CommWorks
a 3Com company

Total Control® 1000 Enhanced Data System

Trouble Locating and Clearing Guide
Release 4.5
Part Number 10048400

CommWorks
a 3Com company

Total Control® 1000 Enhanced Data System

Trouble Locating and Clearing Guide
Release 4.5
Part Number 10048400

CONTENTS

6 DS-3 Ingress Trouble Locating and Clearing

7 SDH STM-0 Converter Trouble Locating and Clearing

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 the various components of the CommWorks Total Control® 1000 Enhanced Data System and how they work together to build a communications platform for integrating local and wide area networks.

This guide is intended for network administrators or engineers who will be installing and configuring the Total Control 1000 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 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 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

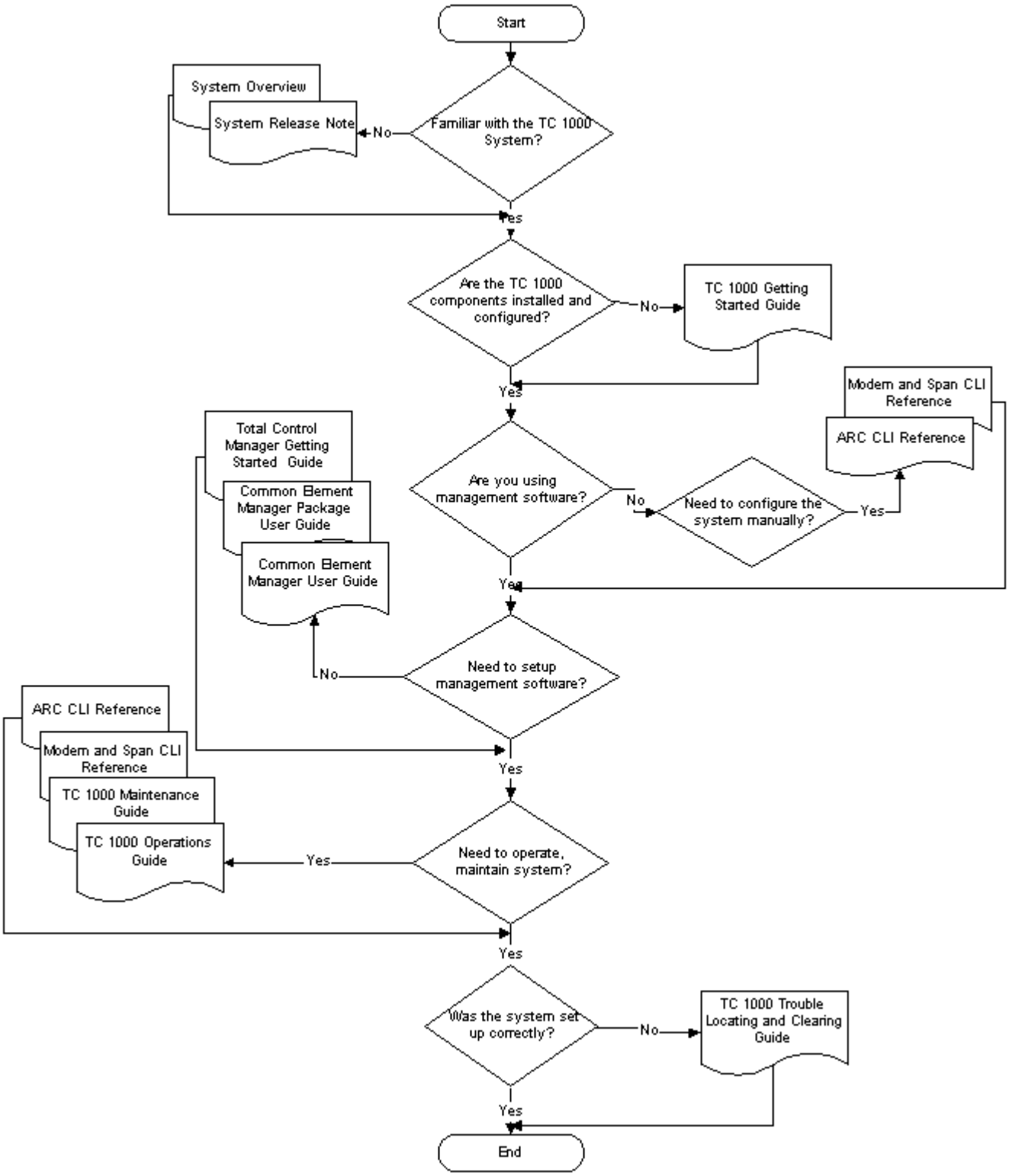
Total Control HiPer System

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
- Trouble locating and clearing attempts

1 TROUBLE LOCATING AND CLEARING OVERVIEW

This chapter includes information and resources useful for general trouble locating and clearing.

This chapter contains the following topics:

Trouble Locating and Clearing Total Control 1000 Products

You can configure and manage the Total Control® 1000 Enhanced Data System using the CLI to access the different cards locally or remotely.

You can also use an SNMP MIB browser or one of CommWorks' management software programs, total control manager or common element manager, to configure and manage your chassis.

CommWorks® 5115 common element manager is recommended for most functions. Refer to the CommWorks 5115 Common Element Manager *User's Guide*, included with this documentation set, for more information.

Knowledgebase Overview

Knowledgebase is an online database of technical information to help you diagnose and solve installation, upgrade and configuration problems with 3Com products.

For additional information, see the Knowledgebase web site at: *http://knowledgebase.3com.com*. Troubleshoot your product with 3Com Knowledgebase, an interactive tool containing thousands of technical solutions compiled by 3Com support engineers around the globe.

TotalService Overview

Use our support website—*http://TOTALSERVICE.commworks.com/*—for all your questions regarding support for all our products. You can download the latest software build, view the current product documentation, track a current part shipment, or view warranty and product repair information from this website.

2 Power Supply Unit and Interface Trouble Locating and Clearing

This chapter describes trouble locating and clearing information regarding Power Supply Units (PSUs) and Power Supply Interfaces (PSIs).

This chapter contains the following topics:

Overview

The Total Control 1000 system uses PSUs and PSIs to provide electricity to the chassis.

A few important compatibility issues regarding PSU/PSI card sets:

- For Total Control 1000 chassis, PSUs are available for AC or DC power, and in two power ratings, 70A and 130A.
- 35A and 45A PSUs are not compatible with this release.
- One 130A PSU can supply a fully loaded chassis. However, a second PSU is recommended for redundancy.
- Cannot use one AC PSU and one DC PSU in the same chassis.
- Cannot use PSUs with different ratings in the same chassis.
- PSUs are hot-swappable (assuming that two are installed and operable within the same chassis).

Power Failure Diagnostics

PSU failure may be caused by any of the following conditions:

- Input voltage failure
- Internal power supply fuse failure
- Internal power supply failure
- Input voltage out of specification (for example, too low)

Total Control 1000 power supply units are fully short-circuit protected. If there is a current overload sensed at the power supply output terminals, the power supply automatically shuts down until the fault is corrected. Once it is corrected, the power supply automatically comes back on.

If a PSU/PSI RUN/FAIL LED is red, try the following brief sequence of tests. Depending on the situation, these procedures should enable you to diagnose the cause of the problem.

Refer to the Getting Started Guide *for more information, including installation procedures, about the PSU/PSI card set.*

Power Supply Overvoltage

If overvoltage is sensed at the output terminals, the power supply immediately shuts down.

1 Remove the PSU and PSI whose LED is flashing by following the procedures in Removing Power Supply Units and Removing Power Supply Interfaces. Then, plug them in again to recycle the power.

WARNING: *Be careful to observe the warnings in that section about shock hazards and touching hot components.*

2 Reinsert the unit and check the RUN/FAIL indicator on the PSU front panel and/or PSI rear panel.

The problem may have been minor, and the unit may reset. If not, completely remove the faulty PSU/PSI and contact CommWorks Customer Service.

Overload Conditions

Check for a modem or interface unit failure that may be causing an overload condition. Remove each modem and NIC one at a time, until the power supply indicator LED lights. The last modem or interface unit removed is probably the cause of the overload condition.

Removing Power Supply Units

To remove PSUs from the Total Control 1000:

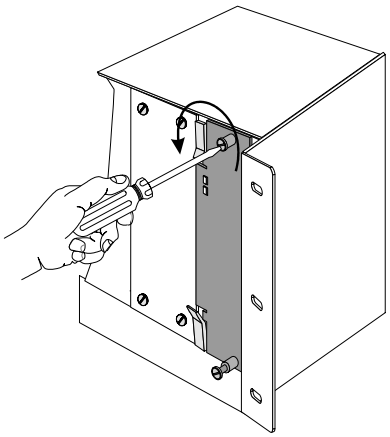
ESD: *To reduce the risk of electrostatic discharge (ESD), take proper grounding precautions before handling the PSU.*

1 Remove the PSI corresponding to the PSU being removed according the *Removing Power Supply Interfaces* section of this chapter.

WARNING: *Wait 10 seconds after power has been removed from the PSU/PSI set to allow all capacitors on the cards discharge. Do not touch the PSI/PSU during this period. After 10 seconds the Run/Fail (RN/FL) LED turns off and the PSU can be removed. Some components may still be very hot. Use caution when handling the PSI.*

2 Use a flat-head screwdriver to loosen the screws on the rear panel of the PSU.

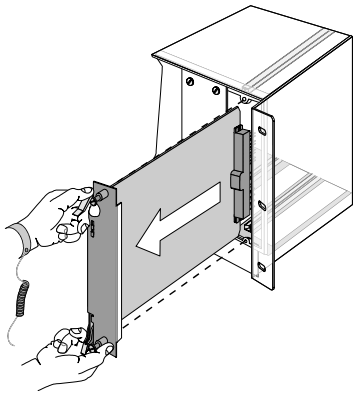
Figure 2 Loosening the Screws on the PSU



3 Lift the ejector tabs at the top and bottom of the PSU's front panel.

4 Slide the PSU out of the chassis.

Figure 3 Sliding the PSU



Removing Power Supply Interfaces

To remove PSIs from the Total Control 1000 chassis:

ESD: *To reduce the risk of electrostatic discharge (ESD), take proper grounding precautions before handling the PSI.*

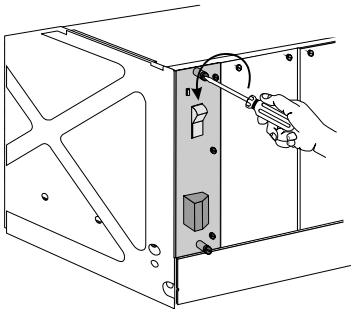
1 Turn off the power source.

2 Turn the power switch of the PSI being removed to the off (0) position.

WARNING: *Wait 10 seconds to allow all capacitors on the PSI to discharge. Do not touch the PSI during this period. After 10 seconds the Run/Fail (RN/FL) LED turns off and the PSI can be removed. Some components may still be very hot. Use caution when handling the PSI.*

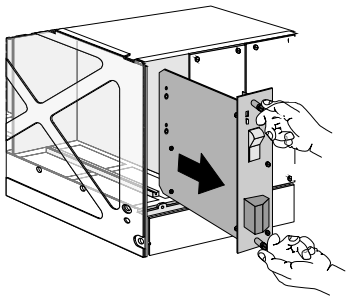
3 Use a flat-head screwdriver to loosen the screws on the rear panel of the PSI.

Figure 4 Loosening the Screws of the PSI



4 Grasp the screws and pull the PSI towards you.

Figure 5 Removing the PSI



5 Detach the power cables from the PSI.

6 Remove the PSU corresponding to the PSI being removed according to the instructions in the *Removing Power Supply Units* section of this chapter.

3 Access Router Card and HiPer ARC Trouble Locating and Clearing

This chapter contains trouble locating and clearing information relating to the access router card Network Application Card (NAC).

This chapter contains the following topics:

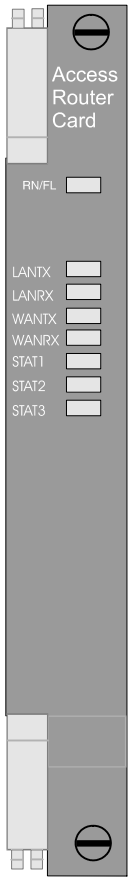
Overview

The access router card is a multi-protocol, dial-up router and terminal server commonly described as a remote access server. It is a software-based router for incoming call traffic terminated on Digital Signal Processor (DSP) multispan Network Application Cards (NACs). Access router cards receive incoming traffic from DSP multispan cards, encrypt the information and forward this traffic on to various egress ports.

Access Router Card NAC Faceplate

Figure 6 shows the Light Emitting Diodes (LEDs) on the access router card faceplate.

Figure 6 Access Router Card NAC Faceplate



Run/Fail LED

The Run/Fail (RN/FL) LED lets you know if the card is functioning properly. Table 3 lists what the Run/Fail LEDs signify during normal operation, except during start-up tests and software downloads.

Table 3 Access Router Card Run/Fail LED During Normal Operation

LED	Description
Off	Power off
Green	Power On
Red	Critical Failure

During start-up tests and software downloads *only*, the Run/Fail LED cycles through several colors as described in Table 4.

Table 4 Run/Fail LED During Start-up Tests and Software Downloads

LED	Description
Red	During start-up Power On Self Test (POST)
Amber (flashing slowly)	Checking for software download
Green (flashing rapidly)	Loading an application into RAM
Green	Power cycle is finished and card is operational

LAN TX LED The LAN TX LED indicates packets are being transmitted through the LAN (Ethernet) interface.

Table 5 Access Router Card LAN TX LED Description

LED	Description
Red	Interface failure
Red (flashing)	Collision (one flash per error)
Amber (flashing)	Multiple collisions, network busy
Off	Idle

LAN RX LED The LAN RX LED indicates packets are being received from the LAN (Ethernet) interface.

Table 6 Access Router Card LAN RX LED Description

LED	Meaning
Red	Interface failure
Red (flashing)	Collision error
Green	Receiving packet
Off	Idle

WAN TX LED The WAN TX LED indicates packets are being transmitted through the WAN interface using WAN NICs, like the V.35 and Quad T1/E1 NIC.

WAN RX LED The WAN RX LED indicates packets are being received from the WAN interface using WAN NICs, like the V.35 and Quad T1/E1 NIC.

STAT LEDs The front panel LEDs labeled STAT1, STAT2 and STAT3 are not used at this time.

Verifying Software Version Numbers

Before you perform any trouble locating and clearing, ensure you are using the correct access router card software version. Check this version number with the published version number in the Total Control 1000 Enhanced Data System System 4.5 GA System Release Notes. You will need to know this number if you contact Commworks Technical Support.

Common Element Manager

To verify the access router card software version using common element manager:

1. From the Explorer tab, click the access router card.
2. From the Properties tab, click the **Identification** tab.
3. Check the **Version** field for the current software number.

Total Control Manager

To verify the access router card software version using total control manager:

1. From total control manager's Virtual Front Panel Display (VFPD), select the access router card.

   The card turns blue.
2. From the main menu, click **Configure** and then click **Programmed Settings**.

   The HiPer ARC Card Programmed Settings window appears.
3. From the Parameter Group drop-down menu, select **HiPer ARC Identification** to query data from the access router card.
4. Check the **Software Version** field for the current software version.

Command Line Interface

To verify the access router card software version using the CLI:

1. Access the access router card CLI.
2. From the access router card CLI, enter the following command:

   ```
   HiPer> _show version
   ```

   Figure 7 displays the CLI output for the access router card:

   Figure 7 Access Router Card Software Verification - Command Line Interface

No Calls Complete Through the Access Router Card

A call is defined as a session where PPP finishes Link Control Protocol (LCP) and the client is able to pass data. If the access router card is not completing calls check the following settings:

Checking the Access Router Card for Configuration Problems

To verify the configuration:

1 Check the Call Initiation Process (CIP) to show if the access router card is being presented with a call. Enter the **Show Events** Command to display CIP information.

Event messages are automatically displayed on a local console. Of all ICMP messages generated, only Received Destination Unreachable messages are logged to the console.

If the access router card is being presented with a call the following message will appear:

```
CIP: Call arrived request, id 16777391, was accepted on
interface slot:2/mod:1

CIP: An incoming call established request, id =
16777391, is received on if slot:2/mod:1

At 21:11:53, Facility "Call Initiation Process", Level
"COMMON": CIP: Detected PPP frame, state 1, line 398,
File ../../src/cip_xmt_rx.c
```

The first line indicates the modem is answering a call.

The second line indicates the modem is asking the access router card to answer the call.

The third line indicates that the call was answered and PPP was detected.

