the Auxiliary port, which has a standard 115200 bps interface, when downloading software.

Performing Z-Modem Software Download-2

To download software:

If power to the NAC is removed during any of these software download steps, restart the procedure.

1. Launch a terminal emulation program supporting the Z-Modem transfer protocol (for example, HyperTerminal).
2. Manually reboot the NAC by unseating and reseating it.
3. When the "Enter Command" prompt appears, type **AT{Z}** in all capital letters. Using your terminal emulation program, select and send the boot file.

Use all capital letters when typing **AT{Z}.** *Begin sending the files before the hardware reboot cycle begins. The hardware reboot cycle begins about 10 seconds after manually rebooting the card.*

This message displays when the download is complete.

```
"0;Download successful: File=file.dmf"Programming flash
"!!-----> SDL2 for the PPC403 <-------!!"
"__ Enter Download Trigger __"
```

Do not input the trigger when prompted the second time unless you want to re-download the code.

The software download is now complete.

Storing Dual Software Images to NVRAM

When ready to switch from an active software image to a second software image through the CLI, follow this set of procedures from the console prompt during initial bootup (<):

1. Enter the following command to download code to the first slot:

   AT{Z1}

2. Enter the following command to download code to the second slot:

   AT{Z2}

3. Enter the following command to make the first slot the boot slot:

   AT{B1}

4. Enter the following command to make the second slot the boot slot:

   AT{B2}

5 Enter the following command to download to and make the first slot the boot slot:

```
AT{ZB1}
```

6 Enter the following command to download to and make the second slot the boot slot:

```
AT{ZB2}
```

Network Management Card Software Downloads

To download software to the network management card using a terminal emulation software package:

If power to the NAC is removed during any of these software download steps, restart the procedure.

1 Launch a terminal emulation program supporting the Z-Modem transfer protocol (for example, HyperTerminal) and set the baud rate to **9600**.

2 Manually reboot the NAC by unseating and reseating it.

3 Wait for **BIOS Extension Link Date.....** message to display.

If this message does not display, increase speed settings to 19200, disconnect and reconnect Hyper Terminal and repeat step 2.

If message does not display again, increase speed to 38400, and next time to 115200. After increasing of speed repeat step 2

4 When BIOS Extension Link Date message displays, type **AT{Z}**.

The network management card responds with the "Begin download now" message.

5 From Hyper Terminal select **Transfer** menu, then **Send File**.

The Send File window appears.

6 Select file to be downloaded and Zmodem protocol. Click **Send** to start download.

After competing download the network management card reboots and runs the new image.

Similar steps may be used with other terminal emulator and Z-modem protocol software. In UNIX environment it may be "tip" (emulator) along with "lsz" (protocol).

7 After completing the upgrade, save the chassis to NVRAM.

Downloading Software Using Common Element Manager

Common element manager can transfer software across a LAN or WAN to a chassis NAC.

Checking the Software Version

To check the currently installed version of software:

1. From the Explorer tab, click the specific card or server component.
2. In the Identification tab, verify the Version.

Installing Software

To install code for the selected element, use the **Software** command. You can also set the current code version as a baseline so that you can reinstall it. Which code is available is determined by placing software files in the appropriate directory. The software options are as follows:

- Install baseline—downloads and installs the baseline software.
- Install current—downloads and installs the current software.
- Install planned—downloads and installs the planned software. Use planned software during the Upgrading a Card operation.
- Set baseline to current—sets the baseline software to the currently installed version of software.

Before you upgrade the software, you may want to set the currently installed software as the baseline. This allows you to revert to the currently installed software if needed. Refer to Setting the Baseline to Current.

Setting the Baseline to Current

To set the currently installed software as the baseline software using common element manager:

1. From the **Explorer** tab, right-click the component whose software you want to set as the baseline.
2. From the pop-up menu, select **Software**.
3. Select **Set Baseline to Current**.

   A dialog box appears and common element manager sets the current software as the baseline software.
4. Click **Close**.

Upgrading a Component

To upgrade a component using common element manager:

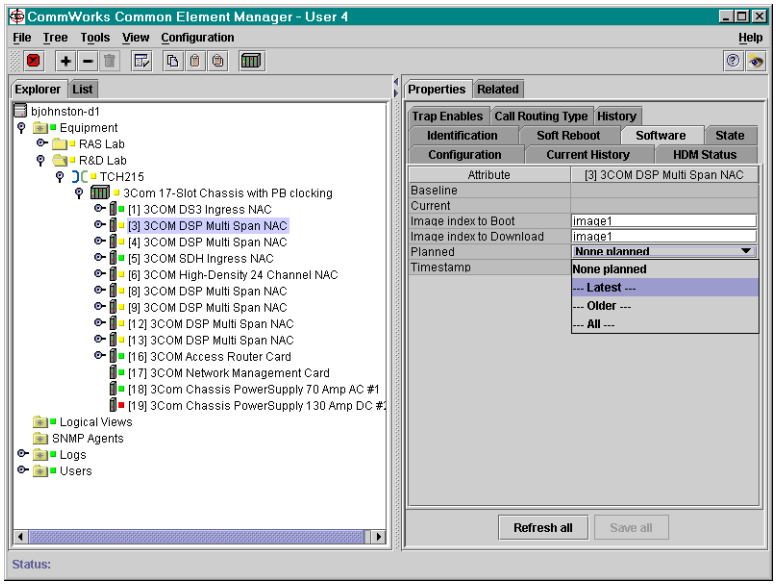
1. Place code into the ‘software_upgrade’ directory of your common element manager server.

   For example, <main_dir>\CEM\software_upgrade.
2. From the **Explorer** tab, click the component you want to upgrade.
3. From the **Properties** tab, click the **Software** tab.

4 Double-click the **Planned** field.

5 From the drop-down menu, select the appropriate code version.

Figure 3 Software Upgrade Drop-down List



6 Click **Save all**.

7 Right-click the component you want to upgrade.

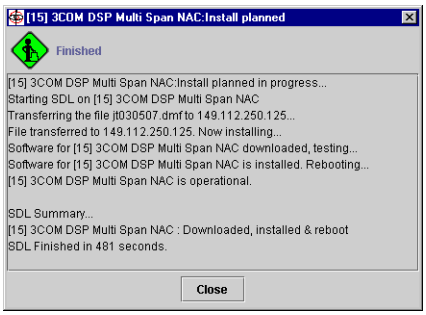
8 From the pop-up menu, select **Software**.

9 Select **Install planned**.

A dialog appears and displays the progress of the installation; common element manager marks the component with a lock icon.

After the download is complete, the **Working** icon changes to a **Finished** icon.

Figure 4 Software Download Completed Window



10 Click **OK**.

11 Right-click the chassis that was just upgraded.

12 Select **Rediscover** from the pop-up menu.

When upgrading a card, common element manager reboots the cards; when upgrading a server component, common element manger restarts the service and services related to the component you are upgrading.

Restoring the Baseline

If you set a software version as the baseline (refer to Setting the Baseline to Current), you can revert to that version of software by restoring the baseline.

To restore the baseline software:

1. From the **Explorer** tab, right-click the card or server component you want to restore to the baseline software.
2. From the pop-up menu, select **Software**.
3. Select **Install Baseline**.

   A dialog box appears and common element manager installs the baseline software.
4. Click **Close**.

Importing SDL Files Using Total Control Manager

Follow these steps to import SDL files using total control manager.

1. On the **Main Menu** bar, click **File**, and then click **Restore NVRAM**.
2. Browse to the directories containing the target file being downloaded and highlight it.
3. Click **OK**.

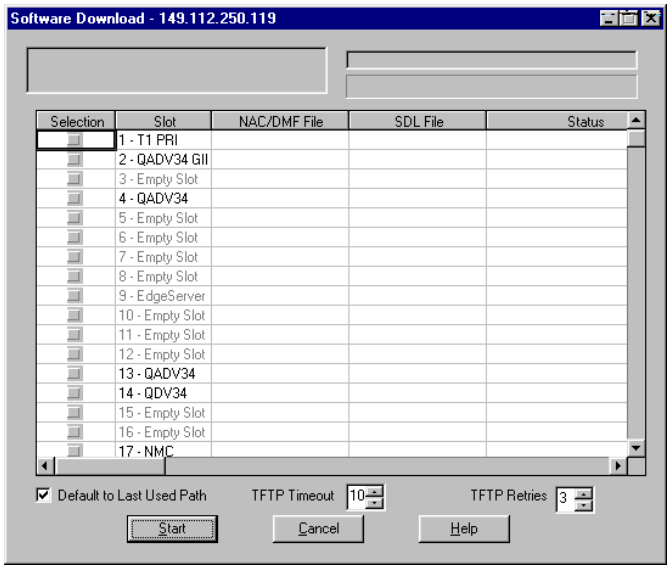
Downloading Software Using Total Control Manager

Follow these steps to download software using total control manager.

1. Select the device or channel to which the action or command will apply.
2. On the **Main menu** bar, click **Configure**, and then click **Software Download**.

The Software Download dialog box displays.

Figure 5 Software Download Dialog Box



3 Double click in the **NAC/DMF File** field next to the device chosen.

4 Browse to the file being downloaded, then click **Open**.

5 Click **Start** on the Software Download dialog box.

For more information on this feature, refer to the *Total Control Manager for Windows and UNIX Getting Started Guide*.

2 SNMP Traps and Alarms

This chapter contains information useful when tracking Simple Network Management (SNMP) traps. Each section provides information about the trap, the condition during which this trap is sent, and a list of possible problem solving steps associated with the trap.

This chapter contains the following topics:

Overview

This topic covers an overview of events, alarms, and traps.

- Event—The network management card Network Application Card (NAC) and all other manageable chassis NACs have an SNMP mechanism for reporting any events on the card to an external Management Station (MS). These event messages are called traps.

  An event is something that happens to the operating status of a chassis device. This event may include a state change, error, or device reset. An event is reported as either an SNMP trap or a RADIUS log record. If you enable an event when you configure the NAC, the event causes the network management card to generate a trap or log record. If you disable an event, it is discarded and not sent to the network management card.
- Alarm—An alarm is the action the MS takes in response to the trap message it receives. Alarms are specific to third-party software packages and customer applications. They may include reports, buzzers, or pages to the network manager.
- Trap—Trap settings are configured and saved on the network management card only. When an event occurs within the chassis, a message is sent to the network management card. Events are checked against a trap enable or disable table kept in the network management card memory. If the trap is enabled within the network management card, an event message is sent to the MS. If logging is enabled, a log message is sent to the logging server. If traps or logging are disabled, the event is discarded.

Four options typically exist when setting traps as listed in Table 4.

Table 4 Commands for Setting Traps

Command	Description
enableTrap (1)	Enabling the trap allows the network management card to send the trap to the MS alarm server.
disableAll (2)	Disabling all prevents the network management card from sending the trap to the MS alarm server and RADIUS logging server.
enableLog (3)	Enabling the log allows the network management card to send the trap to the RADIUS logging server.
enableAll (4)	Enabling all allows the network management card to send the trap to both the MS alarmserver and RADIUS logging server.

Too many traps and logs may cause unacceptable traffic levels on a LAN; perform a traffic analysis to determine the acceptable traffic level.

- Trap Destination Table—Traps are sent to all MS that are registered in the network management card's trap destination table. RADIUS logs use a separate destination table. Use an SNMP MIB browser or common element manager to set the trap destinations.

  By default, the trap destination table contains no entries. Traps and log messages will not be generated until you specify a destination IP address.

- Transient Events—Many events are considered transient in that they may only last for a short period of time before they are cleared. For example, noise on a T1 span may cause a temporary line condition that generates a trap. When the condition improves, it generates a "clear" event.

  Although these traps represent potentially serious conditions, they may clear themselves within a short time. To avoid unnecessary alarms, build a delay mechanism into your alarm server software. When configuring an alarm server, you need to determine the appropriate severity level of these alarms based upon your specific network needs. Use transient events to monitor the condition of your network. Performance monitor packages will accumulate these events as statistics, allowing you to determine the quality of a span line by event frequency.

Total Control 1000 Traps

The traps listed in this section are generated from the Total Control 1000 system.

Table 5 Total Control 1000 Traps

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
1	moduleInserted **Trap enable object:** *uchasModuleInsertedTrapEna*	All except network management card	Module inserted—a card was inserted into an empty slot in the hub. No corrective action needed unless the event is not expected.
2	moduleRemoved **Trap enable object:** *uchasModuleRemovedTrapEna*	All except network management card	Module removed—a card was removed from the hub. No corrective action needed unless the event is not expected.
3	psuWarning **Trap enable object:** *uchasPSUWarningTrapEna*	PSU	PSU warning—the power supply is out of the normal operating range. The network management card detected a PSU that is not responding properly to periodic polls. Check the chassis PSU.
4	psuFailure **Trap enable object:** *uchasPSUFailureTrapEna*	PSU	PSU failure—the power supply has failed. The network management card detected a PSU that is not responding to periodic polls. Check the chassis PSU.
5	tempWarning **Trap enable object:** *uchasTempWarningTrapEna*	Chassis through network management card	Temperature warning—the internal hub temperature is out of the normal operating range. The chassis over-temperature sensor detected a high operating temperature. The chassis is either too hot, the network management card is reading the temperature incorrectly, or the over-temperature sensor failed. The normal operating temperature must be below 41° C (104° F). If the temperature reading stays above 40° C, check the actual site temperature. If the reading is inaccurate, replace the sensor or the network management card.
6	fanFailure **Trap enable object:** *uchasFanFailureTrapEna*	Chassis through network management card	Fan failure—the hub cooling fan failed. The chassis fan sensor detected a non-operational fan, the fan sensor failed, or the network management card misread the sensor. Make sure the fan is functioning. Make sure the fan tray is connected. Check the network management card for a red Hub Status LED. Swap the network management card with a known good network management card, then check to see if problem continues.
7	entityWatchdogTimeout **Trap enable object:** *uchasEntityWatchdogTrapEna*	All except network management card	Entity watchdog timeout—a watchdog timeout was detected. This may be an indication of a software failure. A card in the chassis detected a software failure and rebooted itself. Replace a failed card.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
8	entityMgtBusFailure **Trap enable object:** *uchasEntityMgtBusFailTrapEna*	All except network management card	Entity management bus failure—a chassis NAC (entity) failed to respond to the network management card. Typically, this trap indicates a session between the network management card and a chassis NAC has failed and re-established itself. If you continue to receive this trap, and it is associated with a specific NAC, the NAC may need to be replaced.
9	incomingConnectionEstablished **Trap enable object:** obsolete	Dual modem Quad modem	Incoming connection established—an incoming connection was established on a modem. Obsolete—replaced by trap 54, which provides tracking.
10	outgoingConnectionEstablished **Trap enable object:** obsolete	Dual modem Quad modem	Outgoing connection established—an outgoing connection was established on a modem. Obsolete—replaced by trap 55, which provides tracking.
11	incomingConnectionTerminated **Trap enable object:** obsolete	Dual modem Quad modem HiPer DSP	Incoming connection terminated—an incoming connection was terminated on a modem. Obsolete—replaced by trap 56.
12	outgoingConnectionTerminated **Trap enable object:** obsolete	Dual modem Quad modem HiPer DSP	Outgoing connection terminated—an outgoing connection was terminated on a modem. Obsolete—replaced by trap 57.
13	connectAttemptFailure **Trap enable object:** obsolete	Dual modem Quad modem	Connection attempt failure—a modem in the chassis failed to connect a call with another modem. Obsolete—replaced with traps 86 and 87, which provide directionality.
14	connectTimerExpired **Trap enable object:** *mdmTeConnTimeLimit* *hdmTeConnTimeLimit* (DSP)	Dual modem Quad modem HiPer DSP modem-level trap	Connection timer expired—the modem's connection time limit expired. A connection on a modem has not passed any data for a specified period, so the modem disconnected the call.
15	dteTransmitDataIdle **Trap enable object:** *mdmTeDteXmitDataIdle* *hdmTeDteXmitDataIdle* (DSP)	Dual modem Quad modem HiPer DSP modem-level trap	DTE transmit idle—the modem has not received any packets from the attached DTE for a period longer than its idle time threshold.
16	dtrTrue **Trap enable object:** *mdmTeDtrTrue*	Dual modem Quad modem	DTR true—the attached DTE is asserting the DTR signal in a "true" condition.
17	dtrFalse **Trap enable object:** *mdmTeDtrFalse*	Dual modem Quad modem	DTR false—the attached DTE is asserting the DTR signal in a "false" condition. Check DTE or connected terminal. If using a NETServer, try resetting the corresponding S-port. Try a software reset on the modem. Reboot the modem NAC. Swap the modem to see if the problem follows the card. Replace if needed.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
18	blerCountAtThreshold **Trap enable object:** *mdmTeBlerCountAtThresh* *hdmTeBlerCountAtThresh* (DSP)	Dual modem Quad modem HiPer DSP modem-level trap	BLER count at threshold—the modem has exceeded the maximum number of block errors (BLERs) configured for this call. The threshold is defined in the modem's BLER counter (within the template on a HiPer DSP). Causes include: Line noise Line interference Bad cabling Take these trouble clearing actions: Reset the threshold value in the modem's BLER counter. Check line status. Check cabling.
19	fallbackCountAtThreshold **Trap enable object:** *mdmTeFallbkCountAtThresh* *hdmTeFallbkCountAtThresh* (DSP)	Dual modem Quad modem HiPer DSP modem-level trap	Fallback counter at threshold—the modem has exceeded the maximum number of fallbacks (retrains) configured for this call. The threshold is defined in the modem's fallback counter (within the template on a HiPer DSP). Causes include: Line noise Line interference Bad cabling Take these trouble clearing actions: Reset the threshold value in the modem's fallback counter. Check line status. Check cabling.
20	noDialTone **Trap enable object:** *mdmTeNoDialTone*	Dual modem Quad modem	No dial tone—the modem did not detect a dial tone on its NIC interface when it went off-hook to dial. Take these trouble clearing actions: Check for dialtone on the line; switch lines if needed. Replace the NIC if needed.
21	noLoopCurrent **Trap enable object:** *mdmTeNoLoopCurrent*	Dual modem Quad modem	No loop current—the modem did not detect loop current on its NIC interface when it went off-hook to dial. Take these trouble clearing actions: Check the line; switch lines if needed. Replace the NIC if needed.
22	yellowAlarm **Trap enable object:** *uds1TrapEnaYellowAlarm* (T1) *usrds1EventYellowAlarm* (DSP)	T1 HiPer DSP span-level span monitor trap	Yellow alarm—a yellow alarm condition exists when the remote end of a DS1 is experiencing an "out of frame" (OOF) condition. The PRI/T1 card does not detect a valid received signal, which may indicate the telco switch is malfunctioning or there is a line problem. Check the line for physical errors (BER). This trap is used with yellowAlarmClear (50).