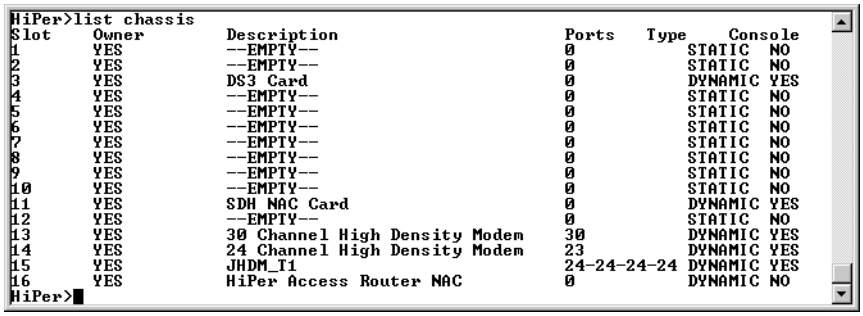
If one or two lines are present then there may be a problem with the modem's configuration.

2 If CIP indicates there are no calls being presented to the access router card, then the access router card may not be configured correctly and is unable to complete a call. To configure the card:

a Check to see if the access router card "owns" the modems when receiving the calls. Enter the **List Chassis** command to view the Chassis Table:

Figure 8 shows an example of a chassis table:

Figure 8 Access Router Card - List Chassis Command



```
HiPer>list chassis
Slot    Owner        Description                    Ports    Type     Console
1       YES          --EMPTY--                      0              STATIC  NO
2       YES          --EMPTY--                      0              STATIC  NO
3       YES          DS3 Card                       0              DYNAMIC YES
4       YES          --EMPTY--                      0              STATIC  NO
5       YES          --EMPTY--                      0              STATIC  NO
6       YES          --EMPTY--                      0              STATIC  NO
7       YES          --EMPTY--                      0              STATIC  NO
8       YES          --EMPTY--                      0              STATIC  NO
9       YES          --EMPTY--                      0              STATIC  NO
10      YES          --EMPTY--                      0              STATIC  NO
11      YES          SDH NAC Card                   0              DYNAMIC YES
12      YES          --EMPTY--                      0              STATIC  NO
13      YES          30 Channel High Density Modem  30             DYNAMIC YES
14      YES          24 Channel High Density Modem  23             DYNAMIC YES
15      YES          JHDM_T1                        24-24-24-24    DYNAMIC YES
16      YES          HiPer Access Router NAC        0              DYNAMIC NO
HiPer>
```

If this table is incorrect and only one access router card is in the Chassis, use the network management card chassis awareness to correct it:

a Type **Show NMC** to check if Chassis Awareness is enabled. If it is not enabled, enable it by typing **enable nmc chassis_awareness**

b Once chassis awareness is enabled, make sure you do not have any left over STATIC definitions by using the **List Chassis** command again.

c If you do, use the following command to set the card slot to empty:

```
1-16 OWNER YES CARD_TYPE EMPTY
```

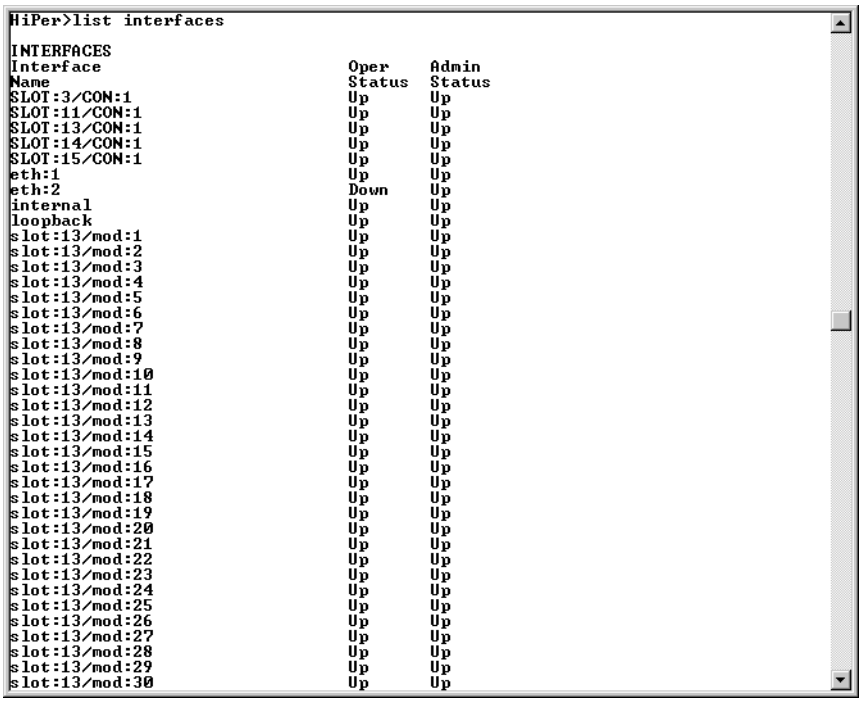
d Enter the **Save All** Command then reset the access router card.

e When the access router card finishes booting, enter the **List Chassis** command. The table should show all the correct cards with correct ownership.

3 If the card owner ship is correct and calls are still not being presented to the access router card, be sure the modem interfaces are enabled. To see the status of the interfaces, enter **List Interfaces**.

Figure 9 shows an example of an interface table:

Figure 9 Access Router Card - List Interfaces Command



```
HiPer>list interfaces

INTERFACES
Interface                       Oper    Admin
Name                            Status  Status
SLOT:3/CON:1                    Up      Up
SLOT:11/CON:1                   Up      Up
SLOT:13/CON:1                   Up      Up
SLOT:14/CON:1                   Up      Up
SLOT:15/CON:1                   Up      Up
eth:1                           Up      Up
eth:2                           Down    Up
internal                        Up      Up
loopback                        Up      Up
slot:13/mod:1                   Up      Up
slot:13/mod:2                   Up      Up
slot:13/mod:3                   Up      Up
slot:13/mod:4                   Up      Up
slot:13/mod:5                   Up      Up
slot:13/mod:6                   Up      Up
slot:13/mod:7                   Up      Up
slot:13/mod:8                   Up      Up
slot:13/mod:9                   Up      Up
slot:13/mod:10                  Up      Up
slot:13/mod:11                  Up      Up
slot:13/mod:12                  Up      Up
slot:13/mod:13                  Up      Up
slot:13/mod:14                  Up      Up
slot:13/mod:15                  Up      Up
slot:13/mod:16                  Up      Up
slot:13/mod:17                  Up      Up
slot:13/mod:18                  Up      Up
slot:13/mod:19                  Up      Up
slot:13/mod:20                  Up      Up
slot:13/mod:21                  Up      Up
slot:13/mod:22                  Up      Up
slot:13/mod:23                  Up      Up
slot:13/mod:24                  Up      Up
slot:13/mod:25                  Up      Up
slot:13/mod:26                  Up      Up
slot:13/mod:27                  Up      Up
slot:13/mod:28                  Up      Up
slot:13/mod:29                  Up      Up
slot:13/mod:30                  Up      Up
```

Operational Status indicates that the access router card has communication with the modem card. **Administrative Status** indicates the user-defined status of the interface. In order to take calls, the status must be **UP** for both.

a If the Operational Status is down for any interface then there is a packet bus problem. Check to see if the card is present in the slot and that its Run/Fail light is Green.

b If the Admin Status is down for any interface then modem is not enabled. To enable the modem type the following command:

`enable interface <interface name> slot:1/modem:x`

where x is 1-24 for T1 spans and 1 to 32 for E1 spans

Once the interface is configured and enabled, and all the cards belong to the access router card, the access router card is configured correctly to receive calls.

Checking the Access Router Card for Authentication Problems

If the access router card is configured correctly and is still unable to process calls correctly, it could be a problem with how it authenticates the call.

Check to see if the access router card is dropping the call during or after authentication, from the PPP monitor logs. The LCP authentication protocol should show complete. Either a PAP-ACK or CHAP-ACK will show this.

Call Fails Right After LCP Authentication

The PPP trace should not show any PAP/CHAP requests for this condition to be true. There may be no PPP trace if the client was using a clear text login

If the clients are attempting to use a scripted text login or use some other PPP stack that requires text instead of auto detecting PPP Configure the access router card for clear text logins:

1. It is possible to change the access router card to only allow PPP and no clear logins. If this is done, any client doing a clear login will not connect. Type the command **show interface slot:X/mod:y**. The output will contain a line like the following.

   ```
   Connection Type: NORMAL
   ```

   The default setting is "NORMAL", which will allow clear text login and PPP auto-detection.

2. If this is set to something other than "NORMAL", it can be change with the command **SET MODEM GROUP ALL CONNECTION_TYPE NORMAL**.

LCP Authentication Does Not Show Complete

If LCP authentication did not complete:

1. Check that the authentication server being used by the access router card is configured properly. Be sure the RADIUS server and the username and password are valid.
2. If the authentication server is configured correctly, check if the DNIS preauthentication feature is being used:
3. Enter **Show Interface Slot:x/mod:y** for the interface the failed call is arriving on. The following should be displayed:

   ```
   DNIS Authentication: ENABLED
   ```

   a. If DNIS preauth is not part of your configuration, type **SET MODEM GROUP ALL DNIS_AUTHENTICATION DISABLED**.

   b. If DNIS preauth is required, confirm that the other DNIS settings are correct. enter **SHOW INTERFACE SLOT:X/MOD:Y** to display the DNIS settings. DNIS preauthentication sends the client's phone number as the username and either a NULL password or a password that has been configured on the access router card to the AAA server. Correct any settings that are incorrect.

If RADIUS/TACACS are being used to validate the phone number information and the interfaces are properly configured for DNIS go to Step 4.

4 If DNIS is disabled or the settings are all correct, this would indicate that there is no simple configuration problem.

Examine the log files from your authentication server to help determine why the server "does not like" the request packet. The AUTH request from the access router card does not have many different configurations. You can remove the Vendor-Specific Attributes (VSAs) and ensure that all empty attributes are padded with 0s and not NULL. To do this type the following:

```
ENABLE RADIUS FILL_NULL_ATTRIBUTES

SET AUTHENTICATION VSA DISABLED
```

If changing these items fixes the problem, your server has no support for VSAs, it does not support NULL filled attributes, or both. Only the NULL issue can be addressed on the access router card. VSA support is a function of the RADIUS server.

If LCP Authentication Does Complete

If calls are dropping right after LCP converges:

1 Check if the time elapsed when each call drops. If all the calls drop after the same elapse time, make sure the cause is not an erroneous value for the time-outs.

2 If the time-out value is correct, check the PPP trace to see if the call fails after a CCP reset.

Some client's compression protocols are not interoperable with the access router card. One symptom of this is frequent CCP Resets found in the PPP traces. Excessive CCP resets will generally lead to a call drop. Turn off CCP on the access router card for that specific client to test the condition. Type **set ppp ccp_MODEMTYPE_ACCEPT NONE**.

Calls Fail After Authentication has Completed

If monitoring PPP during the LCP phase indicates that calls are failing after authentication has completed, check the following configurations:

1 Check the users defined service-type. The defined service-type could differ from the type of service the user is attempting to connect as.

The user having a RADIUS/TACACS definition that gives a service-type other than PPP, such as login would cause this. In this case the access router card would receive the authentication acknowledgement and see that the user is not allowed to do PPP, the result would be a dropped call.

This can be determined by checking the authentication server's configuration for that user, or monitoring the protocol. If RADIUS is being used, the access router card's RADIUS monitor will show the contents of the ACK packet.

TACACS must be captured by other means and decoded manually. There will also be syslog messages that indicate a service-type mismatch for that user.

a For PPP the service type in RADIUS should be "Framed" and the protocol is normally "PPP". (SLIP in some rare cases).

b If the users are local to the access router card, the user type should be "NETWORK" and the protocol either PPP or SLIP.

c Consult your RADIUS/TACACS vendor for specifics on authentication server setup that matches these requirements.

2 Check if there are IP addresses available. In either case the call will drop if the access router card cannot get an address to assign to the user.

A message similar to Figure 10 will be sent to syslog when this occurs:

Figure 10 SYSLOG Message - Access Router Card

```
At 19:32:58, Facility "IP", Level

"CRITICAL"::ip_fwd_get_opt: no IP address available
for

dynamic address assignment
```

Your calls are dropping due to missing IP pool or from running out of addresses:

a If you are using DHCP proxy, make sure your access router card has DHCP turned on, then check the DHCP server to ensure it has enough addresses to cover all available ports on the access router card.

b If you are using a locally configured IP Pool, check to see if one is present by using the command **LIST IP POOLS** the output should be similar to the output in Figure 11.

Figure 11 LIST IP POOLS - Access Router Card CLI Command

```
IP ADDRESS POOLS

Name                Address        Size InUse State
Route      Unused Status

pool1             207.24.79.200/C  5    0     PUBLIC
NO_AGGREGATE 0    ACTIVE
```

The size of the pool should be the same as the number of available modems for dial-in that this access router card is servicing. The state should be **PUBLIC**. It is possible to combine smaller pools from different networks to achieve the total size desired as long as all the pools are tagged as **PUBLIC**.

c To change the size of a pool use the command:

SET IP POOL <NAME> **SIZE** <SIZE>

d To add a pool use the following command to create a PUBLIC pool:

ADD IP POOL <NAME> **INITIAL_POOL_ADDRESSS** <START ADDRESS> **SIZE** <SIZE>

e If you are using PRIVATE pools (pool name is specified by the authentication server) make sure that the private pool exists and that it has enough addresses for all the users that may use it.

Refer to the Operations Guide for more information.

f If DHCP proxy is being used, use the command **SHOW DHCP_PROXY SETTINGS** to verify that the service is enabled. If it is not, the command **SET DHCP_PROXY ENABLED** will enable it. There are no other settings on the access router card required for DHCP proxy to work.

3 Check if there is a filter assigned and not defined. The access router card supports the use of packet filters. These filters may be assigned on a per user basis via the authentication protocol (RADIUS) or set on the modem interfaces. If either is done, but the filter has not been defined on the access router card the call will drop. This is a security feature.

The syslog will show this problem with the following messages.

Figure 12 SYSLOG Report

```
FM: Filter file std.ppp.in is not in the filter list,
filter not applied

At 19:42:51, Facility "IP", Level "CRITICAL":: IP,
FILTER_APPLY_RSP  failed

(ES_NULL_FUNC)
```

In this case the authentication protocol was assigning the filter “std.ppp.in” to the user, but that filter was not defined on the card.

a If the calls are dropping due to a filter being assigned to a user but not being present on the access router card. To see the filters configured use the command **LIST FILTERS**. If the users filter does not show up in the list, it must be added. The access router card supports two methods of adding filters,

- local edit
- TFTP filter file.

b After creating the file, use the command **ADD FILTER <FILE NAME>** to add the filter. If the syntax is correct the command completes with out error.

4 Check if the client is accepting the assigned IP address.

If the client is configured for a static IP address but the access router card is attempting to assign an address from a IP pool or a different static address from the user's profile the call will drop. The problem can be seen by observing the IPCP negotiations in PPP LCP using the **MONITOR PPP** command, as shown in Figure 13.

Figure 13 MONITOR PPP - Access Router Card CLI Command

```
Incoming PPP Data on interface: slot:2/mod:1 Time: 18-FEB-2000  20:32:39

    IPCP       CFG_REQ           COMPR_TYPE     00 2d 0f 01

                                 NEW_ADDRS      0a 0a 0a 01

                                 PRIM DNS       00 00 00 00

Outgoing PPP Data on interface: slot:2/mod:1 Time: 18-FEB-2000  20:32:39

    IPCP       CFG_NAK           COMPR_TYPE     00 2d 0f 00

                                 NEW_ADDRS      cf 18 4f ca

                                 PRIM DNS       cf 18 a9 fd

Incoming PPP Data on interface: slot:2/mod:1 Time: 18-FEB-2000  20:32:39

    IPCP       CFG_REQ           COMPR_TYPE     00 2d 0f 01

                                 NEW_ADDRS      0a 0a 0a 01

                                 PRIM DNS       00 00 00 00

Outgoing PPP Data on interface: slot:2/mod:1 Time: 18-FEB-2000  20:32:39

    IPCP       CFG_NAK           COMPR_TYPE     00 2d 0f 00

                                 NEW_ADDRS      cf 18 4f ca

                                 PRIM DNS       cf 18 a9 fd
```

Notice that the client keeps asking for the same 10.10.10.1 address even though the access router card is trying to assign 207.24.79.X. A similar problem could occur if the individual user is configured to negotiate an address and the client is expecting to be assigned one.

If this is the case, the client PPP device is not properly configured. Since it is not possible to cover proper configuration of all client device, it recommended that the client is configured to have an IP address assigned to it. This ensures that the client gets the proper IP address

Some Calls Complete on the Access Router Card

If you have determined that some, but not all calls are failing on the access router card, check the following settings:

1. Check the RADIUS/TACACS configuration to determine if those users that connect are configured differently from those who do not.

   If this is the case, determine the reason for the difference in configuration. This difference should point to the problem.

   An examination of the user configuration in RADIUS or in the local users table should reveal the differences. Start by changing the problem user's configuration to match a working user.

2. If no configuration differences exist, survey all failed users and see if they have modems from the same manufacturer or chip set.
3. If this is the case, the failures are all tied to a specific modem, make sure that the modem firmware is updated to the latest available from the vendor. If this does not correct the problem, contact CommWorks customer support.
4. If the modems are the same, check the software versions of the clients that fail. For example are all failures with Windows NT Service Pack 3 or Windows 95 with DUN 1.0?
5. If this correlation is found the failures are all tied to a specific client platform, make sure that the client software is updated to the latest available from the vendor. If this does not correct the problem contact CommWorks customer support.
6. Check to see if all the calls that complete area all digital or all analog. If only one type of call can complete and your configuration you should support both check your modem configurations.
7. Check if the failures are isolated to a single modem card or telco span.

   The sysloging from CIP should help determine if the calls are only failing from a specific set of modems.

   a. Swap the span to a different set of modems. This should indicate if the problem follows the span or is related to specific modems. If this test shows either, the problem is isolated to a single modem or span.

   b. Verify configurations and software versions on the problem card and match the working cards and the span provisioning from the telco. If this is correct, swap the card with a "known" good card.

   c. There are two possible points of hardware failure:

      - the chassis slot may be defective
      - the card may be defective

This can be determined by moving the card.

8 If you determine that the hardware is the problem, return the card for repair. If hardware is ruled out by swapping of cards and spans, re-check the configuration for the interfaces on that card in the access router card and that card's configuration. It is also possible that the telco has provisioned the span incorrectly.

Using PPP Monitoring to Track Problems

The access router card will display the PPP but will not diagnose any problems for you. To get a good understanding of the output use the book *PPP Design and Debugging* by James Calrlson as a reference guide. Table 7 lists relevant RFC documents related to PPP:

Table 7 RFC References - PPP Design and Debugging

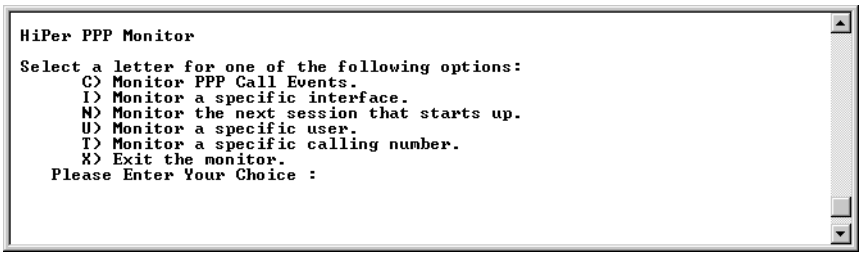
RFC	Description
RFC 2153	PPP Vendor Extensions
RFC 1332	The PPP Internet Protocol Control Protocol (IPCP) - Address Negotiation
RFC 1877	PPP IPCP Extensions for DNS & NBNS
RFC 1994	Authentication (PAP/CHAP)

Start the PPP monitor by entering the following command from the access router card command prompt:

```
MONITOR PPP
```

Figure 14 displays the access router card monitor facility:

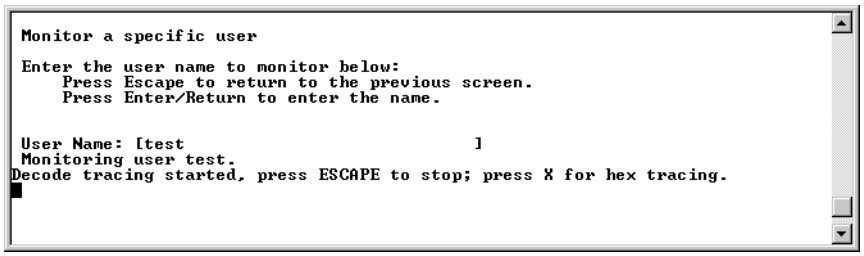
Figure 14 Monitor PPP Command Display



Options I,N,U will show you the complete PPP packets to and from the access router card.

For example, if you wanted to see all the PPP from user “test”. Choose option “U” and supply the name “test” as shown below:

Figure 15 Monitoring a Specific User - PPP



You are now in the monitoring mode. Take a screen capture from your terminal program at this time. There is no way to go back and look at the packets on the access router card after the screen pages. Once the user “test” gets authenticated, the access router card displays the final part of LCP and then begins showing the PPP data packets.

Figure 16 shows the screen output.

Figure 16 Monitoring PPP - CLI Final Output

```
Outgoing PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:52
    CHAP       SUCCESS           00
Outgoing PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:52
    IPCP       CFG_REQ           COMPR_TYPE     00 2d 0f 00
                                 NEW_ADDRS      cf 18 4f 15
Incoming PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    IPCP       CFG_REQ           COMPR_TYPE     00 2d 0f 01
                                 NEW_ADDRS      00 00 00 00
   PRIM DNS       00 00 00 00
                                 PRIM NBNS      00 00 00 00
                                 SEC DNS        00 00 00 00
                                 SEC NBNS       00 00 00 00
Outgoing PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    IPCP       CFG_REJ           PRIM NBNS      00 00 00 00
                                 SEC DNS        00 00 00 00
                                 SEC NBNS       00 00 00 00
Incoming PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    CCP        CFG_REQ           MS_COMP        00 00 00 01
                                 STAC_COMP      00 01 04
Outgoing PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    CCP        CFG_REJ           STAC_COMP      00 01 04
Outgoing PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    CCP        CFG_REQ           MS_COMP        00 00 00 01
Incoming PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    IPCP       CFG_ACK           COMPR_TYPE     00 2d 0f 00
                                 NEW_ADDRS      cf 18 4f 15
Incoming PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    IPCP       CFG_REQ           COMPR_TYPE     00 2d 0f 01
                                 NEW_ADDRS      00 00 00 00
                                 PRIM DNS       00 00 00 00
Outgoing PPP Data on interface: slot:2/mod:1 Time: 31-JAN-2000  17:40:53
    IPCP       CFG_NAK           COMPR_TYPE     00 2d 0f 00
                                 NEW_ADDRS      0a 0a 0a 06
                                 PRIM DNS       cf 18 a9 fd
I CCP        CFG_ACK           MS_COMP        00 00 00 01
Tracing stopped, Return/Enter to re-start, ESCAPE to quit.
```

If the complete PPP negotiation that includes all the LCP prior to authentication, options **N** and **I** will capture the entire session. You need to know that user will be next to call in or on what interface to expect the call. If this is a "live" chassis there will be too many calls to predict this. Use the "TAP" facility in that case.

The PPP Call events provide a high level look at all PPP traffic on the card. No decoding is attempted. It is not very useful when looking for root cause of a problem. Two calls are shown, one completes and terminates successfully, the second fails do to an authentication problem that can not be determined from the trace. The trace shows "CHAP Mismatch," the failure was cause by using a name that was not present in the user database.

Figure 17 shows the PPP call events.

Figure 17 PPP Call Events

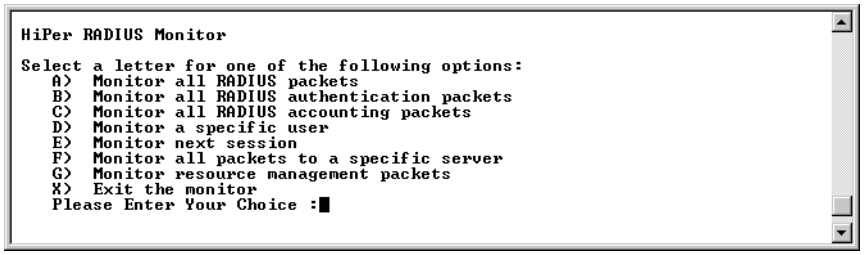
```
Monitoring PPP Call events.

....Tracing of Call Events; Escape to stop...

New PPP Call received on interface slot:2/mod:1

PPP - Authentication Complete to tests.

PPP - Expanded Authentication Complete to tests.

PPP - MPPC Compression Link UP to tests.

PPP - IP Link UP to tests (10.10.10.6)

Local IP Address (207.24.79.21) was configured.

Expanded PPP link down to tests.

PPP connection down to tests.

New PPP Call received on interface slot:2/mod:1

PPP Auth Failed, CHAP Mismatch. PPP link down to .

PPP Link Down to .

PPP connection down to .
```

Monitoring RADIUS for Problems

The access router card will display the RADIUS but will not diagnose any problems for you. To get a good understanding of the output it is recommended that the RFC's 2865 and 2867 be used as a reference guide.

Start the RADIUS monitor with the command **MONITOR RADIUS**. This will bring you to the following menu shown in Figure 18:

Figure 18 RADIUS Monitor



The type of information displayed by options A through G is the same. It shows you the decoded RADIUS packet for all attributes that the access router card understands. Any unknown attributes will not show up. If you suspect a problem caused by unknown attributes, switch the monitor to HEX mode by typing **H** during the session. You must then use the RFC to aid in decoding the packets manually.

Option **G** shows only packets that deal with RADIUS resource management. These packets are not described in the standard RADIUS RFC's. They are part of a specification that never made it to RFC status.

For example, if you wanted to see the RADIUS traffic for the next session, enter option **E** at the prompt. The output will look like Figure 19:

Figure 19 Monitoring Next RADIUS Session - Access Router Card

```
Tracing next RADIUS session
Decode tracing started, press H and D to toggle between hex and decode mode

Press Escape to return to the previous screen.
-----------------------------------------------------------------
Source-IP         Src-Port Destination-IP Dest-Port Id Packet-Type
-----------------------------------------------------------------
207.24.79.21     1645   207.24.169.214      1645    5 Access-Request
-----------------------------------------------------------------
Time Stamp : 01-FEB-2000  19:31:32
-----------------------------------------------------------------

User-Name : tests
CHAP-Password : xxxxxxxxxx
NAS-IP-Address : 207.24.79.21
NAS-Port : 257
Acct-Session-Id : 16777241
Interface-Index : 1513
Nas-Supports-Tags : 0
Service-Type : 2
Framed-Protocol : PPP
Multilink-PPP-Endpoint-Id : f2 22 86 5
MP-EDO : f2 22 86 5
Chasis-Call-Slot : 2
Chasis-Call-Span : 1
Chasis-Call-Channel : 1
Initial-Connect-Rate : 1(NONE)
Calling-Station-Id : 8473579016
Called-Station-Id : 5453087
NAS-Port-Type : 2

-----------------------------------------------------------------
Source-IP         Src-Port Destination-IP Dest-Port Id Packet-Type
-----------------------------------------------------------------
207.24.169.214     1645     207.24.79.21      1645    5 Access-Accept
-----------------------------------------------------------------
Time Stamp : 01-FEB-2000  19:31:32
-----------------------------------------------------------------

Service-Type : 2
Framed-Protocol : PPP
Framed-IP-Address : 10.10.10.6
Framed-IP-Netmask : 255.255.255.255
Framed-Route : 10.10.1.1/24 0.0.0.0 1
Idle-Timeout : 900

Port-Limit : 2
```

Using the Port TAP Facility

The access router card can be setup to "tap" a user or WAN interface. The "tap" displays all the data at the byte level going in or out from the configured interface. This raw data can then be decoded and analyzed as part of the call failure diagnosis.

There are two ways to initiate a tap:

- By configuring a user either via RADIUS or local user configurations to have that users session tapped every time. In this case the tap would start after authentication.
- Configure a tap on a specific interface. This shows all traffic on that interface until the tap is stopped.

Tap data can be viewed in two ways:

- Sent to a outside server running syslog
- Viewed in the CLI

User Configured for TAP

In this configuration syslog is the only allowed method of storing the captured data. For a locally configured user the following commands are used to set up a tap.

```
set tap user <name>
```

The user record should contain the following attributes to enable a tap. The RADIUS server requires support for CommWorks/3Com/USR style VSAs.

Figure 20 Port Tap Facility - User Record

```
# Port-Tap Feature Attributes

USR-ATTRIBUTE       Port-Tap            0x9845  integer

#       Tapping Values
USR-VALUE               Port-Tap                Disabled                0
USR-VALUE               Port-Tap                Enabled                 1
USR-ATTRIBUTE       Port-Tap-Format     0x9846   integer

#       Port Tap Format Enumerations
USR-VALUE               Port-Tap-Format         Ascii                   0
USR-VALUE               Port-Tap-Format         Hex                     1
USR-VALUE               Port-Tap-Format         Clear                   2
USR-ATTRIBUTE       Port-Tap-Output     0x9847   integer

#       Port Tap Output Enumerations
USR-VALUE               Port-Tap-Output         Syslog                  0
USR-VALUE               Port-Tap-Output         Console                 1
USR-ATTRIBUTE       Port-Tap-Facility   0x9848   integer

#       Port Tap Facility Enumerations
USR-VALUE               Port-Tap-Facility       Log-Auth                1
USR-VALUE               Port-Tap-Facility       Log-Level0              2
USR-VALUE               Port-Tap-Facility       Log-Level1              3
USR-VALUE               Port-Tap-Facility       Log-Level2              4
USR-VALUE               Port-Tap-Facility       Log-Level3              5
USR-VALUE               Port-Tap-Facility       Log-Level4              6
USR-VALUE               Port-Tap-Facility       Log-Level5              7
USR-VALUE               Port-Tap-Facility       Log-Level6              8
USR-VALUE               Port-Tap-Facility       Log-Level7              9
USR-ATTRIBUTE       Port-Tap-Loglevel   0x9849   integer

#       Port Tap Log Level Enumerations
USR-VALUE               Port-Tap-Loglevel       Critical                0
USR-VALUE               Port-Tap-Loglevel       Unusual                 1
USR-VALUE               Port-Tap-Loglevel       Common                  2
USR-VALUE               Port-Tap-Loglevel       Verbose                 3
USR-ATTRIBUTE   Port-Tap-Address                0x984a  ipaddr
```

Command Line Interface Configured TAP

The CLI provides the **ADD TAP** command set which can be used to add a number of taps that will track a user or interface. Only modem interfaces can be tapped. This feature has the provision for displaying the TAP data directly on the console or to send it to a syslog server.

The configured taps can be seen with the **LIST TAP** command.

The following is output from an **ADD TAP NEXT FORMAT HEX OUTPUT SCREEN** command.

Figure 21 ADD TAP CLI Output

```
Tapping the next session to start up.

     Press ESC followed by ENTER key to exit tapping.

TAP NEXT   IN:    0: 7E FF 7D 23 C0 21 7D 21 7D 21 7D 20 7D 37 7D 21
TAP NEXT   IN:    0: 7D 24 7D 25 DC 7D 27 7D 22 7D 28 7D 22 7D 31 7D
TAP NEXT   IN:    0: 24 7D 25 DC 7D 33 7D 27 7D 24 30 3A DB 7D 2A 51
TAP NEXT   IN:    0: 26 7E
TAP NEXT  OUT:    1: FF 03 C0 21 01 01 00 1E 01 04 05 EA 03 05 C2 23
TAP NEXT  OUT:    1: 05 05 06 9C 66 7B 27 07 02 08 02 11 04 05 EA 13
TAP NEXT  OUT:    1: 03 00
TAP NEXT  OUT:    2: FF 03 C0 21 02 01 00 17 01 04 05 DC 07 02 08 02
TAP NEXT  OUT:    2: 11 04 05 DC 13 07 04 30 3A DB 0A
TAP NEXT   IN:    3: FF 03 C0 21 02 01 00 1E 01 04 05 EA 03 05 C2 23
TAP NEXT   IN:    3: 05 05 06 9C 66 7B 27 07 02 08 02 11 04 05 EA 13
TAP NEXT   IN:    3: 03 00
TAP NEXT  OUT:    4: C2 23 01 02 00 19 10 CC C1 79 F1 A1 61 2A 9C 4E
TAP NEXT  OUT:    4: 94 45 4B 11 E5 5A 2E 6D 69 6B 65
TAP NEXT  OUT:    5: C2 23 01 03 00 19 10 55 80 DB B5 60 31 39 90 5A
TAP NEXT  OUT:    5: EE 3F AF FF FE E9 42 6D 69 6B 65
TAP NEXT   IN:    6: C2 23 02 03 00 1A 10 7D 15 0D 16 AF 0B 71 5D 46
TAP NEXT   IN:    6: 53 FB A1 50 71 A8 CB 74 65 73 74 73
TAP NEXT   IN:    7: FF 03 C0 21 05 02 00 04
TAP NEXT  OUT:    8: FF 03 C0 21 06 02 00 04


Tap session concluded.  Press ENTER for prompt.
```

Using Syslog Facilities

The access router card has a number of process facilities. In normal operation the card will only send messages of a critical nature to the syslog. For trouble locating and clearing it is possible to have certain processes send detailed information about everything they do to either the console or a syslog server.

To see a list of available facilities and the detail level of their output, use the command **LIST FACILITIES**.

A sample is shown in Figure 22 along with Table 8 listing the more useful facilities.