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
23	redAlarm **Trap enable object:** *uds1TrapEnaRedAlarm* (T1) *usrds1EventRedAlarm* (DSP)	T1 HiPer DSP span-level span monitor trap	Red alarm—the framing pattern was lost on the DS1's receiver. This is also known as an "out of frame" (OOF) condition. The PRI/T1 has lost carrier detect. Check the T1/PRI span configuration. Also check the line quality. This trap is used with redAlarmClear (51).
24	lossOfSignal **Trap enable object:** *uds1TrapEnaLossOfSignal* (T1) *usrds1EventLossOfSignal* (DSP)	T1 HiPer DSP span-level span monitor trap	Loss of signal—the DS1 receiver has received 175 consecutive 0s. The DS1 is unable to recover a receive signal. The PRI/T1 has lost sync with the Telco switch. This may occur after inserting a NIC. Ensure the NIC is seated and configured correctly. This trap is used with lossOfSignalClear (52).
25	alarmIndicationSignal **Trap enable object:** *uds1TrapEnaAlarmIndSignal* (T1) *usrds1EventAlarmIndSignal* (DSP)	T1 HiPer DSP span-level span monitor trap	Alarm indication signal (blue alarm)—the DS1 is receiving an all 1s pattern. This is an indication that the remote end has lost its receive signal. The PRI/T1 card received an indication that the Telco switch is receiving alarms from a higher-order device. This condition may indicate that a T3 or higher transmission facility is in an alarm state. This trap is used with alarmIndicationSignalClear (53).
26	transmitTimingSourceSwitch **Trap enable object:** *dt1TrapEnaTxTmgSrcSwitch*	T1	Transmit timing source switch—the specified dual T1 card has switched to an alternate timing source. The primary timing source is slaved to the first PRI/T1. Take these trouble clearing actions: Check the out-of-band management for the PRI/T1 card. Look for alarm conditions on either T1. Contact the Telco if needed. If you do not find alarms, set the primary timing source back to span 1. If span 1 will not provide timing, have the Telco check the timing pair on the T1. If you still cannot get span 1 to provide timing, you may need to replace the card.
27	modemResetByDte **Trap enable object:** *mdmTeResetByDTE*	Dual modem Quad modem HiPer DSP	Modem reset by DTE—the modem received a reset command from the DTE. **HiPer DSP –** Modem reset by the console.
28	modemRingNoAnswer **Trap enable object:** *anicCfgMdmRingNATrapEna*	Dual modem Quad modem	Modem ring no answer—the modem failed to answer a call. This trap is generated if the DTR is present and the S0 register on the NAC is not equal to zero. This trap applies to analog only. Check the S0 register value.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
29	dteRingNoAnswer **Trap enable object:** *mdmTeDteRingNoAnswer* *anicCfgDteRingNATrapEna* (analog)	Dual modem Quad modem HiPer DSP modem-level trap	**Dual and Quad modems –** The DTE is not responding to the modem, even though the modem answered the call. This trap is generated when the DTR is not present and the S0 register on the NAC is not equal to zero. Typically, the port on the gateway card is inactive. This trap is sent when the modem receives notice of a call but fails to answer because was not directed by the DTE to answer the call. This is considered a "lost call". When the modem is first notified of a call, it sets a 60-second timer. If the modem does not train within 60 seconds, it will send the trap. If another call arrives on that modem, the trap is sent for the first call. On heavily used hubs, an occasional "lost call" may occur and send this trap. If the threshold or pattern of *dteRingNoAnswer* traps is high, this may signal a problem with the modem. **HiPer DSP –** A packet bus session could not be established with a gateway card, the call clears before it is answered by a gateway card, or the gateway card times out before answering the call.
30	pktBusSessActive **Trap enable object:** *pbTrapEnaSessActive* (gateway) *hdmTePbActive* (DSP)	HiPer DSP NETServer X.25 EdgeServer	Packet bus session active—the DTE/gateway NAC established a session with the modem. This trap is normal after a card is reset or after a power cycle.
31	pktBusSessCongestion **Trap enable object:** *pbTrapEnaPktBusCongest*	NETServer X.25 EdgeServer	Packet bus session congestion—a session between the modem and the DTE/gateway NAC encountered congestion on the packet bus.
32	pktBusSessLost **Trap enable object:** *pbTrapEnaPktBusSessLost* (gateway) *hdmTePbLost* (DSP)	HiPer DSP NETServer X.25 EdgeServer	Packet bus session lost—a session between the modem and the DTE/gateway NAC was disconnected.
33	pktBusSessInactive **Trap enable object:** *pbTrapEnaSessionInactive*	NETServer X.25 EdgeServer	Packet bus session inactive—a session between the modem and the DTE/gateway NAC has become inactive.
34	nacUserInterfaceReset **Trap enable object:** *ipgwTrapEnUiReset* *x25gwTrapEnaUiReset* (X.25)	NETServer HiPer ARC T1 X.25	NAC user interface reset—the NAC was reset from the user interface. This trap is generated by non-modem NACs to indicate that an out-of-band connection reset the NAC.
35	gwWanPortOutOfService **Trap enable object:** x25wanTrapEnaOutOfSvc	X.25	GW WAN port out of service—a gateway WAN port has changed from Link Active to Out of Service.
36	gwWanPortLinkActive **Trap enable object:** x25wanTrapEnaLinkActive	X.25	GW WAN port link active—a gateway WAN port has changed from Out of Service to Link Active.
37	dialOutLoginFail **Trap enable object:** *nmcTeDialOutLogFail*	network management card Dual modem Quad modem	Dial out login failure—a dialout login security session failed and the call was not placed. This informational trap is for network management card-based security for Dual and Quad modems.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
38	dialInLoginFail **Trap enable object:** *nmcTeDialInLoginFail*	network management card Dual modem Quad modem	Dial in login failure—A dialin login security session failed and the call was not placed. This informational trap is for network management card-based security for Dual and Quad modems.
39	dialOutRestrictedNum **Trap enable object:** *nmcTeDialOutRestrictNum*	network management card Dual modem Quad modem	Dial out restricted phone number—a dialout security session failed as a result of attempting to dial a restricted phone number. This informational trap is for network management card-based security for Dual and Quad modems. Check the number and retry.
40	dialBackRestrictedNum **Trap enable object:** *nmcTeDialBackRestrictNum*	network management card Dual modem Quad modem	Dial back restricted number—a dialback security session failed as a result of attempting to dial a restricted number. This informational trap is for network management card-based security for Dual and Quad modems. Check the number and retry.
41	userBlacklisted **Trap enable object:** *nmcTeUserBlacklist*	network management card Dual modem Quad modem	User blacklisted—a security user reached their final failed login attempt number and is now blacklisted. This trap is for network management card-based security for Dual and Quad modems. Check the password and reset the user if required.
42	loginAttemptByBlacklistedUser **Trap enable object:** *nmcTeUserBlacklistLogin*	network management card Dual modem Quad modem	Attempted login blacklisted—a currently blacklisted security user attempted to login. This trap is for network management card-based security for Dual and Quad modems. This may be considered a warning condition; you may wish to monitor for a potential security problem.
43	responseAttemptLimExceeded **Trap enable object:** *nmcTeRespAttemptLimExceeded*	network management card Dual modem Quad modem	Response attempt limit exceeded—a security user failed to issue a valid response to a particular security prompt before the configured limit. This trap is for network management card-based security for Dual and Quad modems.
44	mdmLoginAttemptLimExceeded **Trap enable object:** *nmcTeLoginAttemptLimExceed*	network management card Dual modem Quad modem	Login attempt limit exceeded—a user does not appear in the security user database. This trap is for network management card-based security for Dual and Quad modems. Add the user to the security user database.
45	dialOutCallDuration **Trap enable object:** *mdmTeDialOutCallDur*	Dual modem Quad modem	Dial out call duration—a dial-out call ended. This trap is sent to inform the accounting server of the duration of a dial-out call.
46	dialInCallDuration **Trap enable object:** *mdmTeDialInCallDur*	Dual modem Quad modem	Dial in call duration—a dial-in call ended. This trap is sent to inform the accounting server of the duration of a dial-in call.
47	pktBusSessError **Trap enable object:** *pbTrapEnaSessionError*	NETServer X.25	Packet bus session error status—a session between a modem and the DTE/gateway NAC is giving errors. A modem card or the gateway card may need to be replaced.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
48	nmcArCustomTrap Trap enable object:	network management card	Network management card autoresponse trap—an network management card SNMP autoresponse trap was sent. An event in the chassis triggered an autoresponse event. This is a custom trap. The meaning of this trap depends upon how your system administrator has defined it.
49	acctSrvrLoss **Trap enable object:** *nmcTeLogSrvrLoss*	network management card	Accounting server contact lost—the network management card lost its connection to the accounting server. Check the server security failure code returned with the trap for additional information. The network management card has eight RADIUS accounting servers, including a primary server and a set of secondary servers. The network management card polls the RADIUS server to update server status. When this trap occurs, there was no response from the RADIUS server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down. Take the following trouble clearing actions: Check the network connections. Ensure the server is active. Check the server configuration. Restart the server. Check the communication link.
50	yellowAlarmClear **Trap enable object:** *uds1TrapEnaYellowAlarmClr* (T1) *usrds1EventYellowAlarmClr* (DSP)	T1 HiPer DSP span-level span monitor trap	Yellow alarm clear—the PRI/T1 card received a yellow alarm cleared indication from the Telco switch. This informs you that the previous yellowAlarm trap is cleared.
51	redALarmClear **Trap enable object:** *uds1TrapEnaRedAlarmClr* (T1) *usrds1EventRedAlarmClr* (DSP)	T1 HiPer DSP span-level span monitor trap	Red alarm clear—the PRI/T1 card received a red alarm cleared indication from the Telco switch.This informs you that the previous redAlarm trap is cleared.
52	lossOfSignalClear **Trap enable object:** *uds1TrapEnaLossOfSgnlClr*(T1) *usrds1EventLossOfSgnlClr* (DSP)	T1 HiPer DSP span-level span monitor trap	Loss of signal clear—the PRI/T1 card received a loss of signal alarm cleared indication from the Telco switch. This informs you that the previous lossOfSignal trap is cleared.
53	alarmIndicationSignalClear **Trap enable object:** *uds1TrapEnaAlrmIndSgnlClr* (T1) *usrds1EventAlrmIndSgnlClr* (DSP)	T1 HiPer DSP span-level span monitor trap	Received alarm indication signal clear—the PRI/T1 card received a blue alarm cleared indication m the Telco switch. This informs you that the previous alarmIndicationSignal trap is cleared.
54	ctIncomingConnectionEstablished **Trap enable object:** *mdmTeInConnEstablished* *hdmTeInConnEstablished* (DSP)	Quad modem HiPer DSP modem-level trap	Incoming connection established—a modem successfully established an incoming call and sent a call reference number. This trap replaced incomingConnectionEstablished (9).

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
55	ctOutgoingConnectionEstablished **Trap enable object:** *mdmTeOutConnEstablished* *HdmTeOutConnEstablished* (DSP)	Quad modem HiPer DSP modem-level trap	Outgoing connection established—a modem successfully established an outgoing call. This trap replaced outgoingConnectionEstablished (10).
56	ctIncomingConnectionTerminated **Trap enable object:** *mdmTeInConnTerminated* *hdmTeInConnTerminated* (DSP)	Quad modem HiPer DSP modem-level trap	Incoming connection terminated—a modem successfully ended an incoming call. This trap replaced incomingConnectionTerminated (11).
57	ctOutgoingConnectionTerminated **Trap enable object:** *mdmTeOutConnTerminated* *hdmTeOutConnTerminated* (DSP)	Quad modem HiPer DSP modem-level trap	Outgoing connection terminated—a modem successfully ended an outgoing call. This trap replaced outgoingConnectionTerminated (12).
58	ctConnectAttemptFailure **Trap enable object:** obsolete	Quad modem	Connection attempt failure—a modem was unable to successfully establish a call. Obsolete—replaced with traps 86 and 87, which provide directionality. Note: This trap is sometimes still seen with combinations of old versions of network management card/Quad modem software.
59	contCrcAlarm **Trap enable object:** *uds1TrapEnaContCrcAlrm* (T1) *usrds1EventContCrcAlrm* (DSP)	T1 HiPer DSP span-level span monitor trap	Continuous CRC alarm—a continuous CRC error condition occurred on the DS1. The PRI/T1 is receiving a continuous stream of CRC errors from the T1 span.
60	contCrcAlarmClear **Trap enable object:** *uds1TrapEnaContCrcAlrmClr* (T1) *usrds1EventContCrcAlrmClr* (DSP)	T1 HiPer DSP span-level span monitor trap	Continuous CRC alarm cleared—a continuous CRC error condition cleared from the DS1.
61	phyStateChng **Trap enable object:** *uds1TrapEnaPhysStateChng* (T1) *usrds1EventPhysStateChng* (DSP)	T1 HiPer DSP span-level span monitor trap	Physical state change—a physical state change occurred on the DS1. A PRI/T1 connected to the chassis changed physical state. Check out-of-band for both spans to determine if either span is in an alarm condition. Contact the Telco if needed.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
62	securityServerLoss **Trap enable object:** *nmcTeSecSrvrLoss*	network management card	Security server loss—the network management card is unable to contact the security server. The network management card has eight security servers. There is a primary server and a set of secondary servers. The network management card polls the server to update server status. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down. Take the following trouble clearing actions: Check the network connections. Ensure the server is active. Check the server configuration. Restart the server.
63	singlePktBusClockFailure **Trap enable object:** *nmcTeSinglePbClockFailure*	network management card	Single packet bus clock failure—a backplane packet bus clock failed in a single NAC slot. Check the network management card for a red Hub Status LED. Swap the network management card with a known good network management card, then check to see if problem continues.
64	pktBusClockSwitch **Trap enable object:** *pktBusClockSwitch*	network management card	Packet bus clock switch—a backplane packet bus clock failed in multiple NAC slots. The network management card assumed the role of clock master. Check the network management card for a red Hub Status LED. Swap the network management card with a known good network management card, then check to see if problem continues.
65	pktBusClockFailure **Trap enable object:** *pktBusClockFailure*	network management card	Packet bus clock failure.
66	gwNetworkFailed **Trap enable object:** *gwTeArNetFailed* *gwTegwNetworkFailed* (ISDN)	NETServer HiPer ARC	Gateway network failed—the gateway network failed because authentication and accounting failed. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down. The DTE/gateway NAC lost communication with all RADIUS servers: Check the RADIUS server. Check the cable from the DTE to the server. Check the NETServer or HiPer ARC card.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
67	gwNetworkRestored **Trap enable object:** *gwTeArNetRestored* *gwTegwNetworkRestored* (ISDN)	NETServer HiPer ARC	Gateway network restored—the gateway network is restored. This trap indicates gwNetworkFailed (66) cleared.
68	pktBusClkLost **Trap enable object:** *pbdgCfgClockLossEvent*	all except network management card	Packet bus clock lost—the network management card determined that the packet bus clocking source failed, either for a single NAC or for the entire chassis. Identify which slot(s) failed. Swap the NAC with a known good NAC. This condition may clear itself. Do not replace the NAC in question until this trap occurs multiple times. If the problem is related to slot 17, the network management card is providing timing for the backplane. Contact CommWorks tech support.
69	pktBusClkRestore **Trap enable object:** *pbdgCfgClockRestoreEvent*	all except network management card	Packet bus clock restored—the condition causing the Packet bus clock lost trap is cleared. This trap indicates pktBusClkLost(68) cleared.
70	dChanInService **Trap enable object:** *uds1TrapEnaDchanInSrvc* (T1/PRI) *usrds1EventDchanInSrvc* (DSP)	T1/PRI HiPer DSP span-level call control trap	D-Channel in service—the condition causing a D-Channel out of service trap is cleared. This trap indicates dChanOutOfService(71) cleared.
71	dChanOutOfService **Trap enable object:** *uds1TrapEnaDchanOutOfSrvc* (T1/PRI) *usrds1DchanOutOfSrvc* (DSP)	T1/PRI HiPer DSP span-level call control trap	D-Channel out of service—the D-Channel is out of service. The PRI/T1 card has lost D-Channel signalling on one or both spans. Call the Telco if needed.
72	ds0sInService **Trap enable object:** *uds1TrapEnaDs0InSrvc* (T1/PRI) *usrds1EventDs0InSrvc* (DSP)	T1/PRI HiPer DSP span-level call control trap	DS0s in service—the condition causing a DS0 out of service trap is cleared. This trap indicates ds0sOutOfService(73) cleared. This is the only time this trap generates. This trap may be sent when the chassis reboots after a power cycle. This trap will only occur following ds0sOutOfService(73).
73	ds0sOutOfService **Trap enable object:** *uds1TrapEnaDs0OutOfSrvc* (T1/PRI) *usrds1EventDs0OutOfSrvc* (DSP)	T1/PRI HiPer DSP span-level call control trap	DS0s out of service—this trap provides a list of the DS0s going out of service. The NAC received an indication that one or more DS0s are in an out of service condition. Use out-of-band checking to see if any DS0s are busied-out. Unbusy them if they are out of service. Call the Telco if they are out of service or MaintBusy.
74	callEvent **Trap enable object:** obsolete	T1 (obsolete)	Call event—T1, T1-E1/PRI call event. Obsolete—replaced by traps 76-7
75	psuIncompatible **Trap enable object:** *uchasPsuIncompatible*	network management card	PSU incompatible—the power supply is incompatible with the chassis. Use a compatible power supply. Power supply outputs must match each other (for example, you cannot mix a 45 amp and a 70 amp PSU in the same chassis).