Figure 22 Access Router Card - List Facilities Command

```
HiPer>LIST FACILITIES

FACILITIES
Event Facility                    Log Level
ATM AAL Driver                    CRITICAL
ATM ILMI                          CRITICAL
ATM Network Driver                CRITICAL
ATM SAR                           CRITICAL
ATM Signalling                    CRITICAL
Auth Facility                     CRITICAL
Board Support Management Process  CRITICAL
CMIS SNMP Manager                 CRITICAL
Call Initiation Process           CRITICAL
Command Line Interpreter          CRITICAL
Configuration File Manager        CRITICAL
Configurator                      CRITICAL
Console Driver                    CRITICAL
Crypto Driver                     CRITICAL
DHCP relay agent                  CRITICAL
DNS                               CRITICAL
Differential Services             CRITICAL
Discovery                         CRITICAL
Driver                            CRITICAL
Ethernet Driver                   CRITICAL
Event Handler                     CRITICAL
Filter Manager Process            CRITICAL
Frame Relay Process               CRITICAL
GWC Modem Driver                  CRITICAL
GWCWAN Driver                     CRITICAL
HTML                              CRITICAL
IGMP                              CRITICAL
IP                                CRITICAL
IP Routing Process                CRITICAL
IP Spoofing Process               CRITICAL
IPSEC                             CRITICAL
IPX                               CRITICAL
IPX Spoofing Process              CRITICAL
IPX/IP Dial-out Process           CRITICAL
ISAKMP                            CRITICAL
L2TP                              CRITICAL
MCNS Reg/Adm                      CRITICAL
MIB Registrar                     CRITICAL
MPIP                              CRITICAL
NAI                               CRITICAL
NTP - Network Time Protocol       CRITICAL
Network Management Bus Agent      CRITICAL
Network Management Bus Driver     CRITICAL
Network Management Interface      CRITICAL
OSPF Facility                     CRITICAL
PKI                               CRITICAL
PM                                CRITICAL
PPP                               CRITICAL
PPPoE                             CRITICAL
PPTP                              CRITICAL
Polling Process                   CRITICAL
Port Tapper                       CRITICAL
QAM Driver                        CRITICAL
RSH Server                        CRITICAL
Remote Ping Process               CRITICAL
RoboExec                          CRITICAL
```

Table 8 describes the most common list facilities for the access router card:

Table 8 Most Common List Facilities

Call Initiation Process	Details about a call from presentation to completion
GWC Modem Driver	Packet Bus Communication between the access router card and modem
Filter Manager Process	Adding, Using, Verifying Filter files or rules

Table 8 Most Common List Facilities (continued)

IP	IP protocol stack
IP Routing	Changes and updates to the routing and forwarding tables
PPP	PPP stack details

The default setting for all processes is **CRITICAL**. Using the **SET FACILITY** command can change this. For processes with spaces in the name of the command will require you to place the name in quotes. There are four possible levels, listed in order of verbosity (CRITICAL, UNUSUAL, COMMON, DEBUG, and VERBOSE)

The facility **Configurator** is set to debug. This causes the access router card to stream detailed messages about what that process is doing to the configured syslog servers.

If no syslog server is configured or to take a quick look at the output, use the command **SHOW EVENTS**. This causes all messages that would go to syslog to also be echoed to the telnet console. Disabling this feature is done by **HIDE EVENTS**.

Serial console sessions will always show these messages and cannot be suppressed.

Some processes generate such large amounts of data that you may not be able to type the hide command. This would then require opening a second session and turning the process to a less verbose setting.

Syslog servers are added with the **ADD SYSLOG** command syntax.

Access Router Card Trouble Clearing Commands

This section includes trouble clearing commands used on the access router card.

Viewing Facility Errors

The **set facility** command allows you to set and view log levels for the system's processes, ensuring that error messages reaching the threshold for that facility outputs to the console port.

Although messages are sent to the Console port by default, you can configure a SYSLOG host to receive and save messages. See the Using Event Logging section later in this chapter for more information.

Log levels range from the lowest state, *debug*, to the highest, *critical*. The default is *critical*. Type:

set facility <name> **loglevel** [common | critical | debug | unusual | verbose]

For example:

set facility snmp loglevel unusual

*Use the **list facilities** command to view a log level change.*

Terminating an Active Process

The **kill** command terminates an ongoing process. You can kill a process only after it has started. For instance, if you want to kill a **ping** request that has run too long.

Use the **list processes** command to view current active processes.

For example:

Figure 23 Access Router Card - List Processes Command

```
HiPer>> list processes

PROCESSES
Index     Name                              Type           Status
2001      NameManager                       System         Inactive
12001     Console                           System         Inactive
22001     FileManager                       System         Inactive
32001     Configurator                      Application    Inactive
42001     Main                              Application    Active
52001     MIB Registrar                     Application    Inactive
62001     Config File Manager               Application    Inactive
72001     RoboExec NetManagement            Application    Active
82001     Event Handler                     Application    Inactive
92001     System Bus                        Driver         Inactive
a2001     NMB Driver                        Driver         Inactive
b2001     Device Discovery                  Application    Inactive
c2001     Console Driver                    Driver         Inactive
d2001     Loopback Driver                   Driver         Inactive
e2001     Ethernet Driver                   Driver         Inactive
f2001     IP Forwarder                      Forwarder      Inactive
102001    UDP Process                       Application    Inactive
112001    TCP Process                       Application    Inactive
122001    Telnet                            Application    Inactive
132001    SLIP Process                      Application    Inactive
142001    TFTP Process 142001               Application    Inactive
152001    IP Spoofing                       Application    Inactive
162001    DHCP Relay Agent                  Application    Inactive
172001    Ping Service Checker              Application    Inactive
182001    RADIUS User Manager               Application    Inactive
192001    SNMP Agent                        Application    Inactive
1a2001    Point to Point Protocol           Application    Inactive
1b2001    Domain Name System                Application    Inactive
1c2001    Filter Manager Process            Application    Inactive
1d2001    NTP - Network Time Protocol       Application    Inactive
1e2001    NMB Agent                         Application    Inactive
1f2001    BSP Management Process            Application    Inactive
202001    Remote Ping Process               Application    Inactive
212001    File System Compaction Process    Application    Inactive
222001    IPX/IP Dial-out Process           Application    Inactive
232001    Traceroute Process                Application    Inactive
242001    Tunnel Dispatcher                 Application    Inactive
252001    NPPTP                             Application    Inactive
262001    L2TP Process                      Forwarder      Inactive
272001    VTP Process                       Application    Inactive
282001    MPIP Process                      Application    Inactive
292001    PPPoE Process                     Application    Inactive
2a2001    Port Tapping Process              Application    Inactive
2b2001    PM Process                        Application    Inactive
2c2001    IPsec process                     Application    Inactive
2d2001    ISAKMP process                    Application    Inactive
2e2001    NATProcess                        Application    Inactive
2f2001    HTML Process                      Application    Inactive
302001    DiffServ Process                  Application    Inactive
312001    Frame Relay Process               Application    Inactive
322001    RSH Deamon Process                Application    Inactive
332001    Call Init Process                 Application    Inactive
342001    IP Routing Instance               Application    Inactive
352001    IP OSPF                           Application    Inactive
362001    CLI                               Application    Inactive
372001    GWC Modem Driver                  Driver         Inactive
382006    CLI 382006                        Application    Inactive
392003    CLI 392003                        Application    Inactive
HiPer>>
```

CAUTION: *Use the kill command with caution. Stopping all processes on the access router card may cause serious problems. It may be much easier and safer to simply reboot the card.*

Resolving Addresses

The **arp** command performs IP address resolution. Type:

```
arp <ip address or host name>
```

The system will respond with an IP address (and MAC [Ethernet] address if found on a locally connected network) of the host. For example:

```
ARP: 172.122.120.118 -> 08:00:09:cc:58:bf
```

Resolving Host Names

The **host** command returns an IP address for a specified host name by sending it to a DNS server for resolution. Before you can resolve a host, you must have added a DNS local host and server entry for resolution. To do so, use the *add dns host <name> address <ip address>* and *add dns server <ip address>* commands.

For example:

```
add dns server 133.114.121.45 preference 1 name “Our DNS
server”

add dns host hahvahd.college-hu.com address
133.114.121.15

host hahvahd
```

A screen output example:

```
Network Name: hahvahd.college-hu.com
is resolved to Address: 133.114.121.015
```

Using Ping

Overview

The **ping** command is very helpful in testing connectivity with other network devices. Options let you set ping attempts (*count*), the period between ping attempts (*interval*), the time before quitting (*timeout*), a string value specifying data to be sent (*data*), the ping maximum packet dimension (*size*), the ping process off screen (*background*), the progressive ping output for each ping request (*verbose*), and the erasure of entries in the Remote Ping Table (*self_destroy_delay*).

The CLI can perform a ping with either *verbose* or *background* selected, but not both. *Verbose* causes the CLI to display information for each PING transmitted. *Background* causes the CLI to start the PING request and then ignores it. This diagnostic tool can also be initiated from an SNMP station. Type **ping** and the following related commands:

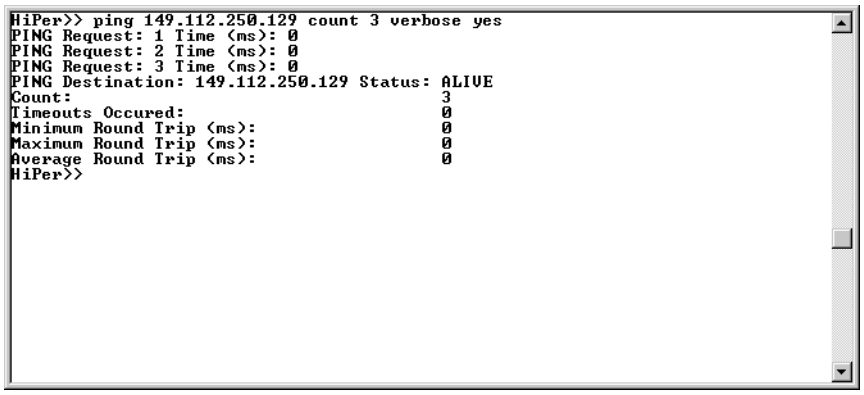
```
ping <IP address>
background [no | yes]
count [1 to 1000]
data [alphanumeric string]
interval [seconds; 1 to 65535]
self_destroy_delay [minutes; 1 to 65535]
size [1 to 1400]
timeout [1 to 60]
verbose [no | yes]
```

For example:

```
ping 149.112.250.129 count 3 verbose yes
```

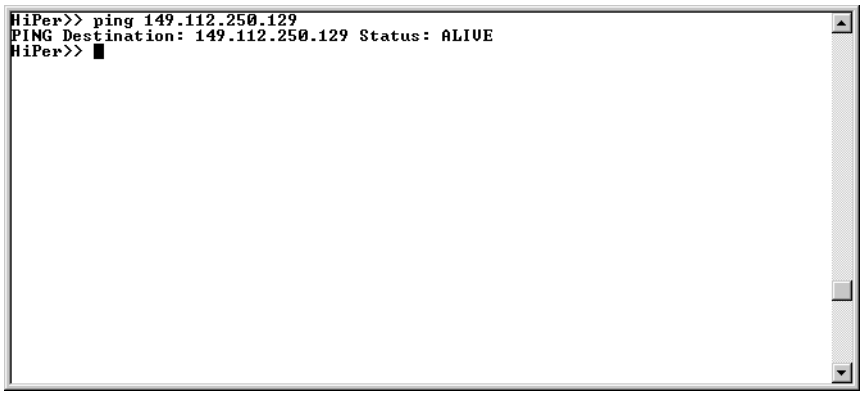
The command would display the following:

Figure 24 Ping CLI Command Output



A ping of a *single* count produces the following, for example:

Figure 25 Ping CLI Command Example - Single Device



Listing Ping Settings

You can use the **LIST PING SYSTEMS** command to display ping results.

Showing Ping Statistics

The **show ping row <number>** command is an alternative to display ping statistics.

Use the **delete ping row** <number> command to erase a row in the Remote Ping Table.

Setting Ping Row Ceiling

The **set ping maximum_rows** command sets the maximum number of rows permissible in the Remote Ping Table. Setting this parameter to a number smaller than the current number of rows will not cause any row deletions immediately but will follow any current ping. Default: **20**. Range: **1-1000**.

Configuring a Ping User

You can configure a ping user to test the connectivity of a specified login host using the **add** and **set login user** commands. A user pings a login host, gets a successful/unsuccessful message and is disconnected. Use these commands to test connectivity:

add user <user name> **type login**

set login user <user name> **login_host** <name or IP_address> **login_service ping**

For example:

add user jack type login

set user jack login_host_name 3.3.3.3 login_service ping

Using Ping to Monitor System Connectivity

The **add ping_service_loss_system** command creates a configurable ping that monitors connectivity across the Ethernet network to a specified server. If contact is lost to the server, the card signals the network management card which can be configured to busy out all chassis modems so no more calls are answered and any hunt groups will answer to other systems.

The configurable parameters are:

- **IP name or address** of the server to be pinged,
- **enable/disable ping service** to the specified server,
- **frequency** of ping requests,

- **misses_allowed** or number of ping failures to allow before busying out the modems
- **timeout** or the interval to wait before busying out the modems.

The command is entered as follows:

```
add ping_service_loss_system <ip_name_or_address>
enabled [yes | no]
frequency [1-200 seconds]
misses_allowed [1-1000]
timeout [1-6000 seconds]
```

For example:

```
add ping_service_loss_system camel enabled yes frequency
30 misses_allowed 75 timeout 500
```

Use can display all configured ping servers with the **show ping service_loss_system** command.

The **set ping service_loss_system** command allows editing of the add command while the **enable service_loss_busyout** <ping> command turns the service on and the **disable service_loss_busyout** <ping> command turns it off. You can also use the **delete ping service_loss_system** command to remove the service altogether.

Viewing Interface Status and Settings

Several commands are useful to display the active/inactive status and settings of specific interfaces (ports). They are: **list switched interfaces, list interfaces** and **show interface settings,** and **show switched interface** <slot:*x*/mod:[1-*y*]>.

Using Event Logging

This section includes information about event logging.

SYSLOG Host Event Logging

You can use the SYSLOG daemon to log events to one or more remote hosts. Event messages are sent to a SYSLOG server via UDP using port 514 - the standard UDP port for SYSLOG messages. If you Telnet to port 514, you will get the output of SYSLOG messages.

When Internet Control Message Protocol (ICMP) logging is enabled, the following ICMP events are logged to SYSLOG:

- Sent Dest Unreachable
- Sent ICMP TimeExceeded
- Rcvd ICMP TimeExceeded
- Sent Parameter Problem
- Rcvd Parameter Problem

- Rcvd Source Quench ICMP
- Rcvd TimeStamp REQ ICMP
- Rcvd Address Mask REQ ICMP
- Rcvd Address Mask Reply ICMP
- Rcvd Router Solicitation ICMP
- Sent Router Advertisement ICMP
- Sent ICMP Redirect (Recv'd ICMP Redirect messages are not logged)

Console Event Logging

Event messages are automatically displayed on a local console. Of all ICMP messages generated, only *Received Destination Unreachable* messages are logged to the console.

TELNET Session

All events normally directed to the Console only can also be echoed to the TELNET or dial-in session you are running by issuing a **show events** command (the **hide events** command disables the function).

Event Logging Levels

Various event messages are generated for each facility, and are sent to any defined logging sinks. For each facility, you can specify the level of event information sent. Although the logging level of each event is fixed, you can configure the level of messages that are sent to a specific logging sink. Logging levels are:

- **Critical**—A serious system error that may affect the integrity of the system
- **Unusual**—An event that normally does not happen, but from which the system should recover
- **Common**—A normal event
- **Verbose**—A normal occurrence that happens frequently

You can configure whether event messages are sent to a logging sink according to the level of the message. For example, if you wanted to see only the *unusual* and *critical* events messages generated by the TELNET facility, you would set the event level threshold for TELNET to *unusual*.

Only messages that are unusual and critical are sent to the Console port.

Enter the following command to list log levels:

```
list facilities  ENTER
```

*Do not confuse **set facility** and **set syslog** commands. **Set facility** determines which messages are generated on the console or to a Telnetted PC - depending on the log level specified for each facility. The **set syslog** command, on the other hand, determines which messages are saved - depending on the global log level you've set for the particular SYSLOG host.*

Setting the Event Log Level

You can set the log level for each facility. By setting the event log level, you define the level at which you want messages associated with the facility to be displayed on the console port. Messages associated with a selected log level are displayed along with any more serious log levels.

To set the log level of a facility, use the following command:

```
set facility <facility_name> loglevel <log level choice>
```

For example, to set the log level of the IP facility to Unusual type:

```
set facility IP loglevel unusual
```

To display the list of facilities and their associated log levels, use the following command:

```
list facility
```

Event Message Examples

The system is capable of delivering hundreds of event messages, from common events to critical events. This section describes some representative event messages that are generated. Each event message is categorized by the facility by which it is generated.

The message description includes information about the meaning of the message, and if necessary, any corrective action you can take.

IP Messages

- "ipCfmSet_ipRoute: gateway of destination X, mask Y is not reachable. static route not added"
  - Meaning—The administrator tried to define a static route using a gateway that is not reachable via any of the existing IP routes
  - Action—Specify a different gateway that has an IP address that can be reached

- "proxy_arp_insert: no common network address found for remote ip address X"
  - Meaning—You are connecting to the system using an IP address that is not on the same IP subnetwork as the network defined for the system's LAN interface. Therefore, no proxy ARPing will be performed.
  - Action—Informational message. No action required

- "The route destination (X) should not contain more bits than are specified in the route mask (Y)"
  - Meaning—The administrator tried to add an IP route where the network prefix of the destination contains more bits than are specified in the network mask

- Action—If no netmask is specified, the natural mask of the address is assumed. To specify a host route, you must specify /H as the netmask. For example:

```
add ip route 204.249.182.199/H
```

- "Failed to delete the route to X. Only routes marked as Static/NetMgt can be deleted."
  - Meaning—The administrator tried to delete an IP route that cannot be deleted
  - Action—Informational message. No action required

- "Failed to create static or default route. The IP subnet for the specified gateway does not exist or is disabled."
  - Meaning—The administrator tried to add an IP route over an interface which is disabled or down
  - Action—Enable the interface before adding the route

*Use the **list ip net** command to view IP network addresses currently in use.*

Call Initiation Process Messages

- "CIP: Unable to find an available default host for user%s,%x/n"
  - Meaning—The user tried to connect to a host from the login host table, but there is no available host
  - Action—The login host table is probably empty. Add a host to the table and let the user dial in again

User Manager Messages

- "AUTH: Unable to authenticate if both authentication IP's are set to 0"
  - Meaning—The user may not be defined locally, remote authentication is not enabled, or a remote authentication IP address is not configured
  - Action—Define the user locally or configure a RADIUS server IP address

- "AUTH: Unable to account if both accounting ip's are set to 0"
  - Meaning—Remote accounting is enabled, but no RADIUS accounting server IP addresses have been configured
  - Action—Either disable remote accounting or configure a RADIUS accounting server IP address

- "AUTH - Most likely client/server configuration mismatch"

Filter Manager Process Messages

- "FM: In filter file <name> had no rules for <protocol> protocol"
  - Meaning—A filter protocol section is defined, but there are no rules associated with it.
  - Action—A protocol section must either contain at least one rule, or be commented out for the syntax to be valid

- "FM: In filter file <name>, previously defined section <protocol section name>"
  - Meaning—There are two protocol sections that use the same name, for example, you defined two IP protocol sections in the filter file
  - Action—Delete one of the duplicate protocol sections

- "FM: In filter file <name>, ambiguous first line"
  - Meaning—The filter file does not contain the required file descriptor on the first line
  - Action—Place file descriptor (#filter) on first line of file

UDP Messages

- "UDP - could not get source IP address"
  - Action—Create an IP network

Configuration File Manager Messages

- "The configuration file <filename> is corrupt. Status <error status>."
  - Meaning—The Configuration file has been corrupted. It will be renamed to <filename>.bad
  - Action—Keep a copy of the <filename>.bad file. If the file was uploaded to using TFTP, upload the file again making sure the TFTP transfer mode is set to octet

- "Could not create a list for CFM Control Structures. Status: <error status>."
  - Meaning—The Configuration File Manager could not allocate the resources necessary for normal operation
  - Action—Reboot the system

IP Dial-out Process Messages

- "INIT: Could not allocate a private data area. Status: <error status>."
  - Meaning—The dial-out process could not allocate enough memory for its data. The dial-out process will not be started
  - Action—Free some memory, for example, delete some users. Once some memory has been freed, save the configuration and reboot the system

4 Network Management Card and HiPer NMC Trouble Locating and Clearing

This chapter includes solutions for the network management card.

This chapter contains the following topics:

Overview

The network management card provides a single point of management access into the Total Control® 1000 chassis. It manages all of the devices installed in the Total Control 1000 chassis and operates under the direction of management software running on a workstation known as the network management station.

Network Management Card NAC Faceplate

The network management card Network Application Card (NAC) has 5 Light Emitting Diodes (LEDs) for representing system and network status, a RUN/FAIL (RN/FL) LED for card status, and a 4 character LED display for identification or status.

Figure 26 Network Management Card NAC Faceplate

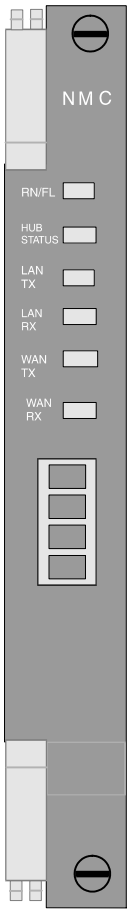


Table 9 lists the purpose of the network management card LEDs.

Table 9 Network Management Card LED Descriptions

LED	Purpose
RN/FL	NAC Run/Fail indicator
HUB ST	Hub (system) status
LAN TX	Local Area Network (LAN) transmit (TX)
LAN RX	Local Area Network (LAN) receive (RX)
WAN TX	Wide Area Network (WAN) transmit (TX)
WAN RX	Wide Area Network (WAN) receive (RX)
HUB NUMBER/STATUS	4 character alphanumeric display for identification or status indication

Verifying Software Version Numbers

Before you perform any trouble locating and clearing, ensure you are using the correct network management card software version. Check this version number with the published version number in the Total Control 1000 Enhanced Data System System 4.5 GA System Release Notes. You will need to know this number if you contact CommWorks Technical Support.

Common Element Manager

To verify the network management software version using common element manager:

1. From the Explorer tab, click the network management card.
2. From the Properties tab, click the **Identification** tab.
3. Check the **Version** field for the current software number.

Total Control Manager

To verify the network management card software version using total control manager:

1. From total control manager's Virtual Front Panel Display (VFPD), select the network management card.

   The card turns blue.
2. From the main menu, click **Configure** and then click **Programmed Settings**.

   The NMC Card Programmed Settings window appears.
3. From the Parameter Group drop-down menu, select **NMC Identification** to query data from the network management card.
4. Check the **Software Version** field for the current software version.

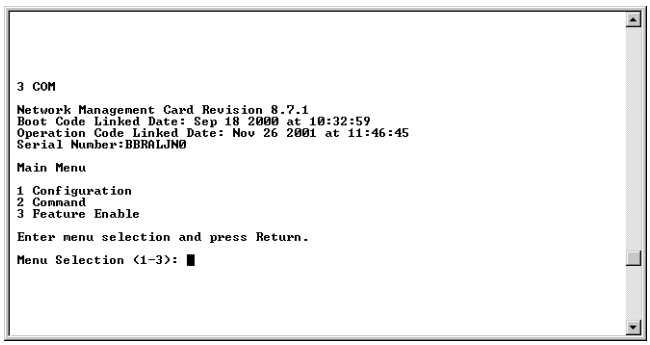
Command Line Interface

To verify the network management card software version using the CLI:

1. Access the CLI Main Menu from the network management card's CLI.
2. View the software version at the network management card Main Menu.

   Figure 27 displays the CLI output for the network management card.

   Figure 27 Network Management Card Software Verification - Command Line Interface



LED Diagnostics

This sections describes LED diagnostics for the LEDs on the network management card.

RN/FL LED Diagnostics and Trouble Locating and Clearing

Table 10 lists network management card RN/FL diagnostics.

Table 10 Network Management Card RN/FL LED Diagnostics

LED Color	Condition	Diagnosis/Troubleshooting
Solid Green	Normal	The NAC is functioning properly.
Flashing Green	Loading boot code	This condition is part of the NAC's bootup routine which should take less than 1 minute to complete. If the condition persists, the NAC may be in need of a software download (SDL). Download the latest version of firmware to the card according to the instructions provided in this guide. When the download is complete, the card will reboot and the LED should turn solid green after the bootup routine
Flashing Red and Green	Non-Critical Failure	A non-critical failure is an error that occurs when the network management card cannot communicate with another NAC in the system. To find out which NAC the network management card cannot communicate with, observe the RN/FL LEDs on the other NACs in the system. The offending NAC will keep rebooting until it can communicate with the network management card over the Management Bus.
Solid Red	Critical Failure	A critical failure is one that will keep the NAC from executing it's functions. Remove the card from the slot and reinstall it following the NAC installation instructions in the *Getting Started Guide*. If the problem persists after the NAC goes through its bootup routine, contact your technical support representative.

HUB ST LED Diagnostics and Trouble Locating and Clearing

Table 11 lists the HUB ST LED indicates system or chassis status.

Table 11 Network Management Card HUB ST LED Diagnostics

LED Color	Condition	Diagnosis/Troubleshooting
Solid Green	Chassis Normal	The chassis is functioning properly.
Solid Red	Chassis Critical Failure	This can be any error that the network management card identifies as potentially harmful. Some errors to look for are: ■ High chassis temperature ■ Fan tray failure ■ Power supply failure ■ Improper NIC/NAC match-ups ■ Timing source loss ■ Bus resets To trouble clear a chassis critical failure, observe the LEDs on the NACs in the chassis and use the status indicating options in the command line.
Flashing Red	Management Bus Failure	The network management card cannot communicate with a card in the chassis over the Management Bus. To find out which NAC the network management card cannot communicate with, observe the RN/FL LEDs on the other NACs in the system. The offending NAC will keep rebooting until it can communicate with the network management card over the Management Bus.

LAN LED Diagnostics and Trouble Locating and Clearing

The network management card NAC has two front panel LEDs for indicating local area network (LAN) activity: LAN TX and LAN RX.

Table 12 lists LAN LED diagnostics:

Table 12 Network Management Card LAN LED Diagnostics

LAN TX	LAN RX	Condition	Diagnosis/Troubleshooting
Flashing Green	Flashing Green	NAC is transmitting and receiving data	The LAN status is operational
Off	Flashing Green	Improper network configuration	The network management card is on the network but is not configured properly. Verify that the network management card's Local LAN IP protocol settings are correct.
Off	Off	No network activity	This is normal if there is no traffic on the LAN. If it is suspected that there is a LAN connectivity problem, Issue a Ping command to the network management card from a remote network node. If the network management card is attached to the network then you will receive a response. If you receive a "Request Timed Out" message, then follow these steps to trouble clear: 1 Verify that you "pinged" the correct address. **2** Check the physical connection to the network management card's Ethernet NIC. The connection should be made to the Ethernet port. **3** Verify that the network management card's Local LAN IP protocol settings are correct.

WAN LED Diagnostics and Trouble Locating and Clearing

The network management card NAC has two front panel LEDs for indicating wide area network (WAN) activity: WAN TX and WAN RX.

Table 13 lists WAN LED diagnostics:

Table 13 Network Management Card WAN LED Diagnostics

LAN TX	LAN RX	Condition	Diagnosis/Troubleshooting
Flashing Green	Flashing Green	NAC is transmitting and receiving data	The WAN status is operational
Off	Flashing Green	Improper network configuration	The network management card is on the network but is not configured properly. Verify that the network management card's Local WAN IP protocol settings are correct. Verify that the baud rates for the network management card's WAN port and on the remote device are compatible.
Off	Off	No network activity	This is normal if there is no traffic on the WAN. If it is suspected that there is a WAN connectivity problem, Issue a Ping command to the network management card from a remote network node. If the network management card is attached to the network then you will receive a response. If you receive a "Request Timed Out" message, then follow these steps to trouble clear: **1** Verify that you "pinged" the correct address. **2** Check the physical connection to the network management card's Ethernet NIC. The connection should be made to the CH2 port. **3** Verify that the network management card's Local WAN IP protocol settings are correct.

HUB NUMBER/STATUS Indicator

The network management card's front panel also contains a 4 character alphanumeric display. This display can be used to designate a name or number for a rack, or a particular status. When the network management card is first powered on, the word WAIT appears in this display while the network management card performs its initialization tasks.

The Hub Number/Status display is set by sending the network management card a command from the management software.

Installation and Configuration Problems

This section provides information on software installation and configuration problems.

Network Management Card Cannot Talk to the Network

After installing and configuring the network management card, and the network management card cannot access the network there could be a problem with its configuration. Use the following procedure to correct this.

To configure the network management card for network access using the command line interface:

1. Plug the console cable into the communication port, and then access the user interface through a terminal emulation program (for example, HyperTerminal).
2. Press **Enter**.
3. If prompted for a password, type the **SNMP read write community string** password.

   The default is **Public** for read only access and **Private** for read/write access.
4. Press **Enter**.
5. Type **1** from the **Main Menu** to access the **Configuration** menu.
6. Type **1**, and then press **Enter** to access the **Local Lan IP Address** menu.
7. Type **1**, and then press **Enter** to access the **Lan IP Address** menu.
8. Type the new **LAN IP Address**, and then press **Enter**.
9. Type **2**, and then press **Enter** to access the **LAN IP Subnet Mask** menu.
10. Type the new **LAN IP Subnet Mask**, and then press **Enter**.
11. Press **Esc** to return to the **Configuration** menu.
12. Type **3**, and then press **Enter** to access the **Local Gateway IP Address** menu.
13. Type the new **Gateway IP Address**, and then press **Enter**.
14. Press **Esc** to return to the **Configuration** menu.
15. Type **9** to access the **Save Configuration to Non Volatile Memory** menu.
16. Press **Enter** to save the LAN IP Configuration to NVRAM.
17. Restart the network management card after changing either the IP address or the netmask.

Network Management Card is Not Sending Accounting Reports

If the network management card is not sending accounting reports try to set up accounting on a network management card using common element manager.

1. From the **Explorer** tab, click the network management card.
2. From the **Properties** tab, click the **Configuration** tab.
3. From the **Configuration** tab, double-click the **LogPriSrvrAddr** field, and then type the IP address for the Primary Accounting server.

4 If a **Secondary Accounting** server exists, double-click the **LogSecSrvrAddr** field, and then type the IP address for the Secondary Log Server IP Address.

5 Double-click the **LogUdpPortNum** field and set the value.

By default, it is set to 1646.

6 Double-click the **LogRetryCnt** field, and then set the number of retries the card will take before the accounting packet drops.

7 Double-click the **LogCallStatGrpSel** field, and then click **group2345** from the drop-down list.

In Group Selection, the different groups signify the following:

Group 1 - USAGE (always sent)

- User Name
- Call Start Date/Time
- Call End Date/Time
- Call Termination Reason
- Number Dialed - OUTGOING ONLY
- ANI-Incoming ONLY
- DNIS-Incoming ONLY

Group 2 - DATA TRANSFER

- Characters Sent
- Character Received
- Octets Sent
- Octets Received
- Blocks Sent
- Blocks Received
- Blocks Resent
- Characters Lost
- Line Reversals

Group 3 - PERFORMANCE

- Block CRC Errors
- Link NAKS
- Link Fallback
- Link Upshifts
- Link Timeouts
- Initial Link TX Rate

- Final Link TX rate
- Retrains Requested
- Retrains Granted

Group 4 - OPERATING MODE STATISTICS

- Sync/Async Mode
- Modulation Type
- Originate/Answer Mode
- Error control Type
- Data Compression Type
- HST Back Channel Rate
- Default DTE Data Rate
- High Freq Equal

8 If MD5 Calculation is to be performed, double-click the **LogMD5Calc** field, and then click **enable**.

By default, it is disabled.

9 If there are other backup logging servers, specify them in the Third, Fourth, Fifth, Sixth, Seventh, and Eighth Backup Logging Server. For example, the Third Backup Logging Server can be configured by typing the IP address in the **Log3SrvrAddr** field.

10 If the logging server has a logical host name, type it in the **LogSrvrName** field.

11 To view the current state of the logging server's host address DNS resolution, double-click the **LogDnsEna** field. By default, this setting is disabled.

Hub Security is Not Working

Use the following procedure to enable hub security on the Total Control 1000 chassis.

To enable hub security using the CLI:

1 Access the network management card CLI.

2 On the **Main Menu**, choose option **3** for **Feature Enable**.

3 On the **Feature Enable** menu:

```
Feature Enable

Current Features Enabled =

0000 0000 0000 0000 0000 0000 0000 0100

Press Esc to Exit or Return to continue.

Enter New Feature Enable String:
```

```
From here type the New Feature Enable string then press

ENTER. Please note: The string is 16 digits long.
```

4 On the **Main Menu**, type **1**.

5 Press **Enter** to access the **Configuration** menu.

6 On the **Configuration** menu, type **9** to access the **Save Configuration to Non-Volatile Memory** menu.

7 Press **Enter** to save the configuration to NVRAM.

8 Restart the network management card to activate the configuration changes.

9 To view the currently-enabled features, repeat **step 1** and see below for which feature(s) are enabled:

The following feature enable string verifies that you have **AutoResponse**. This is automatically enabled by default:

```
Current Features Enabled =

0000 0000 0000 0000 0000 0000 0000 0100
```

10 Press **Esc** to Exit, or **Return** to continue.

11 Enter New Feature Enable String:

```
Current Features Enabled =

0000 0000 0000 0000 0000 0000 0000 0101
```

The feature enable string above verifies that **AutoResponse** and **Hub Security** is installed.

```
Current Features Enabled =

0000 0000 0000 0000 0000 0000 0000 0110
```

This above string shows that **AutoResponse** and the **Cellular** feature is installed.

```
Current Features Enabled =

0000 0000 0000 0000 0000 0000 0010 0100
```

The feature string above shows that both **AutoResponse** & **x2/V.90** are enabled.