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
76	callArriveEvent **Trap enable object:** *dt1TrapEnaCallArriveEvent* (T1/PRI) *usrds1EventCallArrive* (DSP)	T1/PRI HiPer DSP	Call arrive event—T1, T1-E1/PRI call arrive event. This trap is the first indication of a new call on the T1 span.
77	callConnectEvent **Trap enable object:** obsolete	T1/PRI	Call connect event—T1, T1-E1/PRI call connect event. This trap is sent when the call is connected to a modem.
78	callTermNormalEvent **Trap enable object:** *dt1TrapEnaCallTermEvent* (T1/PRI) *usrds1EventCallTerm* (DSP)	T1/PRI HiPer DSP	Call termination normal event—T1, T1-E1/PRI normal call termination event. This trap is sent when the call terminates normally at the DS0 level.
79	callTermFailedEvent **Trap enable object:** obsolete	T1/PRI	Obsolete. Call termination failed event—T1, T1-E1/PRI call termination (fail) event. This trap is sent when a call arrives in the chassis but fails to be delivered to a modem. This may be caused by a modem that may be in a failed operational state. Also look for a modem that does not seem to be taking calls.
80	dnsSrvrLoss **Trap enable object:** *nmcTeDnsSrvrLoss*	network management card	DNS server loss—unable to contact the primary DNS server. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The DNS server is too busy to respond. The DNS server is down. Take the following trouble clearing actions: Check the network connections. Ensure the DNS server is active. Check the DNS server configuration. Restart the DNS server. Check the communication link.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
81	ntpSrvrLossConn **Trap enable object:** *nmcTeNtpSrvrLoss*	network management card	NTP server lost connection—unable to contact the primary NTP server. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The NTP server is too busy to respond. The NTP server is down. Take the following trouble clearing actions: Check the network connections. Ensure the NTP server is active. Check the NTP server configuration. Restart the NTP server.
82	ntpSrvrRestConn **Trap enable object:** *nmcTeNtpSrvrRestore*	network management card	NTP server restored connection—the connection to the NTP server is restored.
83	ipgwLinkUp Trap enable object:	NETServer HiPer ARC	IPGW link up—the IP gateway link is up.
84	ipgwlinkDown **Trap enable object:**	NETServer HiPer ARC	IPGW link down—the IP gateway link is down. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down.
85	ntpSrvrDegrConn **Trap enable object:** nmcTeNtpSrvrDegraded	network management card	NTP server primary contact lost—unable to contact the primary NTP server.
86	inconnectAttemptFailure **Trap enable object:** *mdmTeInConnAttemptFail*	Hiper DSP modem-level trap	In connection attempt failure—the inbound call failed to connect with a modem. The DS0 may be busy or out of service. The modem training sequence may have failed. Refer to the modem disconnect and fail to connect reasons.
87	outconnectAttemptFailure **Trap enable object:** *mdmTeOutConnAttemptFail*	HiPer DSP modem-level trap	Out connection attempt failure—the outbound call failed to connect with a modem. The DS0 may be busy or out of service. Refer to the modem disconnect and fail to connect reasons.
88	applicationProcessorReset **Trap enable object:**	HiPer DSP	Not used.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
89	dspReset **Trap enable object:**	HiPer DSP	Not used.
90	changedtoMainSrvsStat **Trap enable object:**	HiPer DSP span-level call control trap	The Telco placed the span into a maintenance server state (out of service). This reason will only occur with some telco switches.
91	loopbackcleared **Trap enable object:** *usrds1EventloopBackCleard*	HiPer DSP span-level span monitor trap	Loopback has cleared—the loopback condition on the span line cleared.
92	loopbacktrap **Trap enable object:** *usrds1EventloopBack*	HiPer DSP span-level span monitor trap	Loopback has occurred—a loopback has occurred on the span line.
93	telcoAbnormalResp **Trap enable object:** *uds1EvntelcoAbnornalResp*	HiPer DSP span-level call control trap	Not used.
94	dnsSrvrRestore **Trap enable object:** *nmcTeDnsSrvrRestore*	network management card	DNS primary server restored—contact is restored with the primary DNS server.
95	dnsSrvrDegraded **Trap enable object:** *nmcTeDnsSrvrDegraded*	network management card	DNS secondary server in service—contact was lost with the primary DNS server, but the secondary DNS server is in service.
96	acctSrvrRestore **Trap enable object:** *nmcTeLogSrvrRestore*	network management card	Accounting server contact restored—contact is restored with the RADIUS accounting server.
97	acctSrvrGroupOper **Trap enable object:** *nmcTeLogSrvrGroupOper*	network management card	Accounting server group operational—the RADIUS accounting server group is operational. Contact with the primary RADIUS accounting server is restored.
98	acctSrvrGroupDegr **Trap enable object:** *nmcTeLogSrvrGroupDegr*	network management card	Accounting server group degraded—the RADIUS accounting server group is degraded. Contact with the primary server has been lost. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
99	acctSrvrGroupNonOp **Trap enable object:** *nmcTeLogSrvrGroupNonOp*	network management card	Accounting server group non-operational—the RADIUS accounting server group is non-operational. Contact is lost to all servers. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down.
100	securityServerRestore **Trap enable object:** *nmcTeSecSrvrRestore*	network management card	Security server contact restored—contact is restored with the security server.
101	securitySrvrGrpOper **Trap enable object:** *nmcTeSecSrvrGroupOper*	network management card	Security server group operational—the RADIUS security server group is operational. The primary server is restored. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down.
102	securitySrvrGrpDegr **Trap enable object:** *nmcTeSecSrvrGroupDegr*	network management card	Security server group degraded—the RADIUS security server group is degraded. The primary server is lost, the back-up server is in service. When this trap occurs, there was no response from the server after several polls. This may be caused by: Communication link is down. The network is congested. The server is too busy to respond. The server is down.
103	securitySrvrGrpNonOp **Trap enable object:** *nmcTeSecSrvrGrpNonOp*	network management card	Security server group non-operational—the RADIUS security server group is non-operational. Contact is lost to all servers.
104	uds1MultiFrame **Trap enable object:** *uds1TrapEnaMultiFrame* (T1) *hdr2TeMultiFrame* (DSP)	T1 HiPer DSP span-level call control trap	Multi frame misalignment—multiframe misalignment occurred on a specified DS1. Re-initialize the switch span to attempt to clear the condition. This is an R2 trap.
105	uds1RemoteMultiFrame **Trap enable object:** *uds1TrapEnaRemMultiFrame* (T1) *hdr2TeRemMultiFrame* (DSP)	T1 HiPer DSP span-level call control trap	Remote multi frame misalignment—the remote terminal detected a multiframe misalignment on the specified DS1. Re-initialize the E1/CAS span. This is an R2 trap.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
106	uds1MultiFrameClr **Trap enable object:** *uds1TrapEnaMultiFrmClr* (T1) *hdr2TeMultiFrameClr* (DSP)	T1 HiPer DSP span-level call control trap	Multi frame misalignment cleared—a multiframe misalignment condition cleared on the specified DS1. This is an R2 trap.
107	uds1RemoteMultiFrameClr **Trap enable object:** *uds1TrapEnaRemMultiFrmClr* (T1) *hdr2TeRemMultiFrameClr* (DSP)	T1 HiPer DSP span-level call control trap	Remote multi frame misalignment cleared—the remote terminal detected the multiframe misalignment on the specified DS1 cleared. This is an R2 trap.
108	gwyTdmClockUp **Trap enable object:**	HiPer ARC EdgeServer	Gateway TDM clock up—the gateway card detected the TDM clock is present.
109	gwyTdmClockDown **Trap enable object:**	HiPer ARC EdgeServer	Gateway TDM clock down—the gateway card detected the TDM clock is lost.
110	gwyTdmClockError **Trap enable object:**	HiPer ARC EdgeServer	Gateway TDM clock error—the gateway card detected an error in the TDM clock.
111	cdmaFrSrvViolation	EdgeServer	Not used.
112	cdmaAtViolation	EdgeServer	Not used.
113	cdma42bisViolation	EdgeServer	Not used.
114	usrDs1InCallFailedEvent **Trap enable object:** *usrds1EventDs0InConnFail*	HiPer DSP span-level call control trap	T1-E1/PRI in call failed event—an incoming T1-E1/PRI call failed.
115	usrDs1OutCallFailedEvent **Trap enable object:** *usrds1EventDs0OutConnFail*	HiPer DSP span-level call control trap	T1-E1/PRI out call failed event—an outgoing T1-E1/PRI call failed.
118	callArriveEventHdsp **Trap enable object:** *usrds1EventCallArrive*	HiPer DSP span-level call control trap	This is a normal event. This trap is the first indication of a new incoming call on the HiPer DSP span. This trap is used with callTerminateEventHdsp(119). Together, these traps are useful for matching up span level failures and call accounting. The traps are still generated when the call enters the span, even if a modem did not answer the call.
119	callTerminateEventHdsp **Trap enable object:** *usrds1EventCallTerm*	HiPer DSP span-level call control trap	This is a normal event. This trap occurs when the call terminates normally on the HiPer DSP span. This trap is used with callArriveEventHdsp(118).
120	usrDs1HdspInCallFailedEvent **Trap enable object:** *usrds1EventDs0InConnFail*	HiPer DSP span-level call control trap	An incoming call failed because a modem could not be associated with the call. Make sure the call was not made to an inactive port, a busy DS0, or an out of service DS0.
121	usrDs1HdspOutCallFailedEvent **Trap enable object:** *usrds1EventDs0OutConnFail*	HiPer DSP span-level call control trap	An outgoing call failed. Make sure the call was not made from an inactive port, a busy DS0, or an out of service DS0.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
122	rds1EvDchSwitchOverStart **Trap enable object:** *usrds1EventNfasDchSwStart*	HiPer DSP span-level call control trap	This trap occurs when the primary NFAS D-channel is taken out of service and control starts to switch over to the back-up NFAS D-channel. The switchover can occur because: The span line is down The span line was removed The NAC failed This trap will always be generated with rds1EvDchSwitchOverEnd(123) or rds1EvDchSwitchOverFailure(124).
123	rds1EvDchSwitchOverEnd **Trap enable object:** *usrds1EventNfasDchSwEnd*	HiPer DSP span-level call control trap	This trap occurs when the primary NFAS D-channel has completed the switchover to the back-up NFAS D-channel. This trap will always be generated with rds1EvDchSwitchOverStart(122).
124	rds1EvDchSwitchOverFailure **Trap enable object:** *usrds1EventNfasDchSwfail*	HiPer DSP span-level call control trap	This trap occurs if the primary NFAS D-channel fails to switch to the back-up NFAS D-channel. Failure can occur because: The span line is down The span line was removed The back-up NFAS D-channel is not configured properly (see *usrds1CfgNFASSpanType* and *usrds1CfgSigGroupType)* The NAC failed A telco problem occurred This trap will always be generated with rds1EvDchSwitchOverStart(122).
125	mdm105ResponderTest **Trap enable object:** *mdmTe105ResponderTest*	Quad	Modem 105 responder test—a Modem 105 Responder test occurred in Slot %d, Channel %d.
126 to 165	EdgeServer and CDMA/IWF traps	N/A	Not used.
166 to 177	HiPer TRAX traps	N/A	Not used.
178	AuxIN1Open **Trap enable object:** nmcCmdFunction	network management card	Aux In1 Port Open—the Aux Input Port 1 on the 10/100 Ethernet AUX I/O NIC was put in an open state.
179	AuxIN2Open **Trap enable object:** nmcCmdFunction	network management card	Aux In2 Port Open—the Aux Input Port 2 on the 10/100 Ethernet AUX I/O NIC was put in an open state.
180	AuxIN1Closed **Trap enable object:** nmcCmdFunction	network management card	Aux In1 Port Closed—the Aux Input Port 1 on the 10/100 Ethernet AUX I/O NIC was put in a closed state.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
181	AuxIN2Closed **Trap enable object:** nmcCmdFunction	network management card	Aux In2 Port Closed—the Aux Input Port 2 on the 10/100 Ethernet AUX I/O NIC was put in an open state.
182	AuxOut1Open **Trap enable object:** nmcCmdFunction openAuxOutputPort1(12)	network management card	Aux Output Port1 Open—the Aux Output Port 1 on the 10/100 Ethernet AUX I/O NIC was put in a closed state.
183	AuxOut1Closed **Trap enable object:** nmcCmdFunction closeAuxOutputPort1(14)	network management card	Aux Output Port1 Closed—the Aux Output Port 1 on the 10/100 Ethernet AUX I/O NIC was put in a closed state.
184	AuxOut2Open **Trap enable object:** nmcCmdFunction openAuxOutputPort2(13)	network management card	Aux Output Port2 Open—the Aux Output Port 2 on the 10/100 Ethernet AUX I/O NIC was put in an open state.
185	AuxOut2Closed **Trap enable object:** nmcCmdFunction closeAuxOutputPort2(15)	network management card	Aux Output Port2 Closed—the Aux Output Port 2 on the 10/100 Ethernet AUX I/O NIC was put in a closed state.
186 to 187	CDMA/IWF traps	N/A	Not used.
189	rds1EnterMaintMode usrdf1EventExitMaintMode	HiPer DSP DSP multispan	Exits maintenance mode.
223	HiPerDspDS0EnteredLoopback usrds1EventDs0LpBkEntered	HiPer DSP DSP multispan	This event indicates that a DS0 on the HiPer DSP or DSP multispan entered the loopback state.
224	hiPerDspDS0ClearedLoopback usrds1EventDs0LpBkCleared	HiPer DSP DSP multispan	This event indicates that a DS0 on the HiPer DSP or DSP multispan cleared the loopback state.
225	HiPerDspEnfasSignalingLinkUp (t1hTeEnfasLinkUp, d3iTeEnfasLinkUp)	HiPer DSP DSP multispan DS-3	This event indicates that the ENFAS signaling link on the HiPer DSP or DSP multispan has come up.
226	HiPerDspEnfasSignalingLinkDown (t1hTeEnfasLinkDown, d3iTeEnfasLinkDown)	HiPer DSP DSP multispan DS-3	This event indicates that the ENFAS signaling link on the HiPer DSP or DSP multispan has gone down.
227	Ss7iCommunicationToSS7GatewayLost Ss7iTrapGwConnDown	SS7i	This event indicates that the communication between the SS7i ESIG and the SS7 gateway has been lost.
228	Ss7iCommunicationToSS7GatewayRestored Ss7iTrapGwConnUp	SS7i	This event indicates that the communication between the SS7i ESIG and the SS7 gateway has been restored.
229	Ss7iEnfasConnoHiPerDspLost Ss7iTrapPbusLinkDown	SS7i	This event indicates that the ENFAS connection between the SS7i ESIG and the HiPer DSP has been lost.
230	Ss7iEnfasConnToHiPerDspRestored Ss7iTrapPbusLinkUp	SS7i	This event indicates that the ENFAS connection between the SS7i ESIG and the HiPer DSP has been restored.
295	dspResetAndOutOfService **Trap enable object:** hdmTeDSPResetAndOOS	HiPer DSP DSP multispan	This trap is generated when a DSP has been reset and out of service.

Table 5 Total Control 1000 Traps (continued)

Trap ID	Trap Description/ Trap Enable	Card(s) Affected	Condition/Probable Cause
296	modemReset **Trap enable object:** hdmTeMDMReset	HiPer DSP DSP multispan	This trap is generated when a modem has been reset.
297	modemResetAndOutofService **Trap enable object:** hdmTeMDMResetAndOOS	HiPer DSP DSP multispan	This trap is generated when a modem has been reset and out of service.
334	lineStatusChangeEvent **Trap enable object:** ds3LineStatusChangeTE	DS3	This trap indicates the change of line status of the interface. It can represent a number of state changes such as presence and clearing of different alarm conditions.
337	tdmClockLost **Trap enable object:** d3iTeTdmClockLost	DS3	This trap is generated on the detection of loss of TDM clock.
338	tdmClockRestored **Trap enable object:** d3iTeTdmClockRestored	DS3	This trap is generated upon restoration of the TDM clock.
342	OwnCardStateChangeEvent d3iTeOwnCardStateChange	DS3	This trap is generated by DS3 card to indicate the change of its state.
344	SdhSectionOrder sdhSectionOrderTE	SDH	Detection of Section alarm condition on the specified SDH Converter Card.
345	SdhAU1HighOrder sdhAU1HighOrderTE	SDH	Detection of High Path AU#1 alarm condition on the specified SDH Converter Card.
346	SdhAU2HighOrder sdhAU2HighOrderTE	SDH	Detection of High Path AU#2 alarm condition on the specified SDH Converter Card.
347	SdhAU3HighOrder sdhAU3HighOrderTE	SDH	Detection of High Path AU#3 alarm condition on the specified SDH Converter Card.
348	SdhAU1LowOrder sdhAU1LowOrderTE	SDH	Detection of Low Path AU#1 alarm condition on the specified SDH Converter Card.
349	SdhAU2LowOrder sdhAU2LowOrderTE	SDH	Detection of Low Path AU#2 alarm condition on the specified SDH Converter Card.
350	SdhAU3LowOrder sdhAU3LowOrderTE	SDH	Detection of Low Path AU#3 alarm condition on the specified SDH Converter Card.
351	SdhApsSwitch sdhApsSwitchTE	SDH	Detection of APS switch condition on the specified SDH Converter Card.
352	SdhTransNameChg sdhTransNameChgTE	SDH	Detection of transmission name change condition on the specified SDH Converter Card.
353	SdhApsCableFault sdhApsCableFaultTE	SDH	Detection of APS cable failure condition on the specified SDH Converter Card.
354	SdhOthSidePowerOff sdhOthSidePowerOffTE	SDH	Detection of power supply failure of cards in the other side condition on the specified SDH Converter Card.
355	SdhOthSideCardFault sdhOthSideCardFaultTE	SDH	Detection of heart beat check in the other side card condition on the specified SDH Converter Card.
356	SdhEquipFailure sdhEquipFailureTE	SDH	Detection of Equipment Failure condition on the specified SDH Converter Card.

Maintaining Traps

You can maintain traps for the Total Control 1000 system using:

- Command Line Interface
- Common Element Manager
- Total Control Manager

Command Line Interface

To maintain traps for the DSP multispan card, SDH STM-0 converter card, and the DS-3 Ingress card using the Command Line Interface, refer to the *Modem and Span Command Line Reference*

To maintain traps for the access router card using the Command Line Interface, refer to the *Access Router Card Command Line Reference.*

Common Element Manager

This topic describes how to define and maintain traps for the chassis using common element manager.

When setting traps with common element manager, you have four options. Select one according to Table 6.

Table 6 Trap Options

Trap	Description
disableAll	Disables all traps.
enableTrap	Enables a trap for an Alarm Server.
enableLog	Enables a trap for a Logging Server.
enableAll	Enables a trap for both the Logging Server and Alarm Server.

When you set *enableAll*, the network management card sends information twice, i.e., to both the Logging Server and the Alarm Server.

Setting or Viewing Traps

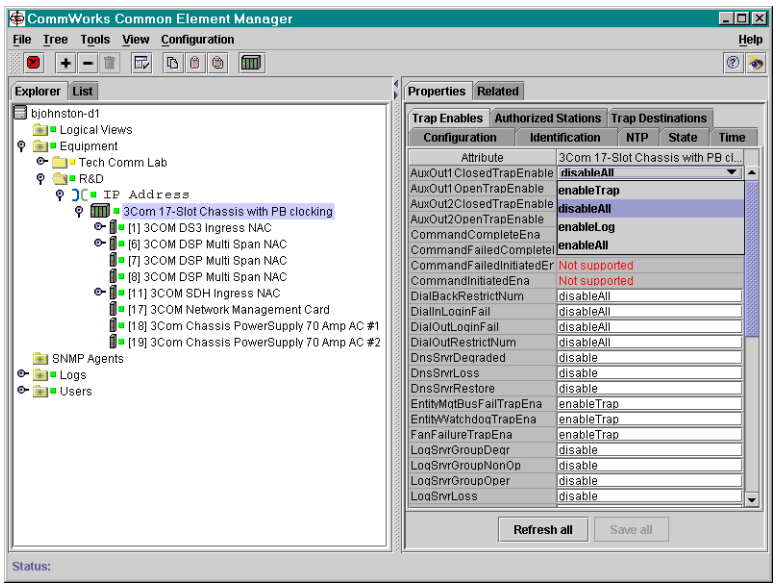
1 From the common element manager explorer tab, click the needed component.

The network management card, access router card, and the DS-3 Ingress card are not valid for this function.)

2 Click **Properties** and then the **Trap Enables** tab.

The Trap Enables tab displays as shown in Figure 6.

Figure 6 Enabling Traps for the Chassis



3 Double click on the trap status field. The drop down list displays.

Select one of the following. Refer to Table 6 for an explanation of what these settings indicate.

- enableTrap
- disableAll
- enableLog
- enableAll

4 Click **Save all**.

If you do not save the settings to the chassis' NVRAM, the trap settings will return to their default settings when the network management card reboots.

Receiving Traps

To enable trap logging using common element manager:

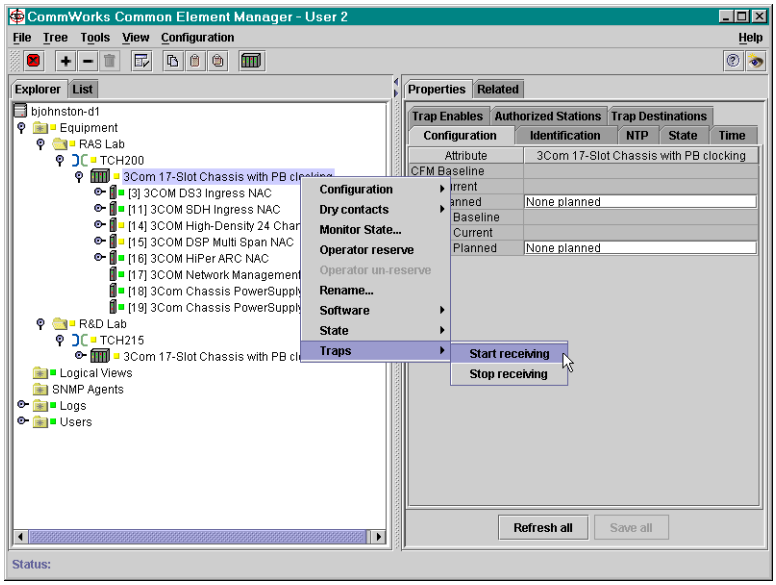
1 From the common element manager explorer tab, right-click the chassis.

The network management card, access router card, and the DS-3 Ingress card are not valid for this function.)

2 From the pop-up menu, select **Traps**.

The Setting Traps window appears as shown in Figure 7.

Figure 7 Setting Traps Window



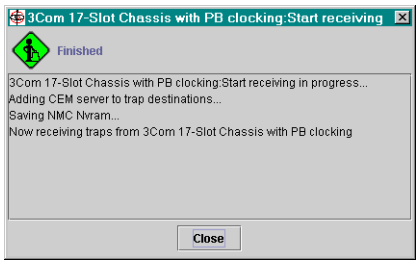
3 To enable trap logging, select **Start Receiving**.

A status box appears.

Common element manager adds the server to the trap destinations and then automatically saves the current settings to NVRAM. When trap logging is established, the **Working** icon changes to a **Finished** icon.

The Trap Receiving Finished window appears as shown in Figure 8.

Figure 8 Trap Receiving Finished Window



4 Click **Close**.

Total Control Manager

This section describes how to define and maintain traps for the chassis using total control manager.

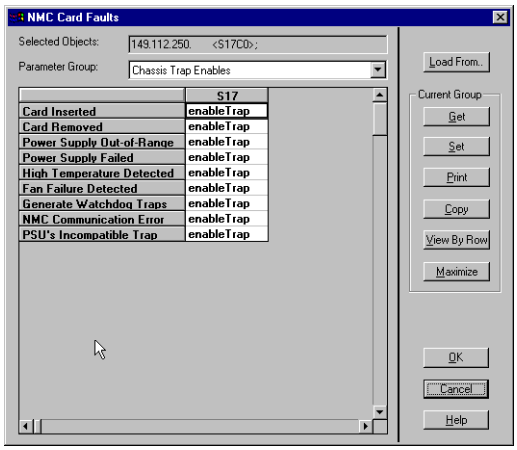
To set traps using total control manager:

1 Select the device or channel to which the parameters changes will apply.

2 On the **Main Menu** bar, click **Fault**, and then click **Trap Destinations**.

The Faults dialog box appears.

Figure 9 Card Faults Dialog Box



3 Select a parameter group.

4 Click in the S17 field next to the trap description, click the arrow, click enable or disable.

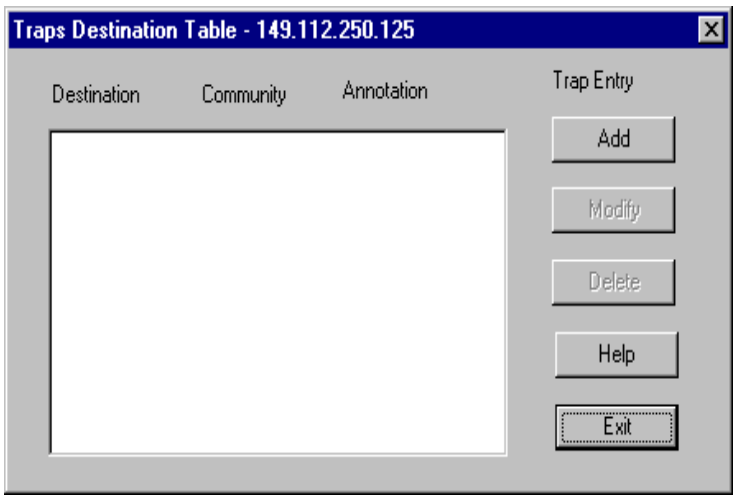
Maintaining Trap Destinations

To view the Trap Destination Table using total control manager:

1 On the **Main Menu** bar, click **Fault**, and then click **Trap Destinations**

The Traps Destination Table dialog box appears.

Figure 10 Traps Destination Table Dialog Box



You can add, modify, or delete, the Trap Destination Table from this dialog box.

To add a Trap Destination to the table:

a Click **Add**.

The Add Trap Destination dialog box appears.

Figure 11 Add Trap Destination Dialog Box

b Type in the Destination IP, Community String, and an Annotation, then click **OK** to add a destination.

To modify an entry in the trap destination table:

a Highlight a destination on Figure 11, click **Modify** to change the community string and annotation.

To delete an entry in the trap destination table:

a Highlight a destination on Figure 11, and click **Delete** to remove the destination from the list.

2 Click **OK**.

SDH STM-0 Card

Configure the SDH STM-0 module to generate Simple Network Management Protocol (SNMP) traps on detection of certain conditions. The SDH STM-0 module can generate a trap that is sent to an event viewer, a log file which is sent to an accounting server, or both.

Using total control manager, you can enable or disable the trap, enable or disable the log file, and configure where the traps are to be sent.

You will need a standard SNMP event viewer to view generated traps.

To enable traps that pertain to the SDH STM-0 span, follow this procedure:

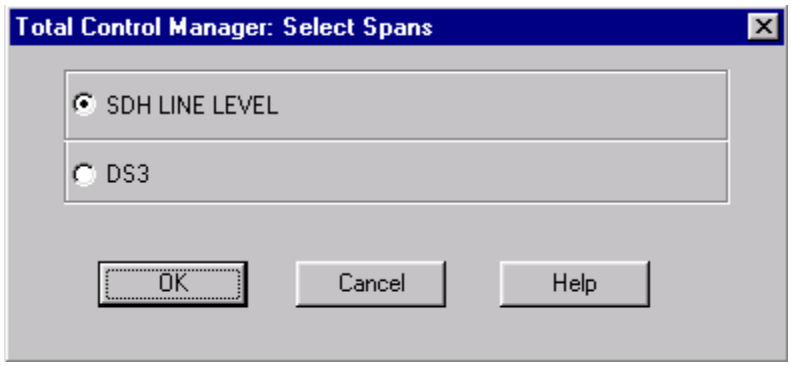
1 From total control manager's VFPD, click the LEDs on the SDH STM-0 NAC.

The LEDs turn blue. To select LEDs on both SDH STM-0 NACs, hold down **Shift** while clicking.

2 From the Fault menu, click **Trap Settings**.

The Select Spans window appears.

Figure 12 Selecting Spans Window



3 Select **SDH LINE LEVEL**.

4 Click **OK**.

The SDH Line Level Faults window appears.

5 From the Parameter Group drop-down menu, click **SDH Trap**.

The available SDH STM-0 line level traps for the SDH STM-0 module are listed in Table 7.

Table 7 SDH STM-0 Card Level Traps

Trap	Description	Settings	Default
Section Alarm	Alarm is generated upon detection of Section Alarm condition on the specified SDH STM-0 NAC.	enableTrap disableAll enableLog enableAll	disableAll
High Path AU #1	Alarm is generated upon detection of High Path AU #1 Alarm condition.	enableTrap disableAll enableLog enableAll	disableAll
High Path AU #2	Alarm is generated upon detection of High Path AU #2 Alarm condition.	enableTrap disableAll enableLog enableAll	disableAll
High Path AU #3	Alarm is generated upon detection of High Path AU #3 Alarm condition.	enableTrap disableAll enableLog enableAll	disableAll

Table 7 SDH STM-0 Card Level Traps (continued)

Trap	Description	Settings	Default
Low Path #1	Alarm is generated upon detection of a Low Path Alarm which is subordinate to High Path AU #1.	enableTrap disableAll enableLog enableAll	disableAll
Low Path #2	Alarm is generated upon detection of a Low Path Alarm which is subordinate to High Path AU #2.	enableTrap disableAll enableLog enableAll	disableAll
Low Path #3	Alarm is generated upon detection of a Low Path Alarm which is subordinate to High Path AU #3.	enableTrap disableAll enableLog enableAll	disableAll
APS Switch	Alarm is generated upon detection of an APS switch.	enableTrap disableAll enableLog enableAll	disableAll
Transmission Name Change	Alarm is generated upon detection of transmission name change.	enableTrap disableAll enableLog enableAll	disableAll
APS Cable Fault	Alarm is generated upon detection of APS cable failure.	enableTrap disableAll enableLog enableAll	disableAll
Other Side Power Failure	Alarm is generated upon detection of power supply failure of standby cards.	enableTrap disableAll enableLog enableAll	disableAll
Other Side Card Fault	Alarm is generated upon detection of heart beat check of standby cards.	enableTrap disableAll enableLog enableAll	disableAll
Equipment Failure	Alarm is generated upon detection of critical Equipment Failure.	enableTrap disableAll enableLog enableAll	disableAll

6 Click **Set** when finished setting desired traps.

7 Click **Exit**.

8 Configure trap destination parameters on the network management card. Refer to SNMP Traps and Alarms chapter for detailed instructions.

The network management card forwards traps generated by the SDH STM-0 to a workstation, or alarm server. You must configure the network management card with the IP address of the workstation running a standard event viewer application.

9 Save all configuration changes to the network management card's NVRAM.

The SDH STM-0 NAC does not directly transmit DS-3-related traps, but it changes the state of the SDH STM-0 interface to Internal Interface Failure (IIF) when a DS-3 alarm disrupts the service.

DS-3 Ingress Alarms

The SDH STM-0 module provides the hardware necessary to service the following DS-3 alarms on the DS-3 span:

- AIS—Alarm Indication Signal
- LOS—Loss of Signal
- LOF—Loss of Frame
- RAI—Remote Alarm Indication
- Idle Sequences

DS-3 Ingress Errors/Statistics

The SDH STM-0 module provides the hardware necessary to service the following DS-3 errors and statistics on the DS-3 span:

- LCV—Line Code Violation
- EXZ—Excessive Zeros
- P-bit Parity
- FEBE—Far End Block Errors
- Framing Bit Errors

Please refer to the Modem and Span Command Line Interface Reference for configuration information relating to DS-3 Ingress card and DS-3 span level traps.

3 Access Router Card

This chapter includes procedures that are useful for maintaining the access router card in your CommWorks Total Control® 1000 chassis.

This chapter contains the following topics:

For information about installing and initial configuration of this card, refer to the Total Control 1000 *Getting Started Guide*.

For information about further configuration options, refer to the *Operation Guide* or the *Access Router Card Command Line Interface Reference*.

Hot Swapping

Hot swapping an access router card or power cycling a Total Control 1000 chassis running access router card's may cause a corrupted flash file system. To prevent this from occurring enter the reboot command at the command line prompt and respond **Yes** to the reboot command.

Approximately five seconds after issuing this command it is safe to remove the power from an access router card (through hot swap or powering down the chassis). It remains safe to reboot the chassis until the prompt appears on the user console or the chassis first begins to respond to pings.

If the power is removed from an access router card during a flash write, a corrupted flash file system will result. The solution is to reformat the flash and download new software. Following the BOOT PROM prompt (shown below) enter **AT{ZF}** to reformat the flash file system. It is then necessary to download new software through z-modem and reconfigure the chassis.

Here is a sample BOOT PROM prompt:

```
BOOT PROM Version 00.03.03 (Built on Jun 15 2000 at
10:08:06)

AT{ZF} <enter>

download code now .....
```

If the flash file system is corrupt, the following is an example of what can display:

```
Fault uncovered
Err : 0x210c      FAULT_NOT_FIXABLE
(Control Structure Fault) VF_FDFRE - FD in use marked
free
FN1 : 0x24          PATH1 : /EventHandler.cfg

Fault uncovered
Err : 0x2112      FAULT FIXABLE
(File Descriptor Fault) VF_PARFD - Wrong parent FN in FD
FN1 : 0x24          PATH1 : /EventHandler.cfg
Fault processing (Taking default pHILE action)
```

Monitoring Realtime PPP Activity

This topic provides information about monitoring realtime point to point protocol (PPP) and tap commands using the common element manager and the command line interface (CLI) and .

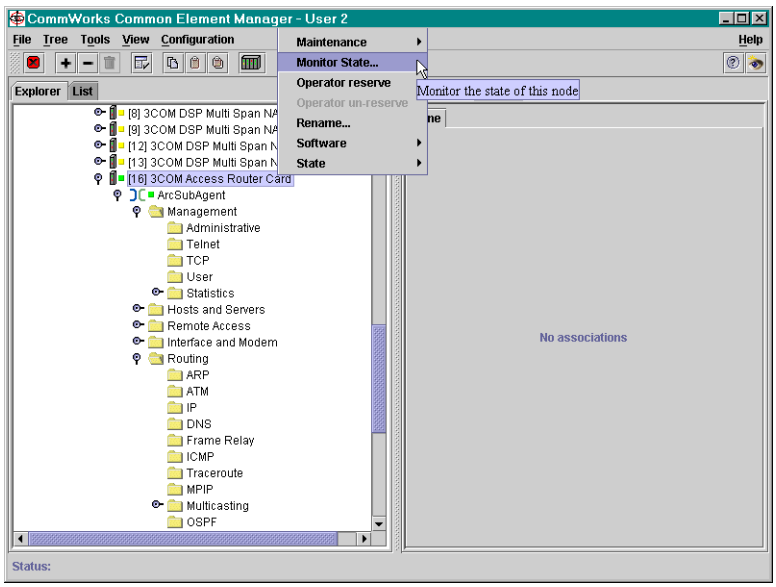
Common Element Manager

To monitor the ppp using common element manager:

1. From the Explorer tab, right-click the item you want to monitor.
2. Select Monitor State from the pop-up menu.

   Figure 13 shows the pop-up menu.

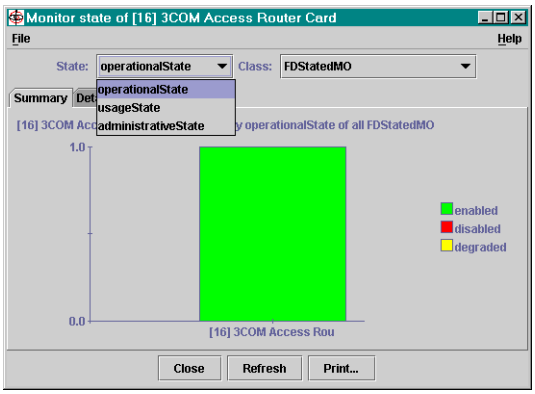
   Figure 13 Monitoring the PPP Window



3. Select the State and Class you want to monitor from the drop-down menus on the Monitor State Window.

Figure 14 shows the Monitor State window.

Figure 14 Monitor State Window



A real time graph displays showing the items that you selected.

4 Click Close, Refresh, or Print.

Command Line Interface

To monitor the ppp using CLI:

The monitor ppp command allows monitoring of realtime PPP activity. For the best results, we recommend you use this program through TELNET.

To monitor the PPP events, enter:

```
show events
```

The monitor PPP command is limited to checking PPP data streams. It cannot monitor network traffic or capture data and direct it to a SYSLOG host or your console as with the tap commands.

The PPP command performs the following types of monitoring:

- Monitoring PPP call events—displays internal PPP states as they change for each interface. Most of these events are displayed as events if the proper logging level is set for PPP. This is the only monitoring option that displays the action of more than one PPP session.

- Monitoring a specific interface—displays all PPP packets transmitted and received on the specified interface. If a session already is occurring on the specified interface, monitoring begins immediately. If not, monitoring begins with the next session on that interface. If one session stops and starts, monitoring continues.
- Monitoring the next session that starts up—displays results for next PPP session created. This option is useful if you have difficulty connecting and it's unclear which interface you will connect on because of the inclusion in a hunt group. As soon as the next incoming or outgoing PPP call is established, monitoring begins. There is no differentiation on the next session - you select to monitor the next session and the next session displays regardless of interface or user name used.

Only one monitor may be used for Next Session at any one time.

- Monitoring a specific user—displays any PPP sessions currently active for the specified user. As any new session begins for the user, monitoring also begins. This is the best method to display data from a multi-link session.

Since the PPP session does not have a user associated with it until authentication occurs, this method of monitoring does not permit tracing of the authentication negotiation.

- Exiting the monitor—exits the program.

Example:

```
HiPer>> monitor ppp
```

Figure 15 shows what displays when you issue the monitor ppp command.

Figure 15 HiPer PPP Monitor

```
HiPer PPP Monitor

Select a letter for one of the following options:
      C) Monitor PPP Call Events.
      I) Monitor a specific interface.
      N) Monitor the next session that starts up.
      U) Monitor a specific user.
      T) Monitor a specific calling number.
      X) Exit the monitor.
   Please Enter Your Choice :
```

Figure 16 displays the results of Option '**C**'.

Figure 16 Monitoring PPP Call Events - Option C

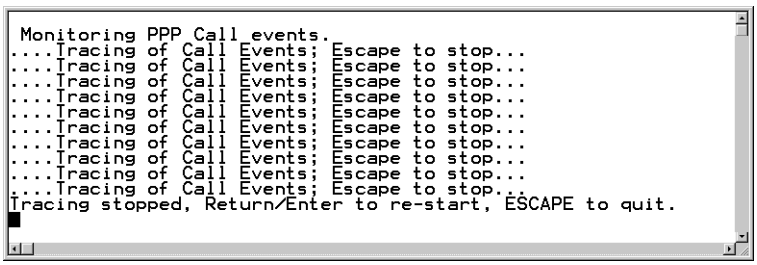


Figure 17 displays the results of Option '**I**'.

Figure 17 Monitoring PPP Call Events - Option I

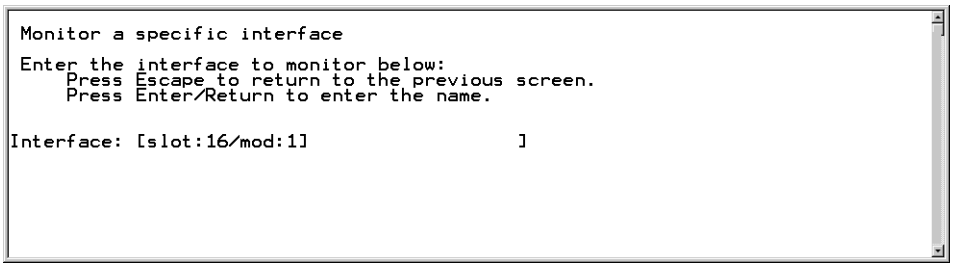


Figure 18 displays the results of Option '**N**'.