If you have DSP multispan cards, you will not need a feature enable key; these cards automatically have X2/V.90 enabled on them.

```
Current Features Enabled =

0000 0000 0000 0000 0000 0000 0010 0111
```

The above string verifies that **all options** are enabled.

Problems with the Network Management Card Retaining Settings

If Auto Configuration on Card Initialization is enabled on your system, the network management card may not retain the proper settings. This setting allows the network management card's NVRAM to overwrite the DSP multispan's NVRAM in the following situations:

- Network management card is reinstalled
- DSP multispan card is reinstalled
- Hardware is reset
- Chassis power-up

Check the Auto Configuration on Card Initialization setting on the network management card. This setting should be disabled.

Common Element Manager

To disable Auto Configuration on Card Initialization using common element manager:

1. From the **Explorer** tab, click the network management card.
2. From the **Configuration** tab, double-click the **PowerUpAutoCfgEnable** field and click **disable** from the drop-down list.
3. Click **Save all**.
4. Right-click the network management card, and select **Configuration**.
5. From the **Configuration** menu, click **Chassis save to NVRAM**.

Total Control Manager

To verify Auto Configuration on Card Initialization is disabled using total control manager:

1. Click the network management card.

   The card turns blue.
2. From the **Configure** menu, click **Programmed Settings**. The NMC Card Programmed Settings window appears.
3. From the Parameter Group box, click **Configuration Group**. The Auto Configuration on Card Initialization settings appear.
4. If this feature is not disabled, click **disable** and then click **Set**.
5. Save the settings to the chassis NVRAM.
   a. Click the network management card.

      The card turns blue.
   b. From the **Configure** menu, click **Actions/Commands**. The total control manager Commands window appears.
   c. In the second Command to Execute box, click **Save Chassis to NVRAM**.
   d. Click **Execute**. The Command Status area displays a completion report.

This feature is not configurable using the CLI.

5 DSP MULTISPAN AND HIPER DSP TROUBLE LOCATING AND CLEARING

This chapter includes information regarding installation, initial configuration, and DSP multispan Network Application Card (NAC) trouble locating and clearing information.

Overview

The DSP multispan card set includes a front-loaded NAC and an associated rear-loaded NIC. Depending on your application needs, the DSP multispan NAC/NIC card set provides Wide Area Network (WAN) ingress access through four T1 spans located on a DSP multispan T1 NIC or three E1 spans located on a DSP multispan E1 NIC.

Incoming calls terminate on highly integrated modems found within the DSP multispan. Users receive WAN access either through Pulse Code Modulated (PCM) encoded analog calls converted to baseband or through ISDN digital data calls.

Once modems process analog and digital calls, the DSP multispan NAC passes the data across the Packet Bus to the access router card. The access router card performs encryption and standard routing functions.

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

DSP Multispan NAC Faceplate

Figure 28 shows the Light Emitting Diodes (LEDs) for the DSP multispan NAC and Table 14 lists the descriptions for each LED.

Figure 28 DSP Multispan NAC Faceplate

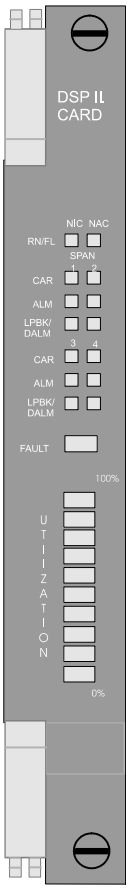


Table 14 lists DSP multispan Faceplace LEDs.

Table 14 DSP Multispan NAC LED Descriptions

LED	Color	Description
RN/FL	green	Card has completed the Power On Self Test (POST).
	flashing green	Diagnostics running or downloading code.
	red	Card failed.
	flashing yellow	Flash programming.
CAR	off	Card has received no signal or poor signal.
	green	Card has received good carrier.
	red	Card has received bad carrier.
	yellow	Card has received remote alarm.
ALM	off	No alarm or remote frame alarm (RFA).
	red	Alarm present.

Table 14 DSP Multispan NAC LED Descriptions (continued)

LED	Color	Description
LPBK/DALM	off	Span is CHT1, or E1/R2, or NFAS with no D-channel.
	green	Green: D-channel is up (PRI mode). Flashing green: Backup D-channel is up (NFAS).
	red	D-channel is down (PRI mode).
	yellow	Loopback test in progress (all modes).
FAULT	yellow	There is a problem in one or more modems.
	red	There is a critical problem in one or more modems, or the NAC in general.
	none	The modems are configured correctly
UTILIZATION	off	Modems are not in use.
	green	Modems in use; the ten utilization LEDs indicate the percentage of modems on DSP multispan in use (0-100%).

Verifying Software Version Numbers

Before you perform any trouble locating and clearing, ensure you are using the correct DSP multispan software version. Check this version number with the published version number in the Total Control 1000 Enhanced Data System System 4.5 GA System Release Notes. You will need to know this number if you contact Commworks Technical Support.

Common Element Manager

To verify the DSP multispan software version using common element manager:

1. From the **Explorer** tab, click the DSP multispan card.
2. From the Properties tab, click the **Identification** tab.
3. Check the **Version** field for the current software number.

Total Control Manager

To verify the DSP multispan software version using total control manager:

1. From total control manager's Virtual Front Panel Display (VFPD), select the DSP multispan card.

   The card turns blue.

2. From the main menu, click **Configure** and then click **Programmed Settings**.

   The Select Card Level or Template(s) window appears.

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

   The DSP MultiSpan Card Programmed Settings window appears.

4. From the Parameter Group drop-down menu, select **DSP Multispan Identification** to query data from the DSP multispan card.
5. Check the **Software Version** field for the current software version.

Command Line Interface

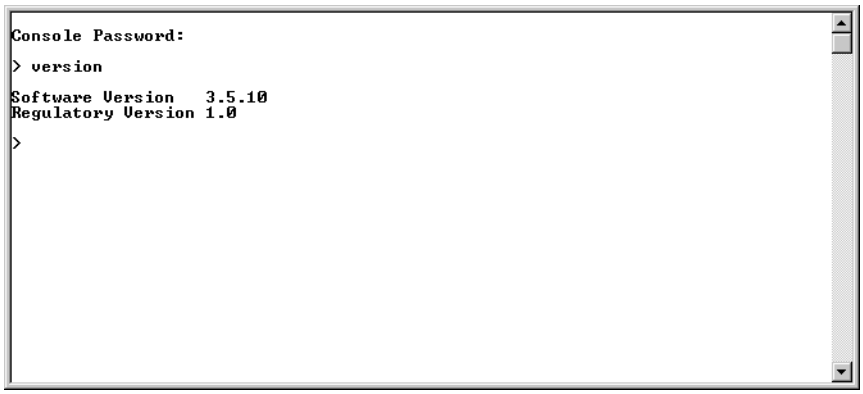
To verify the DSP multispan software version using the Command Line Interface (CLI):

From the DSP multispan CLI, enter the following command from any command prompt level:

```
> version
```

Figure 29 displays the CLI output for the DSP multispan.

Figure 29 DSP Multispan Software Verification - Command Line Interface



Initial Configuration Trouble Locating and Clearing

Table 15 lists problems and possible solutions that may occur during initial configuration.

Table 15 DSP Multispan - Initial Configuration Errors

Physical State	Carrier LED State	Alarm LED State	Loop-back LED State	Alarm/ Error	Diagnosis/Trouble Clearing
F1	Green	Off	Off	No Alarm	N/A
F2	Red	Off	Off	Yellow Alarm Remote Frame Alarm	The remote end has lost the DSP multispan NAC's framing or signal and sends this alarm to the DSP multispan NAC.
F3	Off	Red	Off	Red Alarm Loss of Signal	The received T1 or E1 signal has been lost. The DSP multispan NAC declares a red alarm and sends a yellow alarm to the remote end.
F4	Off	Red	Off	Red Alarm Out of Frame	The received T1 or E1 framing has been lost and the framed payload can no longer be received. The DSP multispan NAC declares a red alarm and sends a yellow alarm to the remote end.

Table 15 DSP Multispan - Initial Configuration Errors (continued)

Physical State	Carrier LED State	Alarm LED State	Loop-back LED State	Alarm/ Error	Diagnosis/Trouble Clearing
F5	Green	Red	Off	Blue Alarm Unframed all ones	The remote end is sending out an all ones signal. This is usually done when the remote end can not send out a framed signal.
F6	Green	Red	Off	Blue Alarm Unframed all ones	The DSP multispan NAC has received excessive CRC errors in a one second period and declares state F5. For E1-PRI certification this is less than 931 errors in one second.
	Green	Off	Red	D-Channel down	
	Green	Off	Amber	Look Back in progress	
F1	Green	Off	Off	No Alarm	

x2 / V.90 Trouble Locating and Clearing

Use the following sections to determine why the DSP multispan will not negotiate x2 / V.90.

V.90 Server Connections

If your DSP will not negotiate V.90, you may have an analog line or a line-side T1 connection between the CO and PSTN, i.e., additional analog-to-digital connections may exist in the signal path. If so, V.90 will not function. Also, client devices will not connect to DSP at V.90 speeds if the DSP multispan is not configured correctly.

Use Table 16 to trouble clear V.90 server problems:

Table 16 V.90 Server Problems

Possible Problem	Solution
The telephone company may have a line-side T1 connection.	Contact your local telephone company for information about obtaining a pure digital service. You can obtain a pure digital service by deploying either a PRI or *trunk-side* T1 connection to the PSTN.
DSP may be configured incorrectly.	Ensure you configured the S-registers properly. Verify the following settings are enabled: ■ V.90 ■ V.8

If V.90 server connections still do not work, contact CommWorks Technical Support. Contact information is in the *About This Guide* section of this guide.

Trouble Clearing V.90 Client Connections

If some client modems connect to the modem at V.90, and some do not, use the following section to trouble clear V.90 client connections.

Common Element Manager

To determine if some client modems are connecting, and some are not, using common element manager:

1. From the **Explorer** tab, double-click the DSP multispan card.
2. Double-click a desired span.

   The span expands to reveal all associated timeslots/modem channels.
3. From the **Properties** tab, click the **Statistics** tab.
4. Check the **X2Status** field to view the current status of x2/V.90 negotiation.

   Table 17 lists x2/V.90 statistics and their descriptions.

Table 17 DSP Multispan Modems - x2 Status

Statistic	Description
x2v90NotOperational	x2 / V.90 is not operational
x2Operational	x2 is operational
v8DisabledLocal	V.8 is disabled on the DSP
x2DisabledLocal	x2 is disabled on the DSP
baud3200DisabledLocal	3200 baud is disabled on the DSP
speedLimitedLocal	The transmit speed is limited on the DSP
v8notDetectedFromRemote	DSP did not detect V.8 on the remote device
x2notDetectedFromRemote	DSP did not detect x2 on the remote device
incompatibleX2Versions	DSP and the client are using incompatible x2 versions
incompatibleX2Modes	DSP and the client are using incompatible x2 modes
baud3200DisabledRemote	3200 baud is disabled on the remote device
excessiveHFAttenuation	DSP detects excessive High Frequency attenuation
channelNoSymbolRate	An attempt to make an x2 or V.90 connection was not successful because the PSTN channel between the two modems does not support a symbol rate required by x2 (3200) or V.90 (3000, 3200, 3429)
exitBeforeX2Connect	The call disconnected before DSP and the client connected using x2
v90Operational	V.90 is operational
x2v90Operational	x2 and V.90 are operational
v90DisabledLocal	V.90 is disabled on the DSP
x2v90DisabledLocal	x2 and V.90 are disabled on the DSP
v90SymRatesDisabledLcl	An attempt to make a V.PCM connection was not successful because all V.90 symbol rates (3000, 3200, & 3429) are disabled in the local modem
v90NotDetectedFrmRemote	DSP did not detect V.90 on the remote device
x2v90NotDetectedFrmRmt	DSP did not detect x2 and V.90 on the remote device

Table 17 DSP Multispan Modems - x2 Status (continued)

Statistic	Description
incompatibleV90Versions	DSP and the client are using incompatible V.90 versions
incompatibleV90Modes	DSP and the client are using incompatible V.90 modes
v90IncompactibleSymRate	An attempt to make a V.90 connection was not successful because no V.90 symbol rate (3000, 3200, & 3429) was supported in common by both modems

Trouble Clearing

If some V.90 client modems cannot connect to your DSP at V.90 speeds, use Table 18 for trouble clearing.

Table 18 V.90 Client Modem Trouble Clearing

Possible Problem	Solution
V.90 may not be enabled on the client modem.	Refer the *Operations Guide* for more information on V.90.
The client modem may not have the proper V.90 software.	Determine what client software the user needs.
The V.90 client modem may be connected to the public network via a PBX or other telephone equipment with more than one analog-to-digital conversions.	Reduce the number of analog-to-digital conversions in the signal path.
The client modem may not be configured properly.	Verify the following settings are enabled: ■ V.90 ■ V.8
Line noise.	Disconnect any other devices that share the analog line and check for line noise. ***Note**: Refer to the section below*—Testing for Line Noise.

Testing for Line Noise

1 Disconnect all other phones, answering machines, caller ID boxes, and modems, from all telephone wall jacks at the location. Use a telephone cable between the modem and a wall jack.

Telephone cable extenders and Y-adapters, if defective, have adverse affects on connections. Also, multiple devices sharing the same line may affect V.90 performance, especially if they are daisy-chained. Disconnect the other devices and connect the modem directly to the wall jack.

2 Noise from electrical wires and appliances often cause problems. Plug a telephone into the same jack your modem is connected to and press (or dial) a single number to end the dial tone, then listen carefully. If you hear a low frequency hum on the line, that is caused by the phone wires coming near electrical wires or appliances. Often the wires and/or appliances are physically very close to the modem. Separate the phone wire from power cables, surge suppressor, etc.

Also, a *hum* or *buzz* may be introduced somewhere between your home and the telephone company. Most modern installations in the US, and elsewhere, provide a box at the back the home that allows you to disconnect your house wiring and plug in with a standard RJ-11 cable directly to the phone line. If possible, connect a phone to the telephone company's connection box at the back of your/the customer's home, and perform the same test. This will isolate noise sources within your home. If the excessive noise is present, then you need to contact your telephone company's repair service.

When contacting the telephone company's repair service, avoid emphasizing modem problems. Focus on the voice problems, and telephone company will generally address the issue.

3 Use the same technique from the previous step. If you hear scratchy noise on the line, this will affect modem performance. This can be caused by poor connections in the home or office, but often it is because of poor connections on phone poles or other connecting points. Use the same test methods as above to isolate whether this is a problem in your house wiring, or with telephone company facilities.

Problems with Configurations

If you are losing modem configurations:

- Review the sections in the *Operations Guide* pertaining to memory and templates. You may not be saving the settings properly.
- Check the network management card settings. If **Auto Config on Card Initialization** is enabled, the network management card will automatically configure the card using the settings in the network management card NVRAM. It will overwrite the DSP multispan settings stored in the DSP multispan NVRAM.

To save the DSP multispan *to the network management card NVRAM, use the* ***Save Chassis to NVRAM*** *feature in the command line.*

- Check your access router card. Total Control access router cards send initialization strings to DSP multispan modems. These initialization strings overwrite current modem configurations.

  For example, the access router card automatically configures modems to its requirements upon initialization of the packet bus. Every time a packet bus session is opened, the access router card sends the following the initialization string to the modem on the other side of the session:

  ATH0S0=0S72.0=1E0Q0V0&A0&K1&L0&N0&TX0S47.5=1S2=255

  That initialization string is hard coded into the access router card, and it represents:

  H0—Hang up a call, if one is currently active.

  S0=0—Rings for Auto Answer.

S72.0=1—Sets the modem to ignore ATZ command over the packet bus and sends an OK.

E0—Do not echo DTE data.

Q0—Display result codes.

V0—Set numeric result codes.

&A0—ARQ result codes disabled.

&K1—Data Compression Mode = auto.

&L0—Normal phone line (as opposed to Leased Line, &L1).

&N0—Link Rate Speed Select.

&T—Take the modem out of ITU-T V.54 test modes.

X0—Set result code options to basic result codes.

S47.5=1—Force gateway NAC routing. Force all call output to packet bus only.

S2=255—Escape character disabled.

To check the initialization string settings of your access router card, refer to the Operations Guide, or refer to the TOTALservice website.

Performing Modem Tests

To perform Modem Tests using total control manager:

1. On the **Main Menu** bar, click **Fault**, and then click **Modem Tests**.
2. In the Modem Loopback/Self Test dialog box, type the slot number in the Testing with card in Slot box.
3. Type a value in the Channel box.
4. Select the test to execute.
5. In the Polling Interval spinbox, designate the number of seconds between polling.
6. Click **Start** to execute the test.