Figure 18 Monitoring PPP Call Events - Option N

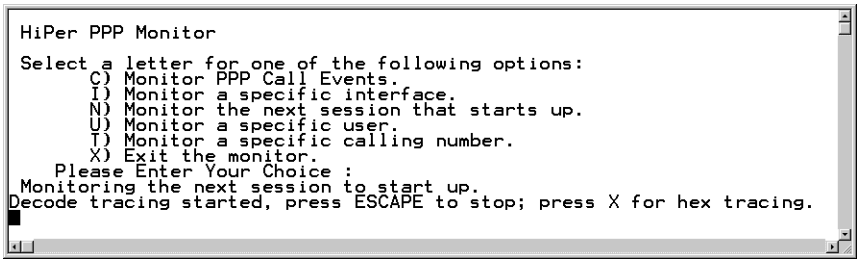
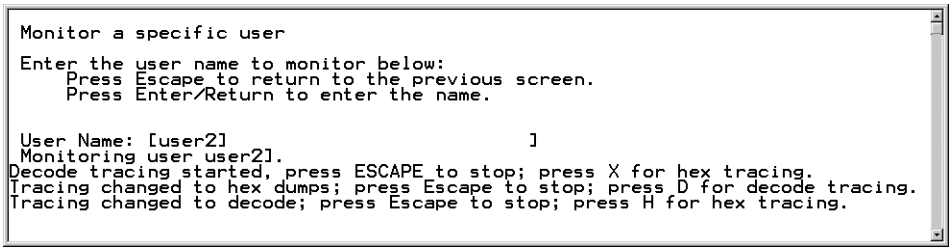


Figure 19 displays the results of Option '**U**'.

Figure 19 Monitoring PPP Call Events - Option U



All PPP packets sent or received while the monitor is "paused" are lost and not saved waiting for the program to resume. Also, if a call is dropped at any time, you must return to the monitor and start again.

Decode and Hexadecimal Display

The Interface, User, and Next Session monitoring, display two types of data: decode and hexadecimal.

- Decode—displays packets in a textual, decoded output. This is the default setting.
- Hexadecimal—displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission.

To switch from decode mode to hexadecimal mode, type: **H** or **X** (not case sensitive). To switch back to decode mode, type: **D**

There may be a lag due to delayed output to the screen.

Tap All Packets

Tap commands access data streams in order to diagnose connection problems or to log data to an off-line location. All data is captured bidirectionally in the stream (including protocol negotiation) on an *interface, user,* or *next call* basis. Data can then be dumped to a SYSLOG host, the console port, or a virtual console port (e.g. TELNET connection) in hexadecimal, ASCII, or clear text.

How Tap Works

A tap added for a user begins tapping all currently active sessions as well as future sessions of that user until a delete command is issued for the added tap.

Taps are identified by an ID number. Adding a tap for the user adds a generic entry for the user and clones of the tap entry are added for each active session of the user. Deleting the generic entry (identified by its ID number) deletes all tap sessions as well. But, deleting a specific session only deletes that session.

Permanent taps for a user are installed automatically when a user logs in and if the user's profile has tapping enabled.

*The **monitor ppp** command performs some similar functions as the tap command but is limited to PPP data streams only. Use tap commands to capture network traffic to a remote SYSLOG host or your console.*

Use the **list tap** command to view currently enabled taps.

Syslog Option

When using the **syslog** option, for each tap, data is prioritized and directed to one of eight priority locations, refer to Monitoring RADIUS Activity. Specifying *facility, priority* and an *IP address* for each tap is useful if the remote SYSLOG daemons are set up to direct different facility and priority levels to different destination files or terminals.

Screen Option

When using the **screen** option, data from the tap is directed to the screen where the Command Line Interface (CLI) command was issued. The CLI prompt appears only when the tap has ended. A simple interface appears on screen with one option available: **Esc** followed by the **Enter** key to end the tap. Pressing these keys in sequence stops a tap.

Taps degrade system performance considerably and are not saved to FLASH memory to guard against accidentally set, long-running taps. The configuration you choose to tap is flushed upon system reboot, so tap commands must be re-issued on system startup. A permanent user tap can be set using vendor-specific RADIUS attributes.

Taps on RADIUS users

Setting appropriate flags in a user's RADIUS profile turns on logging to a network file so that every time a user logs on, the log file is appended to it. This function facilitates auditing and tracking a blacklisted user, for which long-term monitoring may be desirable. Employing the *Port-Tap* attribute can monitor local users while vendor-specific RADIUS attributes can monitor remotely authenticated users.

Monitoring RADIUS Activity

The monitoring of radius feature allows the monitoring of realtime RADIUS activity. This feature provides:

- Monitoring all RADIUS packets—displays all RADIUS packets transmitted or received.
- Monitoring all RADIUS authentication packets—displays all RADIUS authentication packets transmitted or received.
- Monitoring all RADIUS accounting packets—displays all RADIUS accounting packets transmitted or received.
- Monitoring a specific RADIUS user—displays any RADIUS sessions currently active for the specified user. When a new session begins, monitoring also begins.

- Monitoring the next session that starts up—displays results for next RADIUS session created.

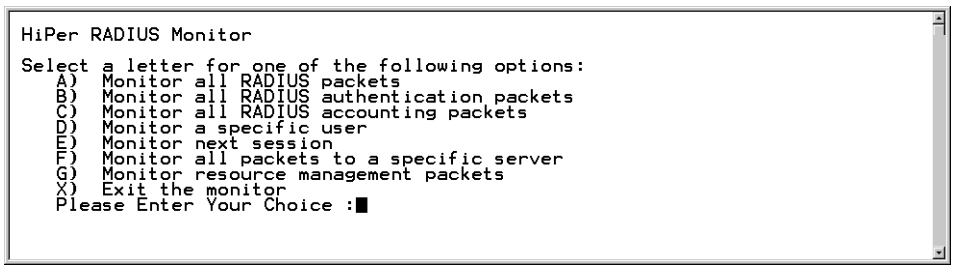
  This option is useful if you are having difficulty connecting and it's unclear which interface you will connect on because of the inclusion in a hunt group. As soon as the next incoming or outgoing RADIUS connection is established, monitoring begins. There is no differentiation on the next session - you select to monitor the next session, and the next session displays regardless of interface or user name employed.
- Monitoring all RADIUS packets sent to or received from a specific server—displays all traffic to and from a specified server.
- Monitor Resource Management Packet—displays the status of the management software.
- Exiting the monitor—exits the program.
- Decode and Hexadecimal Display—displays two types of data: *decode* or *hexadecimal. Decode, (*the default), displays packets in a textual, decoded output. *Hexadecimal* displays packets with decompression in hexadecimal and any ASCII equivalent as soon as they are received or just before transmission. Both modes can be switched on the fly.

Example:

```
HiPer>> monitor radius
```

Figure 20 displays the results of the **monitor radius** command.

Figure 20 RADIUS Monitor



*Pressing the letters **H** or **D** toggles the Decode and Hex Dump modes. By default, RADIUS monitor starts in decode mode. At any time during tracing, pressing **H** toggles it to Hex Dump mode; pressing **D** toggles it back to Decode mode. Pressing the **ESC** key at any time during tracing places the monitor back in Main Menu.*

Type the IP Address of the RADIUS server. You must enter the IP address of the RADIUS server and the host name, or any other alias.

After typing the IP address of the RADIUS server, press **ENTER**.

4 DSP MULTISPAN CARD

This chapter includes procedures that are useful for maintaining the modems in your Total Control® 1000 chassis.

This chapter contains the following:

If applicable, the examples are given using Command Line Interface (CLI) commands, and common element manager.

For more information on the Command Line Interface, refer to the *DSP Multispan Command Line Interface Reference*.

For information about installing and initial configuration of this card, refer to the Total Control 1000 *Getting Started Guide*.

For information about further configuration options, refer to the *Operation Guide*.

Unless otherwise specified, all references to the DSP multispan card also apply to the HiPer DSP card.

Using Modem Soft Reboot

The modem card soft reboot support feature allows you to reboot the modem card after a specified amount of time or when all calls or channels are inactive, whichever occurs first.

This section includes procedures for using soft reboot using common element manager, total control manager, and the command line interface.

To execute the soft reboot support feature, a Total Control® 1000 chassis installation must include a network connection to one or more data hubs containing a modem card set – Network Application Card (NAC) and Network Interface Card (NIC).

Common Element Manager

To set the soft reboot using common element manager:

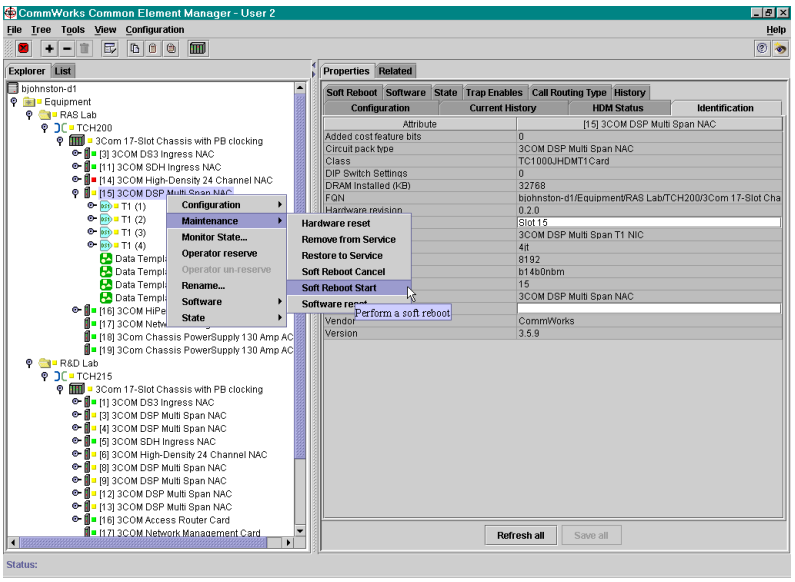
1 From the **Explorer** tab, right click the DSP multispan card.

2 Select **Maintenance** from the pop-up menu.

3 Select **Software Reboot** from the pop-up menu.

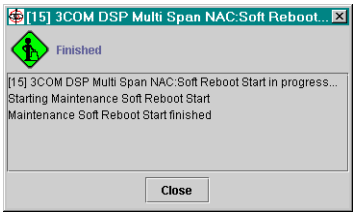
Figure 21 shows the Software Reboot pop-up menu.

Figure 21 Software Reboot Window



A dialog box appears and lists the progress of the command. When the command has executed, the **Working** icon changes to a **Finished** icon.

Figure 22 Software Reboot Finished Window



4 Click **Close**.

Total Control Manager

To set the soft reboot time using total control manager:

1 Click the modem card in total control manager.

The card turns blue.

2 From the **Configure** menu, click **Programmed Settings**.

The **Select Card Level or Template(s)** window displays.

3 Select **Card Level**, and click **OK**.

The DSP MultiSpan Card Programmed Settings window displays.

4 From **Parameter Group**, click **DSP Multispan Configuration** from the drop-down box.

5 Select the desired time amount beside the Soft Reboot Time parameter selection.

To manually soft reboot the modem card using total control manager:

1 Click the modem card within total control manager.

The card turns blue.

2 From the **Configure** menu, click **Actions/Commands**.

The Total Control Manager Commands window displays.

3 Under Command to Execute, select **Software** from the first drop-down box.

4 Select **Soft Reboot** from the second drop-down box.

5 Click **Execute**.

The Command Status box contains a message concerning the status of the executed command.

Command Line Interface

The following are procedures on how to set the soft reboot feature using the Command Line Interface (CLI).

To set the soft reboot time using the CLI, use this command:

```
> softreboottime
```

This command sets and displays the soft reboot timeout value.

Span and Timeslot

You can perform maintenance on both the modem span and timeslots.

The modem allows you to use maintenance modes to remove a span or timeslot from service. Some practical reasons for removing a span or timeslot(s) from service are as follows:

- Testing the modem card
- Awaiting a telephone company to re-activate provisional spans
- Training new operators and employees
- Trouble locating and clearing

This section provides information on the following procedures:

Configuring Maintenance Modes

You can configure the modem for maintenance modes using these two steps.

1 Configuring Timeslot Maintenance Settings

2 Configuring Span Maintenance Settings

*Some of the maintenance settings cause the modem to immediately take timeslots and the span out of service—even if remote users are connected. Using the timeslot **Soft Busy Out** feature is strongly recommended in almost every maintenance scenario.*

Configuring Timeslot Maintenance Settings

To configure Timeslot Maintenance settings using common element manager:

1 From the **Explorer** tab, select one or more DS0s.

2 Right-click one of the selected DS0s.

3 Select **Maintenance** from the pop-up menu.

4 Select a maintenance setting from the pop-up menu.

Figure 23 shows the timeslot maintenance options.

Figure 23 Timeslot Maintenance Options Window

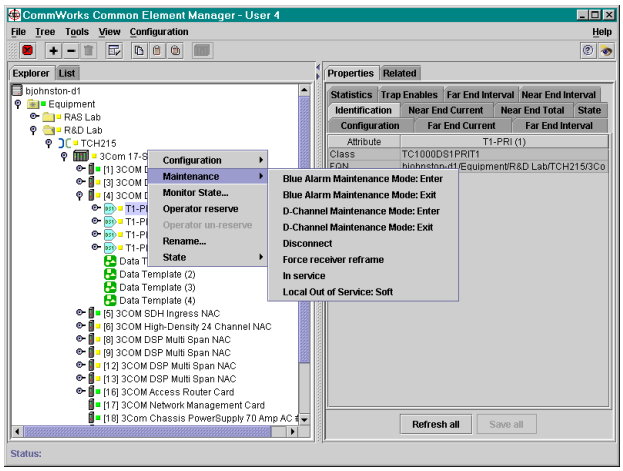


Table 8 list the available options.

Table 8 Timeslot Maintenance Options

Option	Description
Blue Alarm Maintenance Mode: Enter	Causes the modem to transmit all ones, signaling the span is busy on layer 1. Therefore, the network will bypass this span, and new calls try to route to a different span. The *Utilization* LEDs on the modem will flash red when this setting is enabled. Note: This setting will persist (if saved to NVRAM) even if you reboot the modem. Refer to the command below to exit this maintenance mode.
Blue Alarm Maintenance Mode: Exit	If in Blue Alarm Maintenance Mode, causes the modem to stop transmitting all ones.
D-Channel Maintenance Mode: Enter	Disables the D-channel from service on layer 2. The *Utilization* LEDs on the modem will flash yellow when this setting is enabled.
D-Channel Maintenance Mode: Exit	Enables the D-channel for service when it is in D-channel Maintenance Mode.
Disconnect	Disconnects the timeslots.
Force receiver reframe	Enter the force receiver reframe mode.
In Service	Places the selected DS0 in the In Service State.
Local Out of service: Soft	Disables a span from service on layer 3.
Block Timeslot	Sends a code of all 1s to the exchange informing the exchange not to send any calls to this timeslot.
Hard Busy Out	Causes timeslots to immediately disconnect, even if remote users are connected.
Reset DSP	Resets the timeslot.
Soft Busy Out	Causes timeslots to busy out after the remote user disconnects.
Unblock Timeslot	Causes the modem to stop sending all 1s if *Block* is enabled.
callignore	Causes the timeslots to ignore all calls.

Depending on your configuration you may not see all of these selections or the naming may not be exact.

A dialog box appears and lists the progress of the command. When the command has executed, the **Working** icon changes to a **Finished** icon.

5 Click **Close**.

Configuring Span Maintenance Settings

To configure Span Maintenance settings using common element manager:

1 From the **Explorer** tab, right-click the DSP multispan.

2 Select **Maintenance** from the pop-up menu.

3 Select a maintenance setting from the pop-up menu.

Figure 23 shows the span maintenance options.

Figure 24 Span Maintenance Options Window

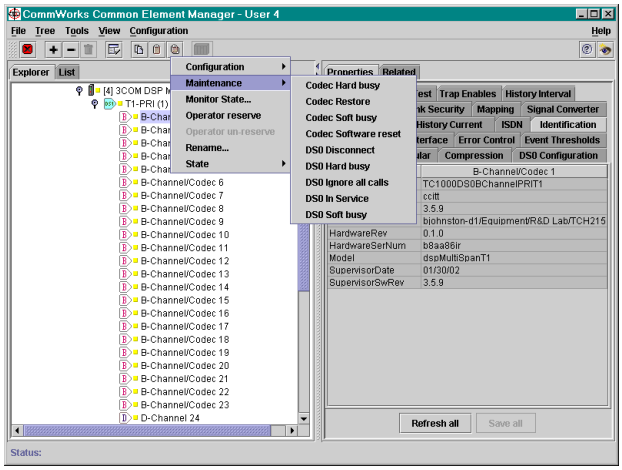


Table 9 list the available options.

Table 9 Span Maintenance Options

Option	Description
Codec Hard Busy	Causes span to immediately disconnect, even if remote users are connected.
Codec Restore	Restores the span to normal service.
Codec Soft busy	Causes spans to busy out after the local user disconnects.
Codec Software reset	Resets the spans software to the default configuration.
DS0 Disconnect	Disconnects all the timeslots on the HiPer DSP.
DS0 Hard busy	Causes timeslot to busy out immediately.
DS0 ignore all calls	Causes the timeslot ignore all calls.
DS0 In Service	Enables a span for service when it is out of service.
Soft Busy Out	Causes timeslots to busy out after the remote user disconnects.

Depending on your configuration you may not see all of these selections or the naming may not be exact.

A dialog box appears and lists the progress of the command. When the command has executed, the **Working** icon changes to a **Finished** icon.

4 Click **Close**.

Do not attempt to dial out when the span is out of service.

Total Control Manager

To configure Timeslot Maintenance settings using total control manager:

1 Click the span LEDs of the appropriate modem card. The LEDs turn blue.

2 From the **Configure** menu, click **Actions Commands**. The Select Timeslots window displays.

3 Click **Timeslot**.

4 Under Span Line 1, click **Select All**.

5 Click **OK**.

The Total Control Manager Commands window displays.

6 In the second **Command to Execute** box select the options that you need.

Table 10 list the available options.

Table 10 Timeslot Maintenance Settings

Command	Description	Use this with
No Command	This option displays so users know they must select a command.	T1, E1/PRI, E1/R2
Disconnect	Disconnects the timeslots.	T1, E1/PRI, E1/R2
Call Ignore	Causes the timeslots to ignore all calls.	T1
Restore	Restores timeslots to normal service.	T1
Soft Busy Out	Causes timeslots to busy out after the remote user disconnects.	T1
Hard Busy Out	Causes timeslots to immediately disconnect, even if remote users are connected.	T1
Block	Sends a code of all 1's to the exchange informing the exchange not to send any calls to this timeslot.	E1/R2
Unblock	Causes the modem to stop sending all 1's if *Block* is enabled.	E1/R2

7 Select the appropriate maintenance setting.

8 Click **Execute**.

To further verify the status of the timeslots, use the performance monitor features of total control manager.

Configuring Span Maintenance Settings

To configure Span Maintenance settings using total control manager:

1 Click the span LEDs of the appropriate modem card. The LEDs turn blue.

2 From the **Configure** menu, click **Actions Commands**.

The Select Timeslots window appears.

3 By default, Span Line is selected. Use this default.

4 Click **OK**.

The Total Control Manager Commands window appears.

5 In the second **Command to Execute** box, select the options that you need.

Table 11 lists the options the available options.