   Total control manager displays the results and errors in the corresponding fields.

Using Remote Testing

To use Remote Testing using total control manager:

1. On the **Main Menu** bar, click **Fault**, and then click **Remote Testing**.
2. In the Remote Testing dialog box, click test to run.
3. Configure the test using the window for the selected test.
4. Click **Start** to run the test.

Call Fails

Use Table 19 to trouble clear call fails:

Table 19 Call Fails Trouble Clearing

Call Fail	Description	Trouble Clearing Notes
N/A	DSP drops calls immediately.	Save the following settings to the modems' NVRAM. Call Control Option: Setting Result Codes (Qn): displayResult Verbal/Numeric Result Codes (Vn): verbal Result Code Groups (X): 0 ARQ Result Codes (&A): arqResultsDisabled Response to +++: ignoreEscCode
N/A	Analog calls fail connect attempts.	Verify you the telephone company is providing an analog/digital PRI service. If they are providing a digital service only, no analog calls will connect.
N/A	A client modem connects to the DSP, and the DSP then sends the username and password to the RADIUS server. The RADIUS server replies to the access router card accepting the signal, but the call is dropped, and the DSP never receives a ny data.	You may have configured DSP incorrectly. **1** Verify you are using the most recent software versions **2** From the common element manager explorer, select the DSP multispan. **3** Right-click the DSP multispan, and select **Software** from the drop-down menu. and then click **Restore factory defaults**. **4** Save to NVRAM. **5** Reset the DSP multispan hardware.
Keypress Abort	The modem detected a keypress while training.	The remote modem user is responsible.
MNP incompatibility	The modem is set to &M5 and the remote modem does not have MNP capability, or there was an MNP negotiation procedure error.	Route the user to a modem with MNP disabled.
Invalid speed	The modem is set to a specific speed or a range of speeds and the remote modem is not operating at the same rate.	Route the remote modem's signal to another modem with the same rate or reconfigure the modem's rate.
XID Timeout	The modems failed to negotiate the V.42 Detection (XID Exchange) phase.	N/A
SABME Timeout (Set Asynchronous Balance Mode Extended)	The modems failed this part of V.42 link negotiation.	Set asynchronous balance mode extended.

Modem Disconnects

Use Table 20 to trouble clear modem disconnects:

Table 20 Modem Disconnect Trouble Clearing

Disconnect Reason	Description	Trouble Clearing Notes
Escape code	The operator sent the modem the +++ escape code.	The remote modem user is responsible.
GSTN (General Switch Telephone Network) Clear Down	The connection was non-ARQ and DTR was dropped from one side of the connection, or the DISC frame was corrupted due to noise.	If the call is not dropped deliberately by either party, try connecting again. If the call disconnects repeatedly, try a lower connection speed.
Loss of carrier	The modem detected loss of the remote modem's carrier and waited the duration specified in S10 (default is 0.7 seconds).	Sometimes call waiting signals can interrupt a remote modem's carrier, thus a longer duration should be specified in S10—preferably 2 seconds.
Inactivity timeout	The modem detected no activity on the line for the duration specified in S19 (default is 0, timer disabled).	If necessary, specify a longer duration in S19.
Retransmit limit	The modems reached the maximum of twelve attempts to transfer a data frame without error.	Study the data frame errors to further diagnose the problem.
LD received	The remote modem sent an MNP error control Link Disconnect request.	The remote modem may have sent an unauthorized +++ATH or it may have dropped DTR.
DISC	The remote modem sent a V.42 Disconnect frame.	This reflects normal operation, but it can also reflect a user software error. The user software may issue an unauthorized +++ATH or it may drop the DTR on the remote modem.
Loop loss disconnect	The modem detected a loss of current on the loop connecting it with the telephone company central office.	This usually occurs because the remote modem has hung up.
Unable to Retrain	After several attempts, disturbances on the phone line prevented the modems from retraining, and they could no longer transmit or receive data.	Resolve phone line disturbances with the telco.
Break Timeout	Incompatible processing of a Break signal occurred.	Try connecting again.
Invalid Codeword	The modem received an invalid V.42 bis frame.	This disconnect reason is very infrequent.
A Rootless Tree	The modem received an invalid V.42 bis frame.	Try connecting again. If this fails repeatedly, tryp MNP or normal mode instead of V.42 / V.42 *bis*.
Illegal Command Code	The modem received an invalid V.42 bis frame.	This disconnect reason is very infrequent.
Extra Stepup	The modem received an invalid V.42 bis frame.	N/A
Normal User Call Clear	The network cleared a call when it received a disconnect from a gateway card.	This is a Q931 telco clear condition.

Table 20 Modem Disconnect Trouble Clearing (continued)

Disconnect Reason	Description	Trouble Clearing Notes
Modem On Hold Cleardown Request Received	V.92 client initiated a disconnect.	Normal disconnect or the client expected more on-hold time negotiated. If necessary, increase on-hold threshold in S-Register 78.
Modem On Hold Teardown	V.92 client violated Modem On Hold handshake.	Report client model and software version to CommWorks Customer Support.
Modem On Hold Timeout	Instance timer threshold or total timer threshold reached.	If necessary, increase on-hold thresholds in S-Register 78.

If a modem makes contact with another modem, but cannot complete protocol and speed negotiations, CommWorks considers this a call fail, not a modem disconnect.

Physical Layer Trouble Locating and Clearing

When trouble clearing the span, first determine if the physical layer is functioning properly.

The following are basic trouble locating suggestions:

- View LEDs
- Check the physical state
- Check the line status

Viewing DSP Multispan LEDs

View the T1/E1 related LEDs to determine if the systems displays an alarm. If the following LED colors appear, the physical layer is functioning properly.

Table 21 T1/E1 Related LEDs - DSP Multispan

LED	Color	This has occurred
RN/FL	green	Card has performed the Power On Self Test (POST)
CAR	green	Card has received good carrier
ALM	off	No alarm or Remote Frame Alarm (RFA)

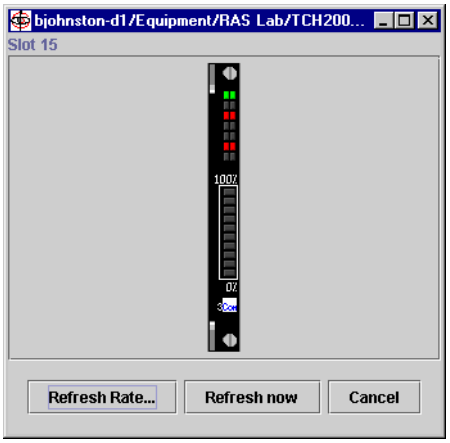
Common Element Manager

To view DSP multispan LEDs remotely using common element manager:

1. From the **Explorer** tab, click a desired DSP multispan card.
2. From the **Main Menu**, click the Device Mimic icon to display a graphical representation of the DSP multispan card.

Figure 30 displays the graphical representation of the DSP multispan NAC using common element manager:

Figure 30 Common Element Manager Device Mimic - DSP Multispan NAC



Checking the Physical State

When the physical layer is functioning properly, *psF1Operational(1)* displays. Use the following procedures to check the physical state.

Common Element Manager

To check the physical state using common element manager:

1. From the **Explorer** tab, click a desired DSP multispan card.
2. Select the desired span and click the **Statistics** tab.
3. Check the **E1PhysicalState** field for a description of the current physical state.

The following are physical states for a DSP multispan span:

- psF1Operational
- psF2Fc1RaiTempCrcErrors
- psF3Fc2LossOfSignal
- psF4Fc3AlarmIndSignal
- psF5Fc4RaiContCrcErrors
- psF6PowerOn

Command Line Interface

To check the physical state using the CLI:

1. From the DSP multispan CLI, enter the following command to move to the span level:

   > **chdev span x**

   where x is the span number.

2 Enter the following command at the span level command prompt:

```
display physst
```

Checking the Line Status

If the Line Status column displays 1, the T1/E1 line is operational and the physical layer is functioning properly.

Common Element Manager

To check line status using common element manager:

1 From the common element manager explorer, select a DSP multispan.

2 Select the E1 span, and then click the **Configuration** tab.

3 On the Configuration tab, right-click **LineStatus** and click **Monitor**.

The Monitor Line Status window appears.

Figure 31 Monitoring Line Status - DSP Multispan

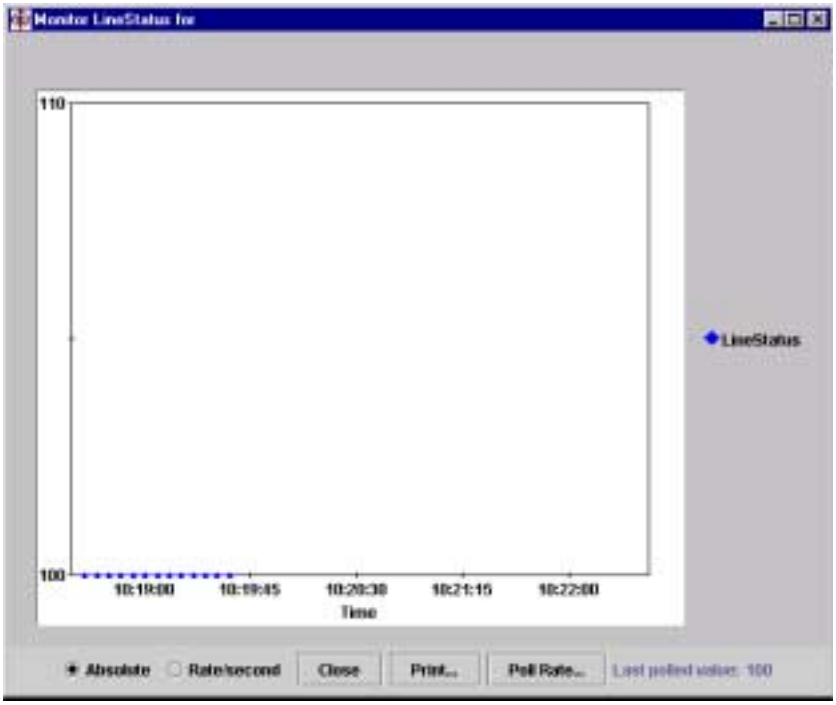


Table 22 contains a list of the Line Status displays and descriptions, as well as related trouble clearing notes.

Table 22 DSP Multispan Line Status

Line Status	Description	Trouble Clearing Notes
1	No Alarm Present.	The line is functioning properly.
2	Far end Loss of Frame (LOF), i.e., Yellow Alarm.	The remote end is not receiving the modem's transmit signal or cannot frame up on the signal.
		Ensure the line type (dsx1LineType) is set correctly.

Table 22 DSP Multispan Line Status (continued)

Line Status	Description	Trouble Clearing Notes
4	Near end sending LOF Indication.	Ensure the line type (dsx1LineType) is set correctly.
8	Far end sending AIS.	This indicates problems with the remote system. If problems persist, contact your telephone company.
		If possible, verify that the remote system has no alarms and the error statistics are not growing.
16	Near end sending AIS.	If the modem NAC is unplugged or reset, the modem NIC will transmit all ones (AIS).
		If the modem NAC is not unplugged or reset, contact CommWorks Technical Support.
32	Near end LOF (a.k.a. Red Alarm).	Ensure the line type (dsx1LineType) is set correctly.
64	Near end Loss Of Signal.	Ensure the span line is connected correctly to the modem NIC and other T1/E1 equipment.
		Verify the T1/E1 cable is the correct type and wired correctly.
		Verify that the NIC interface is correct (long or short), the Line build out (long haul) is set correctly, and the cable distance setting (short haul) is correct.
128	Near end is looped.	N/A
256	E1 TS16 AIS.	N/A
512	Far End Sending TS16 LOMF.	N/A
1024	Near End Sending TS16 LOMF.	N/A
2048	Near End detects a test code.	A remote system is performing a test.
4096	Any line status not defined here.	Contact CommWorks Technical Support. Refer to the *About This Guide* section of this guide for information about contacting CommWorks.

Command Line Interface

To check line status using the CLI:

1 From the DSP multispan CLI, enter the following command to move to the span level:

> **chdev span x**

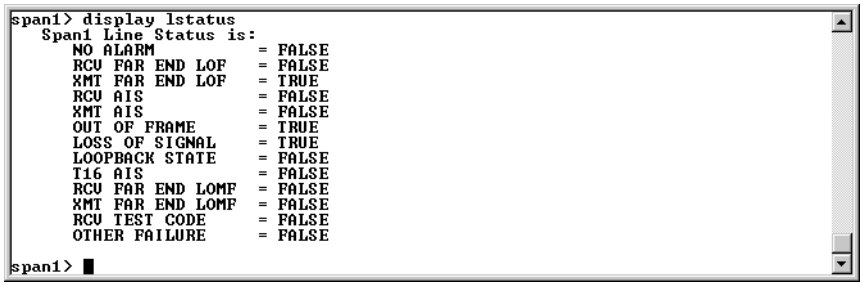
where x is the span number.

2 Enter the following command at the span level command prompt:

display lstatus

Figure 32 displays the CLI output for line status descriptions on the DSP multispan card:

Figure 32 DSP Multispan - CLI Line Status Command



Checking the Received Error Statistics

Check the Received Error statistics (current, interval, or total) on the span line. The modem displays the error statistics in real time.

If checking the current line status, verify that the error statistics are not growing.

Common Element Manager

To check the received error statistics using common element manager:

1. From the **Explorer** tab, double-click the desired DSP multispan.
2. Select a desired span and click one of the following tabs, depending on your customized needs:
   - Near End Current
   - Near End Interval
   - Near End Total
   - Far End Current
   - Far End Interval
   - Far End Total
3. On the selected tab, you can view the following settings:
   - BESs—Bursty Errored Seconds
   - CSSs—Controlled Slip Seconds
   - DMs—Degraded Minutes
   - ESs—Errored Seconds
   - LCVs—Line Code Violations
   - LESs—Line Errored Seconds
   - PCVs—Path Coding Violations
   - SEFSs—Severely Errored Framing Seconds

- SESs—Severely Errored Seconds
- UASs—Unavailable Seconds

If the Near End Current Group error statistics are growing, ensure the dsx1LineCoding is set correctly (For example, AMI instead of B8ZS).

Command Line Interface

To check the received error statistics using common element manager:

1 From the DSP multispan CLI, enter the following command to move to the span level:

> **chdev span x**

where x is the span number.

2 Enter the following command at the span level command prompt:

display near <stat_type>

Replace <stat_type> with one of the following, depending on your customized needs:

Table 23 Display Near End Span Statistics

Command	Description
current	Displays near end current span statistics
total	Displays near end total span statistics
interval	Displays near end interval span statistics

Ordering and Setting Up a Span Line

When you order a span line from the telephone company, make sure you know the answers to the following questions:

1 What is the line type (dsx1LineType)?

2 What is the line coding (dsx1LineCoding)?

3 What is the interface type (long or short haul)?

4 What will be the length of the T1/E1 cable from the modem to the other T1/E1 device? Set the transmit line build out (long haul) or short haul cable distance (short haul) to match. If setting up for T1-PRI, the modem must have the line coding set to B8ZS. Most telephone companies won't offer any other choice for line coding.

6 DS-3 INGRESS TROUBLE LOCATING AND CLEARING

This chapter includes information regarding installation and system trouble locating and clearing information regarding the DS-3 ingress card set.

Overview

The DS-3 ingress NAC is part of the Total Control® 1000 Enhanced Data System, providing Wide Area Network (WAN) ingress options for the DSP multspan modem system.

The DSP multispan NAC possesses a four span modem architecture containing 96 port options for T1 applications and a three span modem architecture containing 90 port options for E1 applications. You have the choice of providing WAN ingress access via four T1 spans (or three E1 spans) on a DSP multispan Network Interface Card (NIC) or one T3 span on the DS-3 ingress NAC/NIC card set. This allows you to configure and manage your Total Control 1000 Hub according to your customized needs.

DS-3 Ingress NAC Faceplate

The DS-3 ingress NAC has the following physical interfaces on the card's front panel. You can find a more detailed description of each interface in the sections following Table 25.

Table 24 DS-3 Ingress NAC Faceplate

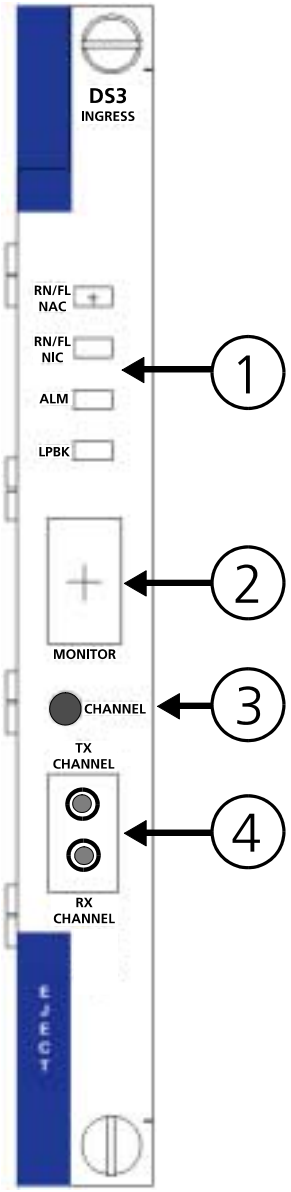


Table 25 describes each interface on the DS-3 ingress card.