Table 11 Span Maintenance Settings

Command	Description	Use this with
No Command	This option displays so users know they must select a command.	T1, E1/PRI, E1/R2
Forced Receiver Reframe	Immediately forces a receiver reframe.	T1, E1/PRI, E1/R2
In Service	Enables a span for service when it is out of service.	T1
Local Out of Service	Disables a span from service on layer 3.	T1
Disconnect	Disconnects the span connection.	T1, E1/PRI, E1/R2
Enter D-channel Maintenance Mode	Disables the D-channel from service on layer 2. The *Utilization* LEDs on the modem will flash yellow when this setting is enabled.	T1, E1/PRI
Exit D-chan Maintenance Mode	Enables the D-channel for service when it is in D-chan Maintenance Mode.	T1, E1/PRI
Enter Blue Alarm Maintenance Mode	Causes the modem to transmit all ones, signaling the span is busy on layer 1. Therefore, the network will bypass this span, and new calls try to route to a different span. The *Utilization* LEDs on the modem will flash red when this setting is enabled. Note: This setting will persist (if saved to NVRAM) even if you reboot the modem. Refer to the command below to exit this maintenance mode.	T1, E1/PRI
Exit Blue Alarm Maintenance Mode	If in Blue Alarm Maintenance Mode, causes the modem to stop transmitting all ones.	T1, E1/PRI
Block Span	Sends a code of all 1's to the exchange informing the exchange not to send any calls to this span.	E1/R2
Unblock Span	Causes the modem to stop sending all 1's if *Block Span* is enabled.	E1/R2

6 Select the appropriate maintenance mode from the table above.

7 Click **Execute**.

Do not attempt to dial out when the span is out of service.

D-channel disconnect mode affects multiple spans when using NFAS.

If you reboot the modem the span will return to its normal state: in service—unless you are using Blue Alarm Maintenance Mode.

If you are using a backup D-channel, it will become in service when you take the primary D-channel out of service: the backup D-channel will become the primary D-channel.

Restoring the Span to Service

Follow the procedures in Configuring Span Maintenance Settings, and select the *Codec Restore* and *DS0 In Service* settings.

Circuit Blocking

This section describes circuit blocking, available settings, and the effects of blocking and unblocking on the Total Control 1000 system. Circuit blocking is only compatible with systems containing spans configured for SS7 signaling.

Primary Rate Interface signaling is not supported for circuit blocking.

Circuits can be blocked and unblocked as follows:

- Placing an SS7 or DSP multispan inbound/outbound circuit in one of four states: unblocked, inbound blocked, outbound blocked, and bothway blocked. When a circuit is blocked both ways, it is functionally out-of-service.
- Blocking and unblocking circuits that are inbound from and outbound to the Public Switched Telephone Network (PSTN).
- Total Control 1000 can issue blocking commands to the DSP multispan if the access router card loses connection to the SIP proxy server, accounting server, or directory server. It can issue unblocking commands when the connection is reestablished.

Table 12 lists the effects of PSTN initiated, SS7 gateway initiated, and DSP multispan initiated circuit blocking on the PSTN, SS7 gateway, and DSP multispan.

Table 12 Effects of Circuit Blocking on the Total Control 1000 System

Initiator / Block Type	Effect on SS7 Gateway	Effect on DSP Multispan	Effect on PSTN
PSTN—Block	The SS7 gateway sends an Outbound Block message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' to Outbound blocked	The circuits on the PSTN are blocked.
PSTN—Unblock	The SS7 gateway sends an Inbound an Outbound Unblock message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' to Unblocked.	The circuits on the PSTN are unblocked.
SS7 gateway—Block Inbound	The SS7 gateway sends an Inbound Block message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	The circuits on the PSTN are blocked.
SS7 gateway—Block Outbound	The SS7 gateway sends an Outbound Block message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	No effect.
SS7 gateway—Block Bothways	The SS7 gateway sends an Inbound and Outbound Block message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' to Bothways blocked.	The circuits on the PSTN are blocked.
SS7 gateway—Unblock Inbound	The SS7 gateway sends an Inbound Unblock message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	The circuits on the PSTN are unblocked.
SS7 gateway—Unblock Outbound	The SS7 gateway sends an Outbound Unblock message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	No effect.
SS7 gateway—Unblock Bothways	The SS7 Gateway sends an Inbound and Outbound Unblock message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' to Unblocked state.	The circuits on the PSTN are unblocked.

Table 12 Effects of Circuit Blocking on the Total Control 1000 System (continued)

Initiator / Block Type	Effect on SS7 Gateway	Effect on DSP Multispan	Effect on PSTN
DSP multispan—Block Inbound	The SS7 gateway receives an Inbound Block message from the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	The circuits on the PSTN are blocked.
DSP multispan—Block Outbound	The SS7 gateway sends an Outbound Block message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	No effect.
DSP multispan—Block Bothways	The SS7 gateway sends an Inbound and Outbound Block message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' to Bothway blocked.	The circuits on the PSTN are blocked.
DSP multispan—Unblock Inbound	The SS7 gateway receives an Inbound Unblock message from the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	The circuits on the PSTN are unblocked.
DSP multispan—Unblock Outbound	The SS7 gateway sends an Outbound Unblock message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' accordingly.	No effect.
DSP multispan—Unblock Bothways	The SS7 gateway sends an Inbound and Outbound Unblock message to the DSP multispan.	The DSP multispan updates the status of the media gateway 'service state' to Unblocked.	The circuits on the PSTN are unblocked.

This section describes DSP multispan initiated circuit blocking only. Refer to the SS7 gateway's documentation for detailed instructions on SS7 gateway initiated circuit blocking.

There are two types of blocking available to the SS7 gateway and the DSP multispan:

- Soft blocking—existing calls that are using the impacted circuits are allowed to continue, but new calls are prevented after the circuit is blocked.
- Hard blocking—existing calls that are using the impacted circuits are discontinued and new calls are not allowed after the circuit is blocked.

Each time a block or unblock is issued, a trap is sent.

Using the Circuit State View

A circuit state change at one piece of equipment usually causes a state change in multiple circuits.

You can use the DSP multispan's CLI or the common element manager to view DSP multispan circuit states.

Common Element Manager

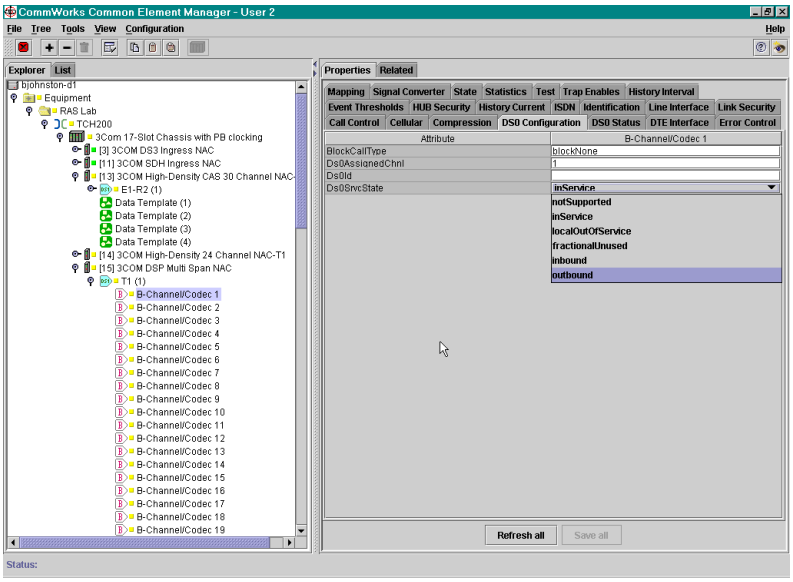
To view the DSP multispan circuit state using the common element manager:

1. From Explorer tab, double-click the span under the DSP multispan.
2. From the Explorer tab, click the desired timeslot channel.
3. Click the **DS0 Configuration** tab.

4 Double-click the DS0SrvcState field for the Performance statistics display for the selected timeslot.

The DS0SrvcState is the current service state of a DS0 timeslot. This object does not apply to robBit T1 operations.

Figure 25 DS0 Configuration Tab



5 Click **Save All**.

The DS0 Status tab contains the results of the DS0 configuration for the circuit state.

Table 13 lists the parameters and their settings on the DS0 Status tab.

Table 13 DSP Multispan Time Slot Performance Parameters

Name	Notes	Available Parameters
ActionQueued	For example, a soft busy-out command issued while a call is up would show up here.	notSupported none localOutOfService callIgnore pbinservice enfaspending
Call ID	Associated call_id, if any.	INTEGER
ChanConnTo	This parameter indicates the channel of the device currently connected. Default is 255.	0...255
CallEvQ93Nal	This object contains the Q931 call reference value, if there is an active call on the DS0 timeslot. Also used in call event trap.	INTEGER

Table 13 DSP Multispan Time Slot Performance Parameters (continued)

Name	Notes	Available Parameters
Timeslot Status	This parameter indicates the current status of the specified timeslot. The status values change dynamically with system operation.	other idle dialingIn dialingOut connectedIn connectedOut ds0CallDisc ds0IsDchan ds0OutOfServ ds0InMaint ds0IsFchan ds0LclOutOfService ds0ReceivingBlock ds0LoopBack ds0LclOutOfServiceGWCNMC ds0IsE1CASSignalingChan

Command Line Interface

From the CLI, you can use the ats and atc commands to view circuit states on the DSP multispan card.

To view the DSP multispan circuit state from the ats screen:

1. From a terminal emulation program (e.g., HyperTerminal), connect to the DSP multispan's Command Line Interface.
2. Access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

   >chdev span x

   The span level command prompt displays:

   span1>

3. At the command prompt, type this command:

   span1> display ats

A screen similar to the format of Figure 26 appears.

Figure 26 DSP Multispan Display ATS Command

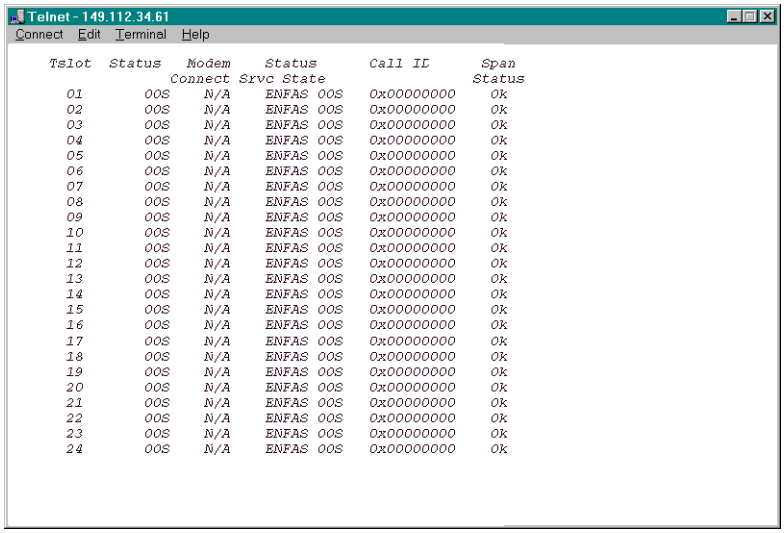


Table 14 describes the DSP multispan ATS command display.

Table 14 DSP Multispan ATS Command Fields

Name	Description	Settings
Tslot	The timeslot number	Each timeslot (1-32) is listed individually
Status	The current status for the timeslot	OOS IDLE Conn In Conn Out Dial In Dial Out Disc Lpbk Maint LCLOOS Blocked
Modem Connect		N/A

Table 14 DSP Multispan ATS Command Fields (continued)

Name	Description	Settings
Status Srvc State	The Service state for the circuit	BW_BLOCKED (Bothway blocked)—All calls blocked
		UNBLOCKED—Can take all calls.
		OB_BLOCKED (outbound blocked)—Outbound calls are blocked. Can take inbound calls.
		IB_BLOCKED (inbound blocked)—Inbound calls are blocked. Can take outbound calls.
		ENFAS OOS (ENFAS out-of-service)—Lost ENFAS connection to access router card
		PB OOS (Packet Bus out-of-service)
		IN
		Local OOS
		Remote OOS
		Maint
Call ID		Null
Span Status		

To view the DSP multispan circuit state from the **atc** screen:

1 From a terminal emulation program, connect to the DSP multispan's Command Line Interface.

2 Access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

```
>chdev span x
```

The span level command prompt displays:

```
span1>
```

3 At the command prompt, type this command:

```
span1> display atc
```

A screen similar to the format of Figure 27 appears.

Figure 27 DSP Multispan Display ATC Command

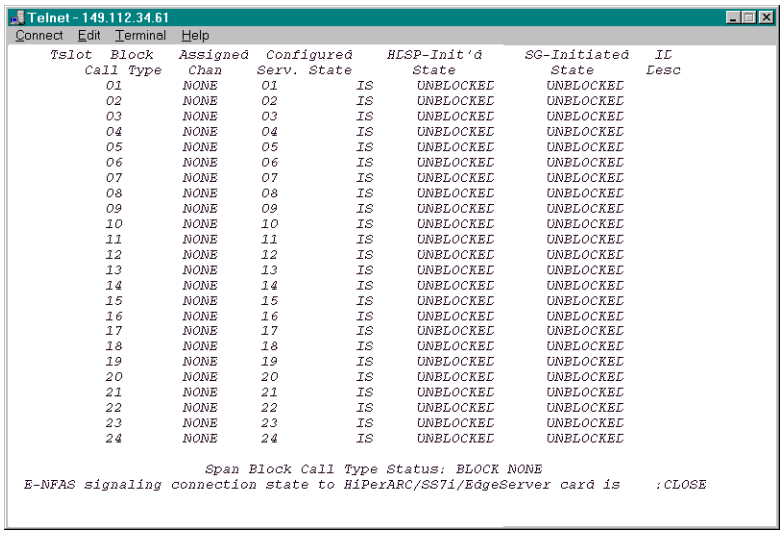


Table 15 lists the various Management Blocking and Signal Gateway Blocking States displayed in the **`atc`** screen.

Table 15 DSP Multispan ATC Command Fields

Name	Description	Settings
Tslot	The time slot number	Each slot (1-32) is listed individually
Block Call Type		none
Assigned Chan		1-32
Configured Serv. State	The service state for which the DSP multispan slot is configured	IS (In Service) OOS (Out Of Service) IB-Blocked (inbound blocked) OB-Blocked (outbound blocked) BW_Blocked (Bothway blocked) Unblocked

Table 15 DSP Multispan ATC Command Fields (continued)

Name	Description	Settings
Management Blocking State	State configured using network management card.	BW_Blocked (Bothway blocked)—All calls blocked Unblocked—Can take all calls. OB_Blocked (outbound blocked)—Outbound calls are blocked. Can take inbound calls. IB_Blocked (inbound blocked)—Inbound calls are blocked. Can take outbound calls. IS—(In Service) OOS—(Out of Service)
Sig Gateway BlockingState	The blocking state configuration received from the the SS7 gateway	BW_Blocked (Bothway blocked) Unblocked—Can take all calls. OB_Blocked (outbound blocked)—Outbound calls are blocked. Can take inbound calls. IB_Blocked (inbound blocked)—Inbound calls are blocked. Can take outbound calls. IS—(In Service) OOS—(Out of Service)
ID Desc		Null

Issuing Circuit Blocking Commands

You can issue circuit blocking from the DSP multispan using the CLI or common element manager. You can issue both blocking and unblocking commands on both the span and timeslot levels.

Common Element Manager

To block *spans* from the DSP multispan using common element manager:

1. From common element manager, double-click the DSP multispan card.

   The span elements appear under the DSP multispan card.

2. Right-click the desired span, and select **Maintenance** from the drop-down menu.

3. Click **Block Span** from the drop-down menu.

   A confirmation box appears.

4. Click **OK**.

To unblock *spans* from the DSP multispan using common element manager:

1. From common element manager, double-click the DSP multispan card.

   The E1 span elements appear under the DSP multispan card.

2 Right-click the desired span, and select **Maintenance** from the drop-down menu.

3 Click **Unblock Span** from the drop-down menu.

A confirmation box appears.

4 Click **OK**.

To block *timeslots* from the DSP multispan using common element manager:

One E1 span, or trunk, contains 32 individual DS0s, or timeslot channels. The D-channel is reserved for signaling, and the F-channel is reserved for framing (synchronization) and maintenance. Do not block the F or D channel timeslots. Block the 30 B-channels that are used for transporting user information.

1 From common element manager, double-click the DSP multispan card.

The span elements appear under the DSP multispan card.

2 Double-click the span under the DSP multispan.

3 Right-click the desired timeslot channel, and click **Block Timeslot** from the drop-down menu.

A confirmation box appears.

4 Click **OK**.

To unblock *timeslots* from the DSP multispan using common element manager:

One E1 span, or trunk, contains 32 individual DS0s, or timeslot channels. The D-channel is reserved for signaling, and the F-channel is reserved for framing (synchronization) and maintenance. Do not unblock the F or D channel timeslots. Unblock the 30 B-channels that are used for transporting user information.

1 From common element manager, double-click the DSP multispan card.

The E1 span elements appear under the DSP multispan card.

2 Double-click the E1 span under the DSP multispan.

3 Right-click the desired timeslot channel, and click **Unblock Timeslot** from the drop-down menu.

A confirmation box appears.

4 Click **OK**.

Command Line Interface

To block *spans* from the DSP multispan using the CLI:

1 From the DSP multispan's CLI, access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

```
>chdev span x
```

The span level command prompt displays:

```
span1>
```

2 As part of the block command, you must specify the direction of the calls to be affected.

For example, use the following command and desired parameter to block calls on a particular span:

span1> **cmd sblock <inbound | outbound | both>**

3 In addition to giving the direction of the calls to be affected, you must specify the level of force of the blocking as either soft or hard.

***Soft blocking**: After you issue the command, active calls on the blocked circuit remain up until they complete. All subsequent calls are blocked.*

***Hard blocking**: After you issue the command, active calls on the blocked circuit are dropped. All subsequent calls are blocked.*

For example:

span1> **cmd sblock inbound <soft | hard>**

To unblock spans from the DSP multispan using the CLI:

1 From the DSP multispan's Command Line Interface, access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

```
>chdev span x
```

The span level command prompt displays:

```
span1>
```

2 As part of the unblock command, you must specify the direction of the calls to be affected.

For example, use the following command and desired parameter to unblock calls on a particular span:

span1> **cmd sunblock <inbound | outbound | both>**

To block *timeslots* from the DSP multispan using the Command Line Interface:

These blocking commands only appear on the command line when the DSP multispan is configured for SS7 signaling. In other words, ***sigmode*** *must be set to* ***nosig*** *and* ***cfgss7mode*** *set to* ***enfas_slap****. Refer to the Total Control 1000 Enhanced Data System* Getting Started Guide *for SS7 configuration.*

1 Access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

```
>chdev span x
```

The span level command prompt displays:

```
span1>
```

2 Access the appropriate timeslot channel. Change to the appropriate timeslot channel by typing the following command, and replacing "x" with the desired timeslot level (0 - 31):

```
chdev tslot x
```

The timeslot level command prompt displays. For example:

```
span1/tslot10>
```

3 As part of the block command, you must specify the direction of the calls to be affected.

For example, use the following command and desired parameter to block calls on a particular timeslot:

```
span1/tslot10> cmd tblock <inbound | outbound | both>
```

4 In addition to giving the direction of the calls to be affected, you must specify the level of force of the blocking as either soft or hard.

Soft blocking*: After you issue the command, active calls on the blocked circuit remain up until they complete. All subsequent calls are blocked.*

Hard blocking*: After you issue the command, active calls on the blocked circuit are dropped. All subsequent calls are blocked.*

For example:

```
span1/tslot10> cmd tblock inbound <soft | hard>
```

To unblock timeslots from the DSP multispan using the Command Line Interface:

These unblocking commands only appear on the command line when the DSP multispan is configured for SS7 signaling. In other words, ***sigmode*** *must be set to* ***nosig*** *and* ***cfgss7mode*** *set to* ***enfas_slap****. Refer to the Total Control 1000 Enhanced Data System* Getting Started Guide *for SS7 configuration.*

1 Access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

```
>chdev span x
```

The span level command prompt displays:

```
span1>
```

2 Access the appropriate timeslot channel. Change to the appropriate timeslot channel by typing the following command, and replacing "x" with the desired timeslot level (0 - 31):

```
chdev tslot <channel number>
```

The timeslot level command prompt displays. For example:

```
span1/tslot10>
```

3 As part of the unblock command, you must specify the direction of the calls to be affected. For example, to block inbound calls, use the command:

```
span1/tslot10> cmd tunblock inbound
```

Configuring Timeslot Service States

Use this procedure to configure the timeslot service state when issuing circuit blocks. Use this feature can be used topreserve and restore a particular service state on a particular timeslot in the event of a power failure on the system.

*These commands only appear on the command line when the DSP multispan is configured for SS7 signaling. (****sigmode*** *must be set to* ***nosig*** *and* ***cfgss7mode*** *set to* ***enfas_slap****. Refer to the Total Control 1000 Enhanced Data System* Getting Started Guide *for SS7 configuration.)*

To use the CLI to configure the timeslot service state from the DSP multispan:

1 Access the appropriate span level. Enter the following command, and replace "x" with the desired span level (e.g., 1, 2, 3):

```
>chdev span x
```

The span level command prompt displays:

```
span1>
```

2 Access the appropriate timeslot channel. Enter the following command, and replace "x" with the desired timeslot level (0 - 31):

```
chdev tslot x
```

The timeslot level command prompt displays. For example:

```
span1/tslot10>
```

3 Use the following command at the timeslot level to configure the service state of an individual timeslot:

```
span1/tslot10> set sstate <timeslot service state>
```

Table 16 lists available parameters for this command.

Table 16 Timeslot Service States

Parameter	Description
is	In service. Default.
oos	Local out of service.
inb	Inbound blocked.
outb	Outbound blocked.

If you fail to save this feature to NVRAM, configuration settings are lost when the card reboots.

4 Save the span configuration by entering the following command:

```
cmd svspcfg
```

5 SDH STM-0 AND DS-3 CARD

This chapter provides information and procedures related to maintaining the SDH STM-0 card.

This chapter contains the following topics:

For more information on how to configure the SDH STM-0 card using the CLI, refer to the Modem and Span Command Line Interface Reference.

Monitoring SDH Performance Statistics

Total control manager's Performance Monitor allows you to view specific SDH STM-0 statistics.

From total control manager, you can monitor four types of statistics relating to the SDH STM-0 module:

- SDH line level statistics
- SDH High Path (AU) level statistics
- SDH Low Path (TU) level statistics
- DS-3 level statistics

Monitoring Line Level Statistics

To view SDH STM-0 card-level performance statistics:

1. From total control manager's VFPD, click the SDH STM-0 NAC.

   The selected card turns blue. To select LEDs on both SDH STM-0 NACs, hold down **Shift** while clicking.

2. From the Performance menu, click **Session Monitor**.

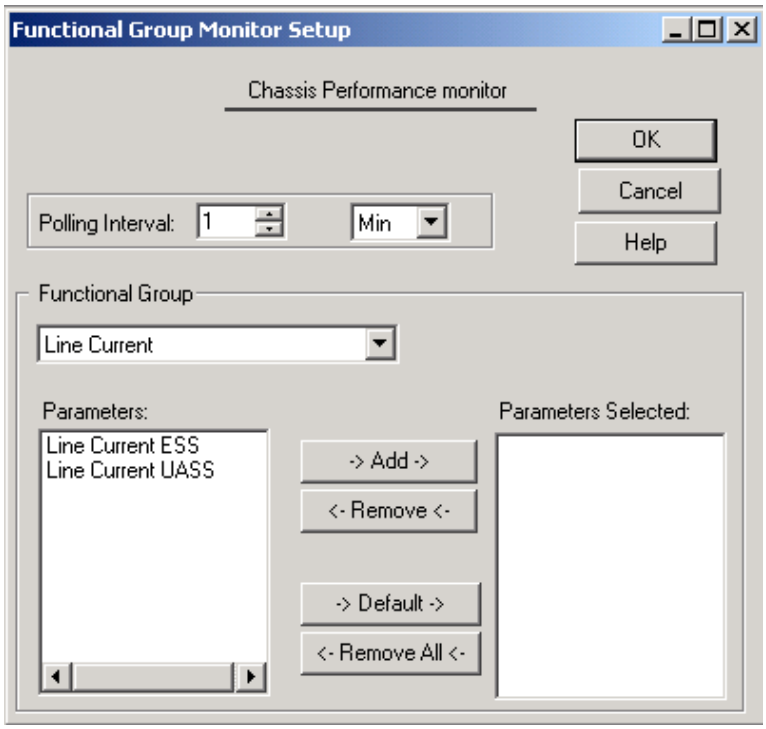
   The Select Spans window appears.

3. Select **SDH LINE LEVEL**.

4. Click **OK**.

The Functional Group Monitor Setup window appears.

Figure 28 Functional Group Monitor Setup Window



5 From the Functional Group drop-down menu, click the functional group that you would like to view statistics for.

The individual statistics that comprise the selected Functional Group are listed in the **Parameters** box.

6 Click the individual statistics you want to view from the Parameters box and click **Add**.

All of the statistics can be selected by clicking **Default**.

The statistics you select appear in the **Parameters Selected** box. Selections may be deleted by clicking either **Remove** or **Remove All**.

Optional: *Change the polling rate by increasing or decreasing the value for the* ***Polling Interval*** *setting. The default polling rate is one minute.*

7 Click **OK** when finished.

The Performance Monitor begins.

Monitoring SDH Line High Path (AU) Statistics

To view SDH Line High Path (AU) performance statistics:

1 From total control manager's VFPD, click the SDH STM-0 NAC.

The selected card turns blue. To select LEDs on both SDH STM-0 NACs, hold down **Shift** while clicking.

2 From the Performance menu, click **Session Monitor**.

The Select Spans window appears.

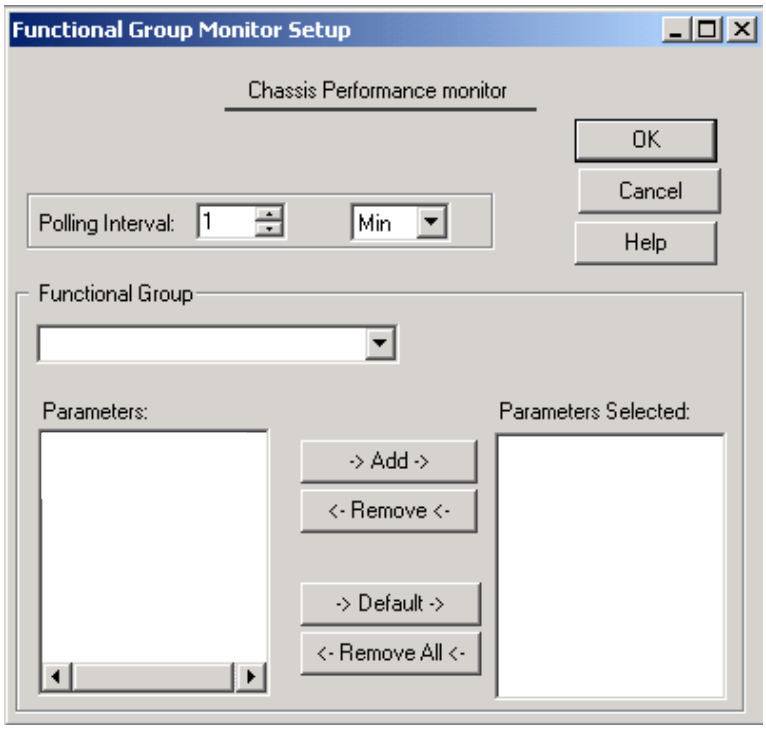
3 Select **SDH Line AU Level**.

4 Select the appropriate SDH High Path by clicking the respective field. You can select up to three high paths.

5 Click **OK**.

The Functional Group Monitor Setup window appears.

Figure 29 Functional Group Monitor Setup Window



6 From the Functional Group drop-down menu, click the functional group that you would like to view statistics for.

The individual statistics that comprise the selected Functional Group are listed in the **Parameters** box.

7 Click the individual statistics you want to view from the Parameters box and click **Add**.

All of the statistics can be selected by clicking **Default**.

The statistics you select appear in the **Parameters Selected** box. Selections may be deleted by clicking either **Remove** or **Remove All**.

Optional: *Change the polling rate by increasing or decreasing the value for the* ***Polling Interval*** *setting. The default polling rate is one minute.*

8 Click **OK** when finished.

The Performance Monitor begins.

Monitoring Line Low Path (TU) Statistics

To view SDH Low Path (TU) performance statistics:

1 From total control manager's VFPD, click the SDH STM-0 NAC.

The selected card turns blue. To select LEDs on both SDH STM-0 NACs, hold down **Shift** while clicking.

2 From the Performance menu, click **Session Monitor**.

The Select Spans window appears.

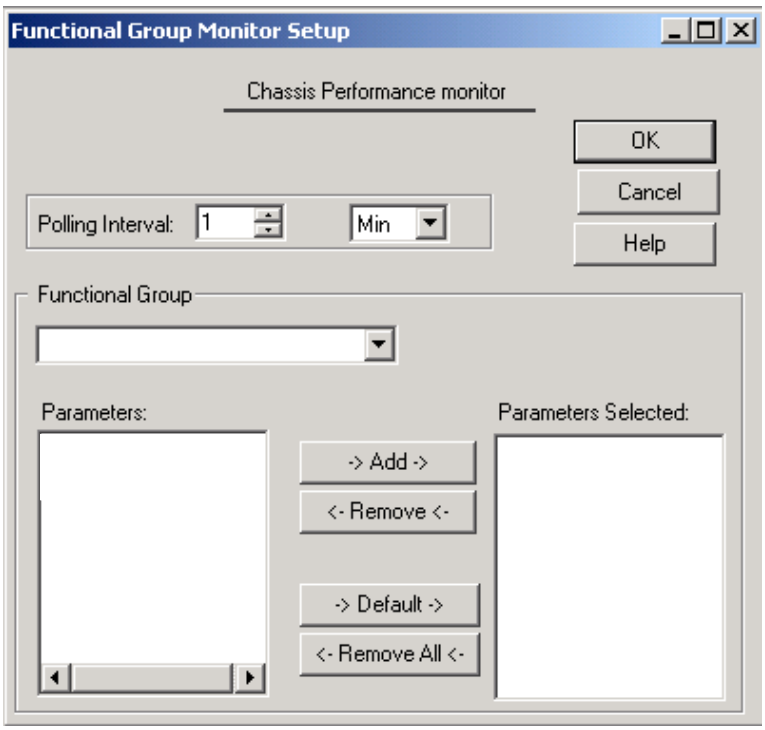
3 Select **SDH Line TU Level**.

4 Select the appropriate SDH Low Path by clicking the respective field.

5 Click **OK**.

The Functional Group Monitor Setup window appears.

Figure 30 Functional Group Monitor Setup Window



6 From the Functional Group drop-down menu, click the functional group that you would like to view statistics for.

The individual statistics that comprise the selected Functional Group are listed in the **Parameters** box.

7 Click the individual statistics you want to view from the Parameters box and click **Add**.

All of the statistics can be selected by clicking **Default**.

The statistics you select appear in the **Parameters Selected** box. Selections may be deleted by clicking either **Remove** or **Remove All**.

Optional: *Change the polling rate by increasing or decreasing the value for the* ***Polling Interval*** *setting. The default polling rate is one minute.*

8 Click **OK** when finished.

The Performance Monitor begins.

Monitoring DS-3 Level Statistics

To view DS-3 level performance statistics:

Use this procedure for monitoring DS-3 line level statistics relating to the SDH STM-0-DS-3 conversion process. For configuration information on monitoring DS-3 Ingress card and DS-3 span level statistics, refer to the Operations Guide.

1 From total control manager's VFPD, click the SDH STM-0 NAC.

The selected card turns blue. To select LEDs on both SDH STM-0 NACs, hold down **Shift** while clicking.

2 From the Performance menu, click **Session Monitor**.

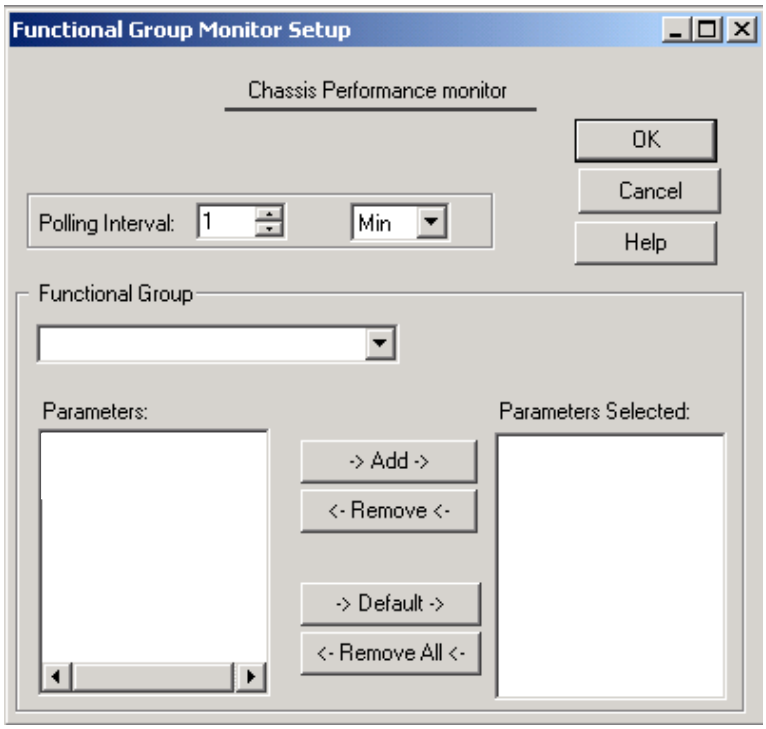
The Select Spans window appears.

3 Select **DS3**.

4 Click **OK**.

The Functional Group Monitor Setup window appears.

Figure 31 Functional Group Monitor Setup Window



5 From the Functional Group drop-down menu, click the functional group that you would like to view statistics for.

The individual statistics that comprise the selected Functional Group are listed in the **Parameters** box.

6 Click the individual statistics you want to view from the Parameters box and click **Add**.

All of the statistics can be selected by clicking **Default**.

The statistics you select appear in the **Parameters Selected** box. Selections may be deleted by clicking either **Remove** or **Remove All**.

Optional: *Change the polling rate by increasing or decreasing the value for the* ***Polling Interval*** *setting. The default polling rate is one minute.*

7 Click **OK** when finished.

The Performance Monitor begins.

Issuing Commands to the SDH STM-0 Module

The SDH STM-0 module categorizes commands in two ways:

- Software Commands issued to the SDH STM-0 NAC
- Hardware Commands issued to the SDH STM-0 NAC

Performing SDH STM-0 Software Commands

To perform a software command on the SDH STM-0 NAC, follow these steps:

1. From total control manager's VFPD, click the SDH STM-0 NAC.

   The SDH STM-0 NAC turns blue.

2. From the Configuration menu, click **Actions/Commands**.

   The total control manager Commands window appears

3. From the first Command to Execute drop-down menu, click **Hardware**.

4. From the second Command to Execute drop-down menu, select the software action you would like to perform.

   Table 17 lists the action descriptions for the software commands.

   Table 17 SDH STM-0 Software Commands

Software Command	Description
No Command	Normal Operation
Save to NVRAM	Allows you to save SDH STM-0 module configurations. No changes to the SDH STM-0 module are needed in an SDH 1.0 chassis configuration.
Restore from Default	Restores SDH STM-0 module configurations to factory default configurations.
Restore from NVRAM	Restores SDH STM-0 module configurations to the last saved configuration.
Software Reset	The SDH STM-0 NAC software resets, but the SDH STM-0 NAC hardware does not reset. Any active calls are dropped when this command is issued.
Restore UI Password From Default	Restores User Interface (Command Line Interface) password to the factory default setting.

5. Click **Execute**.

   The status of the executed command appears in the **Command Status** box.

6. Click **Close** when the operation has been completed successfully.

Performing SDH STM-0 Hardware Commands

To perform a hardware command on the SDH STM-0 NAC, follow these steps:

1. From total control manager's VFPD, click the SDH STM-0 NAC.

   The SDH STM-0 NAC turns blue.

2. From the Configuration menu, click **Actions/Commands**.

   The total control manager Commands window appears.

3. From the first Command to Execute drop-down menu, click **Software**.

4. From the second Command to Execute drop-down menu, select the software action you would like to perform.

Table 18 lists the action descriptions for the hardware commands.

Table 18 SDH STM-0 Hardware Commands

Hardware Command	Description
Hardware No Command	Normal Operation.
Remove from Service	Disables the SDH STM-0 NAC. The SDH STM-0 module cannot process calls in this stage. The card will turn yellow in total control manager as a warning.
Restore to Service	Restores the SDH STM-0 NAC to a usable state.
Hardware Reset	Reboots the SDH STM-0 NAC hardware.

5 Click **Execute**.

The status of the executed command appears in the **Command Status** box.

6 Click **Close** when the operation has been completed successfully.

Removing an Active SDH STM-0

Use this procedure to remove an active SDH STM-0 Network Access card (NAC) for maintenance purposes. You can do this through the common element manager, total control manager, or the Command Line Interface (CLI).

Common Element Manager

To remove and active SDH STM-0 card using common element manager:

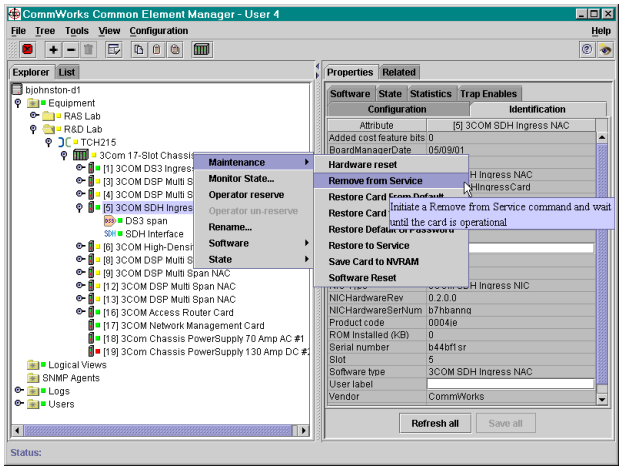
1 From the Explorer tab, right-click the item you want to monitor.

2 Select **Maintenance** from the pop-up menu.

3 Select **Remove** from Service from the pop-up menu.

Figure 32 shows the pop-up menu.

Figure 32 Removing an SDH Card from Service



A dialog box appears and lists the progress of the command. When the command has executed, the **Working** icon changes to a **Finished** icon.

4 Click **Close**.

Total Control Manager

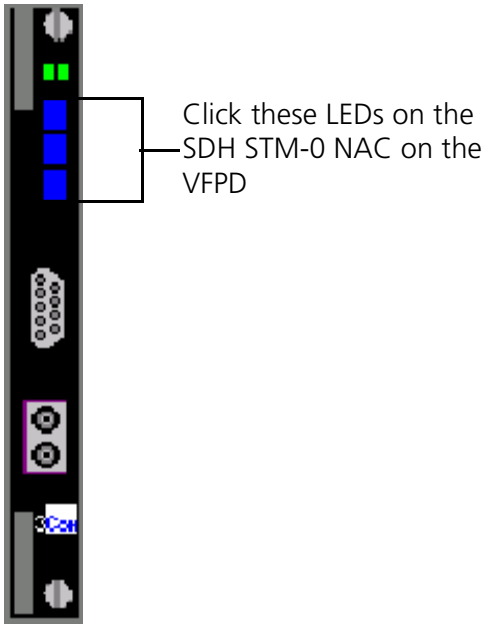
To remove an active SDH STM-0 NAC through total control manager, use the following procedure:

Releasing Both SDH STM-0 NACs

1 From the total control manager Virtual Front Panel Display (VFPD), click the LEDs of the active SDH STM-0 NAC.

The LEDs turn blue.

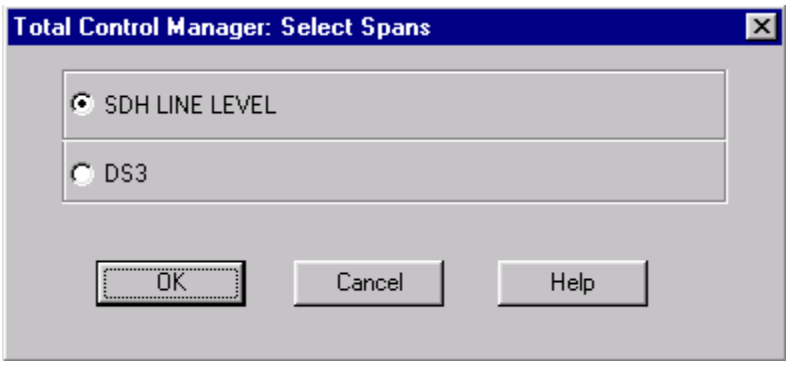
Figure 33 Total Control Manager's Virtual Front Panel Display (VFPD)



2 From the Configure menu, click **Programmed Settings**.

The Select Spans window appears.

Figure 34 Selecting Spans Window



3 Select **SDH LINE LEVEL**.

4 Click **OK**.

The SDH card Programmed Settings window appears.

5 From the Parameter Group drop-down menu, click **General**.

The current general programmed settings for the SDH Line Level appear.

6 From the **Service Cmd Force** field, select **fsSwitchRelease**.

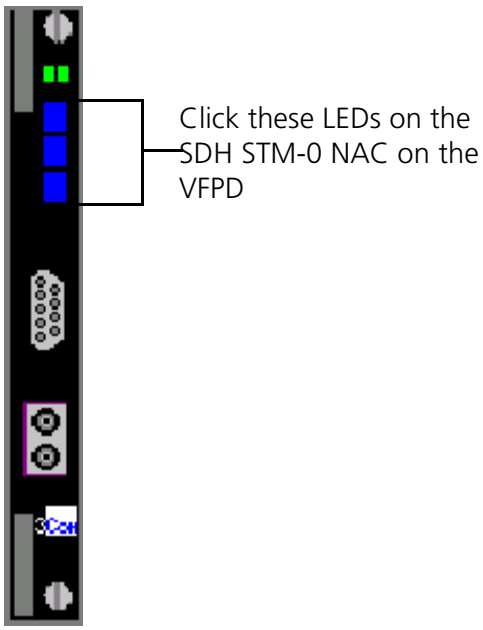
7 Click **Set**.

8 Click **OK**.

9 From the total control manager VFPD, click the LEDs of the standby SDH STM-0 NAC.

The LEDs turn blue.

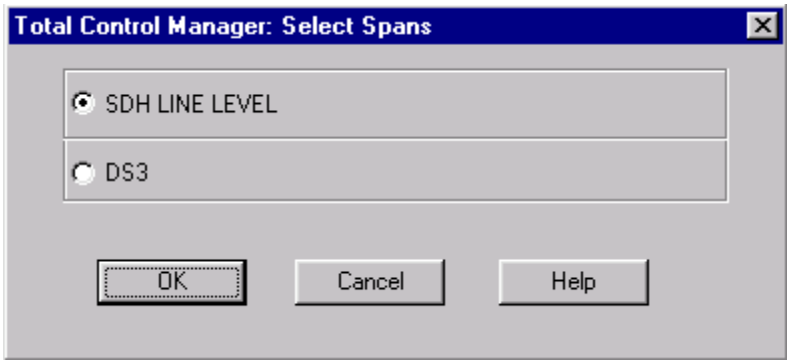
Figure 35 Total Control Manager's Virtual Front Panel Display (VFPD)



10 From the Configure menu, click **Programmed Settings**.

The Select Spans window appears.

Figure 36 Selecting Spans Window



11 Select **SDH LINE LEVEL**.

12 Click **OK**.

The SDH card Programmed Settings window appears.

13 From the Parameter Group drop-down menu, click **General**.

The current general programmed settings for the SDH Line Level appear.

14 From the **Service Cmd Force** field, select **fsSwitchRelease**.

15 Click **Set**.

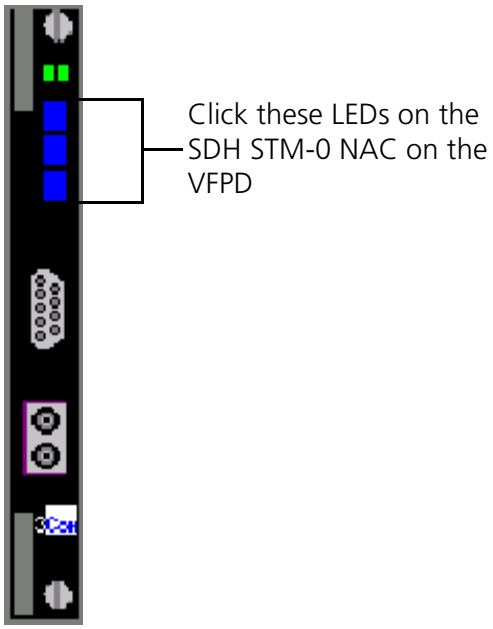
16 Click **OK**.

Switching the Active Card to Standby

1 From the total control manager VFPD, click the LEDs of the active SDH STM-0 NAC.

The LEDs turn blue.

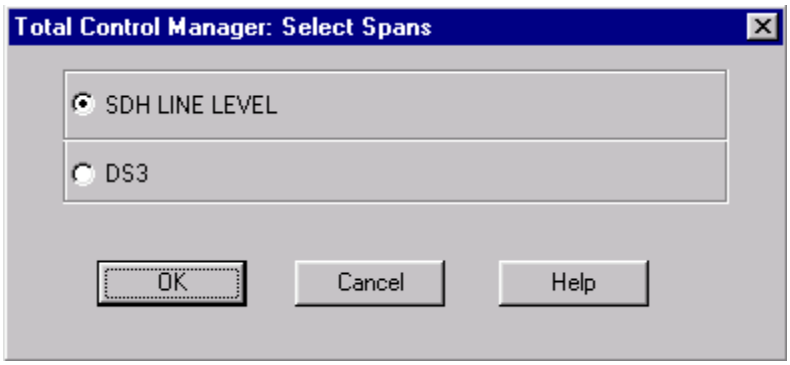
Figure 37 Total Control Manager's Virtual Front Panel Display (VFPD)



2 From the Configure menu, click **Programmed Settings**.

The Select Spans window appears.

Figure 38 Selecting Spans Window



3 Select **SDH LINE LEVEL**.

4 Click **OK**.

The SDH card Programmed Settings window appears.

5 From the Parameter Group drop-down menu, click **General**.

The current general programmed settings for the SDH Line Level appear.

6 From the **Service Cmd Force** field, select **cnvSby**.

7 Click **Set**.

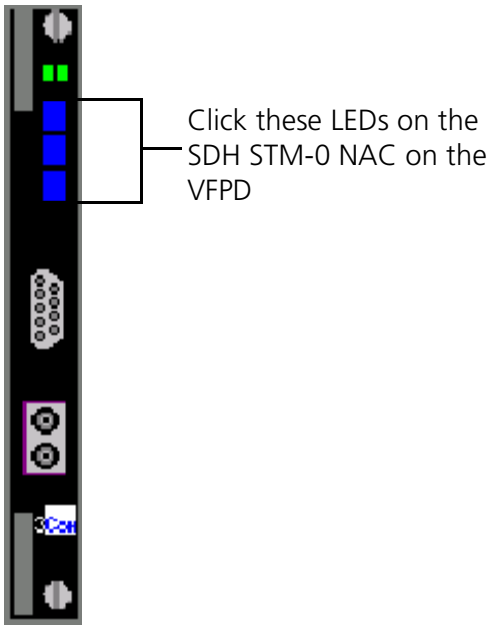
The active SDH STM-0 NAC is now the standby card.

Bringing the Standby Card Out of Service

1 From the Total Control Manger VFPD, click the LEDs of the SDH STM-0 NAC.

The LEDs turn blue.

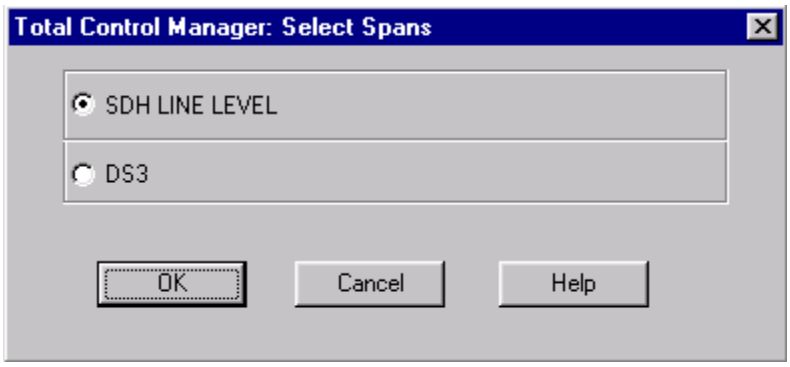
Figure 39 Total Control Manager's Virtual Front Panel Display (VFPD)



2 From the Configure menu, click **Programmed Settings**.

The Select Spans window appears.

Figure 40 Selecting Spans Window



3 Select **SDH LINE LEVEL**.

4 Click **OK**.

The SDH card Programmed Settings window appears.

5 From the Parameter Group drop-down menu, click **General**.

The current general programmed settings for the SDH Line Level appear.

6 From the **Card Operation Mode** field, select **cnvOus**.

7 Click **Set**.

8 Click **OK**.

9 Monitor the standby module. Once the ACT/SBY LED turns red, remove the SDH STM-0 NAC from the chassis.

Command Line Interface

To remove an active SDH STM-0 NAC through the CLI, use the following procedure:

Before removing an active SDH STM-0 NAC through the CLI, you must establish a console connection with both SDH STM-0 modules. Please refer to Modem and Span Command Line Interface Reference for detailed instructions on configuring a CLI connection.

Releasing Both SDH STM-0 NACs

1 Establish a CLI connection to the active SDH STM-0 NAC.

2 Enter the following command from a supported software application (e.g., HyperTerminal):

```
chdev sdh
```

The sdh command prompt appears:

```
sdh>
```

3 Enter the following command:

```
set sorder release
```

4 Establish a CLI connection with the standby SDH STM-0 NAC.

5 Enter the following command:

```
chdev sdh
```

The sdh command prompt appears:

```
sdh>
```

6 Enter the following command:

```
set sorder release
```

Switching the Active Card to Standby

1 Establish a CLI connection with the active SDH STM-0 NAC.

2 Enter the following command from a supported software application (e.g., HyperTerminal):

```
chdev sdh
```

The sdh command prompt appears:

```
sdh>
```

3 Enter the following command:

```
set sorder switch
```

The active SDH STM-0 NAC is now the standby card.

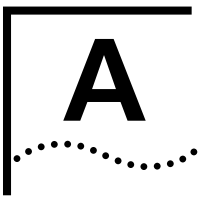
Bringing the Standby Card Out of Service

1 Enter the following command from the sdh level command prompt (sdh>):

```
set opmode ous
```

The standby SDH STM-0 card is out of service.

2 Monitor the standby SDH STM-0 module. Once the ACT/SBY LED turns red, remove the SDH STM-0 NAC from the chassis.



ACRONYMS

This appendix lists acronyms used in the CommWorks Total Control 1000 Enhanced Data System application and documentation.

ABR Area Border Router

ACT Active

AH Authentication Header

AIS Alarm Indication Signal

ANI Automatic Number Identification

APS Automatic Protection Switching

ARC Access Router Card

ARP Address Resolution Protocol

ARQ Automatic Retransmission reQuest

AS Autonomous System

ASBR Autonomous System Boundary Router

ASE Autonomous System External

ATM Asynchronous Transfer Mode

AU High Path

AVP Attribute Value Pair

BACP Bandwidth Allocation Control Protocol

BAP Bandwidth Allocation Protocol

BBS Bulletin Board Systems

Bc Committed Burst Size

BDR Backup Designated Router

Be Excess Burst Size

BECN Backward Explicit Congestion Notification

BERT Bit Error Rate Testing

BLER Block Errors

Bootp Bootstrap Protocol

CBCP Callback Control Protocol

CDR Call Detail Records

CEM Common Element Manager

CHAP Challenge-Handshake Authentication Protocol

CIP Call Information Process

CIR Committed Information Rate

CLI Command Line Interface

CRC Cyclic Redundancy Check

CSU/DSU Channel Service Unit/Digital Service Unit

CTS Clear To Send

DS-1 Digital Signal, level 1

DS-3 Digital Signal, level 3

DES Data Encryption Standard

DHCP Dynamic Host Configuration Protocol

DHTML Dynamic HyperText Markup Language

DLCI Data Link Connection Identifier

DLL Data Link Layer

DNIS Dialed Number Identification Service

DNS Domain Name Server

DPCM Differential Pulse Code Modulation

DR Designated Router

DSA Dynamic Slot Assignment

DSP Digital Signal Processor

DTE Data Terminal Equipment

DTR Data Terminal Ready

DTS Data Transformation Services

EEPROM Electronically Erasable Programmable Read Only Memory

ESD Electrostatic Discharge

ENFAS Enhanced Network Facility Associated Signaling

EO End Office

ESIG Extended SIGnaling

ESP Encapsulating Security Payload

EXZ Excessive Zeros

FEAC Far End Alarm and Control Channel

FEBE Far End Block Errors

FECN Forward Explicit Congestion Notification

FQ	Fair Queuing
FRED	Fair Random Early Drop
GMT	Greenwich Mean Time
GSTN	General Switched Telephone Network
HDLC	High level Data Link Control
HiPer	High Performance (CommWorks name for Total Control 1000 components not compatible with SDH 1.0)
ICMP	Internet Control Message Protocol
IEA	Internet Equal Access
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGMP	Internet Group Management Protocol
INS	In Service
IP	Internet Protocol
IPX	Internetwork Packet eXchange
ISAKMP	Internet Security Association and Key Management Protocol
ISDN	Integrated Services Digital Network
ISP	Internet Service Provider
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LAN	Local Area Network

LAPM Link Access Procedure for Modems

LCV Line Code Violation

LED Light Emitting Diode

LIU Line Interface Unit

LMI Link Management Interface

LNS L2TP Tunnel Server

LOF Loss of Frame

LOS Loss of Signal

LSA Link State Advertisements

LSDB Link State Database

MAC address Media Access Control address

MBP Management Bus Protocol

Mbps MegaBits Per Second; million bits per second

MD5 Message Digest 5

MIB Management Information Base

MNP Microcom Networking Protocol

MPIP Multilink PPP Interspan Protocol

MPPE Microsoft Point-to-Point Encryption

MPPP Multilink Point-to-Point Protocol

MTBF Mean Time Between Failure

MTU Maximum Transmission Unit

MU Monitoring Unit

NAC Network Application Card

NAS Network Application Server

NAT Network Address Translation

NBMA Non-Broadcast Multi-Access

NIC Network Interface Card

NMC Network Management Card

NTP Network Time Protocol

NVRAM Non-Volatile Random Access Memory

OC-1 Optical Carrier, level 1, 52 Mbps

OC-3 Optical Carrier, level 3, 155 Mbps

OOS Out of Service (alternative acronym)'

OSPF Open Shortest Path First

OUS Out of Service

PAP Password Authentication Protocol

PAT Port and Network Address Translation

PCI Peripheral Component Interconnection

PCM Pulse Code Modulation

PDH Plesiochronous Digital Hierarchy

PM Performance Monitor

POP Point Of Presence

POST Power-on Self-test

PPP Point-to-Point Protocol

PPoE Point-to-Point Protocol over Ethernet

PPTP Point-to-Point Tunneling Protocol

PQ Priority Queuing

PSI Power Supply Interfaces

PSTN Public Switched Telephone Network

PSU Power Supply Unit

PTMPT Point-to-Multipoint

PVC Permanent Virtual Circuit

QoS Quality of Service

RADIUS Remote Authentication Dial-In User Service

RAI Remote Alarm Indication

RAM Random Access Memory

RAS Remote Access Server

RFA Remote Frame Alarm

RIP Routing Information Protocol

RN/FL Run/Fail

ROM Read Only Memory

RRA Return Route Assurance

RSHD Remote Shell Daemon

RTP Real Time Protocol

RTS Request To Send

RX Receive

SDH Synchronous Digital Hierarchy

STM-0 Synchronous Transport Module, level 0

STM-1 Synchronous Transport Module, level 1

SABME Set Asynchronous Balance Mode Extended

SAP Service Advertising Protocol

SBY Standby

SDH Synchronous Digital Hierarchy

SDL-2 Software Download-2

SHA Secure Hash Algorithm

SLAP Signaling LAN Application Protocol

SLIP Serial Line Internet Protocol

SNMP Simple Network Management Protocol

SONET Synchronous Optical Network

SS7 Signaling System 7

TCH Total Control Hub (an alternative name for the Total Control 1000 chassis)

TCP Transmission Control Protocol

TDM Time Division Multiplex

TFTP Trivial File Transfer Protocol

TTL Time-to-Live

TX Transmit

TU Tributary Unit; Low Path

UDP User Datagram Protocol

UI User Interface

VC-11 Virtual Container, number 11

VFPD Virtual Front Panel Display; Total Control Manager's graphical user interface

VLSM Variable Length Subnet Masks

VPN Virtual Private Network

VSA Vendor-Specific Attributes

VTP Virtual Terminal Protocol

WAN Wide Area Network

INDEX

CommWorks
a 3Com company

CommWorks Corporation
3800 Golf Road
Rolling Meadows, IL 60008

Part Number 10048391