Table 25 DS-3 Ingress NAC Faceplate Interfaces

Callout	Interface
1	RN/FL NAC Status LED Indicator
	RN/FL NIC Status LED Indicator
	ALM Status LED Indicator
	LPBK Status LED Indicator
2	Monitor Port LED Indicator
3	Channel Line Pushbutton
4	Dual Bantam Jack

Status LED Indicators

The DS-3 ingress NAC front panel contains two types of Light Emitting Diode (LED) indicators that are useful for locating and monitoring problems. The four status LEDs located at the top of the front panel may be off, red, green and amber, and are used to indicate status within a chassis environment.

Monitor Port LED Indicator

The Monitor Port LED Indicator has a four-character, seven-segment display. The first character displays the DS3 line status. The middle two characters display the currently selected DS1 channel line (1 to 29 where 29 is the BITS span) for the Dual Bantam Jack. The last character displays the current status of the selected DS1 line.

The format of the first and fourth characters is:

- Blank—No Alarm; the system is operational or in power up mode
- A—Alarm Indication Signal (AIS); Unframed All Ones Alarm
- R—Remote Alarm Indicator (RAI); Remote Frame Alarm
- L—Loss of Signal (LOS)
- Q—Quasi-Random Signal Source (QRSS)

Channel Line Pushbutton

A Channel Line Pushbutton switch selects which DS1 channel to monitor in one number increments and is shown on the Monitor Port LED Indicator to display the selected DS1 channel.

Dual Bantam Jack

The DS-3 ingress NAC has a dual bantam jack outlet located on the front panel of the card. You can monitor status of both the transmit (Tx) and receive (Rx) paths on any DS1 signal. Use the Channel Line Pushbutton or total control manager to select the desired DS1 line.

Verifying Software Version Numbers

Before you perform any trouble locating and clearing, ensure you are using the correct DS-3 ingress software version. Check this version number with the published version number in the Total Control 1000 Enhanced Data System System 4.5 GA System Release Notes. You will need to know this number if you contact Commworks Technical Support.

Common Element Manager

To verify the DS-3 ingress software version using common element manager:

1. From the Explorer tab, click the DS-3 ingress card.
2. From the Properties tab, click the **Identification** tab.
3. Check the **Version** field for the current software number.

Total Control Manager

To verify the DS-3 ingress software version using total control manager:

1. From total control manager's Virtual Front Panel Display (VFPD), select the DS-3 ingress card.

   The card turns blue.
2. From the main menu, click **Configure** and then click **Programmed Settings**.

   The DS3 Ingress card Programmed Settings window appears.
3. From the Parameter Group drop-down menu, select **DS3 Ingress Identification** to query data from the DS-3 ingress card.
4. Check the **Board Manager Software Revision** field for the current software version.

Command Line Interface

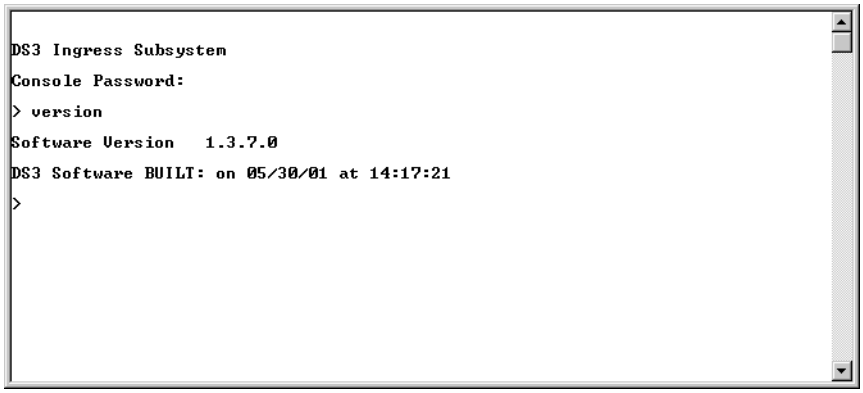
To verify the DS-3 ingress software version using the Command Line Interface (CLI):

From the DS-3 ingress CLI, enter the following command from any command prompt level:

```
> version
```

Figure 33 displays the CLI output for the DS-3 ingress.

Figure 33 DS-3 Ingress Software Verification - Command Line Interface



Normal Operational Mode

In normal operational mode, the LEDs on the DS-3 ingress NAC display the following indicator lights:

Table 26 DS-3 Ingress Operational Mode

LED	Description
RN/FL NAC	Green
RN/FL NIC	Green
ALM	No Light
LBK	No Light

Installation Trouble Locating and Clearing

The following section details problems and possible solutions that may occur during installation.

Table 27 DS-3 Ingress Installation Light Emitting Diodes (LED) Errors

Trouble Locating	Possible Cause	Trouble Clearing
RN/FL LED is showing no indicator light	Loss of power	Check power cable
RN/FL LED is solid red	Improper installation	Remove NAC and reinstall
RN/FL is flashing red	The NAC did not detect a Network Interface Card (NIC)	Install the NIC directly behind the NAC — refer to the NIC's Getting Started Guide

Initial Configuration Trouble Locating and Clearing

The following section describes problems and possible solutions that may occur during initial configuration. Refer to Table 28 for more information.

Table 28 DS-3 Ingress - Initial Configuration Errors

Physical State	Alarm LED State	Loopback LED State	Alarm/Error	DS3 Diagnosis/Trouble Clearing	DS1 Diagnosis/Trouble Clearing
F1	Off	Off	No alarm	N/A	N/A
F2	Yellow	Off	Yellow Alarm (Remote Frame Alarm)	The remote end has lost the DS3 framing or signal and sent this alarm to the DS3 NAC.	The remote end has lost the DS1 framing and sent this alarm to the DS3 NAC.
F3	Red	Off	Red Alarm (Loss of Signal)	The received DS3 signal has been lost. The DS3 NAC declares a red alarm and sends a yellow alarm to the remote end.	The received DS1 signal has been lost. The DS3 NAC declares a red alarm and sends a yellow alarm to the remote end.

Table 28 DS-3 Ingress - Initial Configuration Errors (continued)

Physical State	Alarm LED State	Loopback LED State	Alarm/Error	DS3 Diagnosis/Trouble Clearing	DS1 Diagnosis/Trouble Clearing
F4	Red	Off	Red Alarm (Out of Frame)	The received DS3 framing has been lost. The DS3 NAC declares a red alarm and sends a yellow alarm to the remote end.	The received DS1 framing has been lost. The DS3 NAC declares a red alarm and sends a yellow alarm to the remote end.
F5	Yellow	Off	Receive Blue Alarm Unframe all ones	The remote end is sending out an all-ones signal. This is usually done when the remote end can not send out a frame signal.	The remote end is sending out an all-ones signal. This is usually done when the remote end can not send out a frame signal.
F6	Off	Off	No Alarm	N/A	N/A
	Any	Green	DS3 Loopback in Progress	N/A	Loopback LED does not reflect the DS1 loopback state.

DS-3 Ingress NAC Trouble Locating and Clearing

The following section details problems and possible solutions for the DS-3 ingress NAC.

- Check the DS3 line configuration if the Monitor Port LED Indicator's first character shows an A , L or R. Specifically check the DS3 Line type, Primary timing reference, Secondary timing reference, Line coding, and Line length for each DS3 line.
- Check the DS1 span configuration if the Monitor Port LED Indicator's last character shows an A, L or R. Switch to the span where you observed the alarm by typing **chdev span x** (where "x" is the number of the span) from the CLI. Also, check the DS1 Line type, Line coding, D-channel operation, and Physical state. Check the span status by entering **ds3 1> display spnstatus** from the CLI.
- Check with the telephone company for correct DS3/DS1 line information if configuration failed.
- For DS-3 ingress and DSP multispan NAC configuration information, refer to the *Getting Started Guide*.
- Make sure the DSP multispan NAC has the proper **spansrc** and **clocksrc** to bring up the D-channels.

The following table describes the different operational states for the LED status indicators located on the front panel of the DS-3 ingress NAC.

Table 29 DS-3 Ingress Status LED Indicator Descriptions

LED	Color	Meaning
RN/FL NAC	blank	NAC loss of power
	green	NIC loss of power
		NIC and NAC operational
		received RAI
		Loss of signal
		Loss of Frame
		Received AIS
		Received RAI and CRC errors
		NIC power up
		Any loopback active
	red	NAC reset and boot
RN/FL NIC	blank	NAC loss of power
	green	NIC and NAC operational
		received RAI
		Loss of signal
		Loss of Frame
		Received AIS
		Received RAI and CRC errors
		NIC power up
		Any loopback active
	red	NAC reset and boot
		NIC loss of power
ALM	blank	NAC loss of power
		NAC reset and boot
		NIC loss of power
		NIC and NAC operational
	green	Any loopback active
	red	received RAI
		Loss of signal
		Loss of Frame
		Received AIS
		Received RAI and CRC errors
		NIC power up
		Any loopback active

Table 29 DS-3 Ingress Status LED Indicator Descriptions (continued)

LED	Color	Meaning
LPBK	blank	NAC loss of power
		NAC reset and boot
		NIC loss of power
		NIC and NAC operational
	green	received RAI
		Loss of signal
		Loss of Frame
		Received AIS
		Received RAI and CRC errors
		NIC power up
	red	Any loopback active

7 SDH STM-0 Converter Trouble Locating and Clearing

This chapter includes information regarding installation and system trouble locating and clearing information regarding the SDH STM-0 Converter card set.

This chapter includes the following topics:

Overview

The SDH STM-0 Converter NAC terminates a Sychronous Transport Module (STM-0) over an OC-1 optical fiber interface, de-maps 28 VC-11 mapped DS-1 signals, and multiplexes the 28 DS-1 signals into one DS-3 stream. The data then travels out through an external DS-3 cable from the SDH STM-0 Converter NIC to the DS-3 ingress NIC.

The DS-3 ingress NIC receives DS0 ingress signals (up to 672) from the single DS-3 line and passes this data to the DS-3 ingress NAC across a proprietary serial interface. These calls are terminated on DSP multispan modems. Once the modem processing is complete, the DSP multispan NAC passes the data across the Packet Bus to the access router card. The access router card performs encryption and standard routing functions.

SDH STM-0 Converter NAC Faceplate

The SDH STM-0 Converter NAC has the following physical interfaces on the card's front panel. You can find a more detailed description of each interface in the sections following Table 30.

Figure 34 SDH STM-0 Converter NAC Faceplate

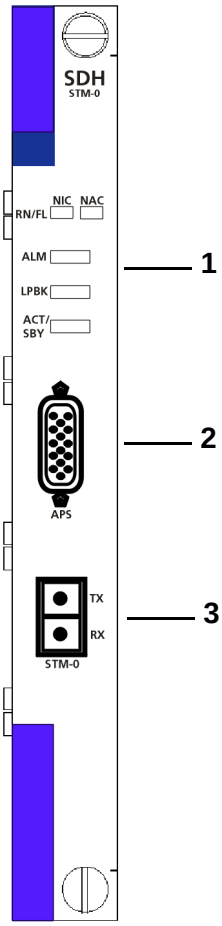


Table 30 lists each interface on the SDH STM-0 Converter card.

Table 30 SDH STM-0 Converter NAC Faceplace Interfaces

Callout	Interface
1	Run/Fail NAC Status LED Indicator
	Run/Fail NIC Status LED Indicator
	Alarm Status LED Indicator
	Loopback Status LED Indicator
	Active/Standby Status LED Indicator
2	APS Connection
3	STM-0 Transmit and Receive Ingress Ports

Status LED Indicators

The SDH STM-0 Converter NAC front panel contains five Light Emitting Diode (LED) indicators that are useful for locating and monitoring problems. The status LEDs located at the top of the front panel may be off, red, green, and amber, and are used to indicate status within a chassis environment.

APS Connection

A proprietary Automatic Protection Switching (APS) cable is provided with the SDH STM-0 Converter card set. This cable is required to facilitate switching between the active SDH STM-0 Converter card and the standby SDH STM-0 Converter card in a redundant configuration.

STM-0 Ingress Port

The STM-0 Ingress port is comprised of one receive and one transmit port, each of which uses an MU style connector. One STM-0/OC-1 optical fiber cable connects to each port.

Verifying Software Version Numbers

Before you perform any trouble locating and clearing, ensure you are using the correct SDH STM-0 Converter software version. Check this version number with the published version number in the Total Control 1000 Enhanced Data System System 4.5 GA System Release Notes. You will need to know this number if you contact CommWorks Technical Support.

Common Element Manager

To verify the SDH STM-0 Converter software version using common element manager:

1. From the Explorer tab, click the SDH STM-0 Converter card.
2. From the **Properties** tab, click the **Identification** tab.
3. Check the **Version** field for the current software number.

Total Control Manager

To verify the SDH STM-0 Converter software version using total control manager:

1. From total control manager's Virtual Front Panel Display (VFPD), select the SDH STM-0 Converter card.

   The card turns blue.
2. From the main menu, click **Configure** and then click **Programmed Settings**.

   The SDH Card Level Programmed Settings window appears.
3. From the Parameter Group drop-down menu, select **SDH Card Identification** to query data from the SDH STM-0 Converter card.
4. Check the **ID Board Manager Sw Rev** field for the current software version.

Command Line Interface

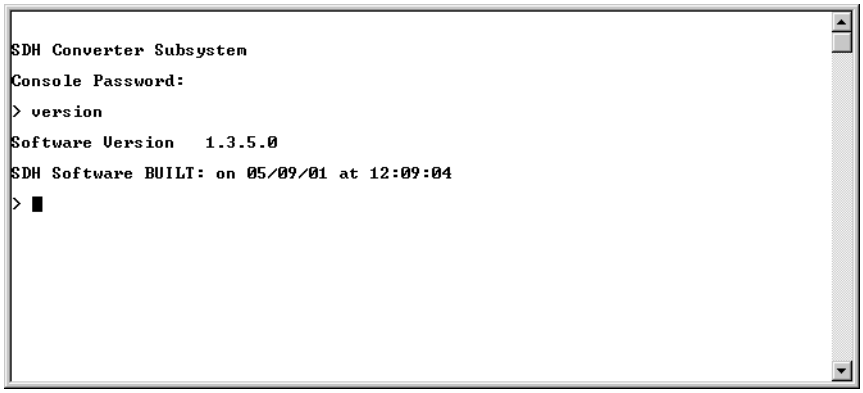
To verify the SDH STM-0 Converter software version using the CLI:

From the SDH STM-0 Converter CLI, enter the following command from any command prompt level:

```
> version
```

Figure 35 displays the CLI output for the SDH STM-0 Converter.

Figure 35 SDH STM-0 Software Verification - Command Line Interface



Normal Operational Mode

In normal operational mode, the LEDs on the SDH STM-0 Converter NAC display the following indicator lights:

Table 31 SDH STM-0 Converter Operational Mode

Active SDH STM-0 NAC	Standby SDH STM-0 NAC
RN/FL NAC - Green	RN/FL NAC - Green
RN/FL NIC - Green	RN/FL NIC - Green
ACT/SBY - Green	ACT/SBY - Amber
ALM - No Light	ALM - No Light
LBK - No Light	LBK - No Light

Installation Trouble Locating and Clearing

This section details problems and possible solutions that may occur during installation.

Table 32 SDH STM-0 Installation Errors

Trouble Locating	Possible Cause	Trouble Clearing
RN/FL NAC Light Emitting Diodes (LEDs) show no indicator lights	■ No power applied to chassis ■ SDH STM-0 Converter NAC is not installed properly	■ Make sure the power is applied to the chassis ■ If power is applied to the chassis and the LEDs on the other NACs in the chassis display indicator lights, try reinstalling the SDH STM-0 Converter NAC
RN/FL NAC LED is Red; no other LED shows activity	■ Serious hardware issues with the SDH STM-0 Converter NAC ■ No BIOS loaded ■ No Application code loaded	Contact CommWorks Technical Support
RN/FL NAC LED is Red; RN/FL NIC LED is Red	■ SDH STM-0 Converter NIC has been installed in the wrong chassis slot ■ SDH STM-0 Converter NIC is not installed properly ■ Serious hardware issues with the SDH STM-0 Converter NIC	Before contacting 3Com Technical Support, make sure an SDH STM-0 Converter NIC is installed in the correct chassis slot. If an SDH STM-0 Converter NIC is installed in the correct chassis slot, reinstall the NIC and reboot the SDH STM-0 Converter NAC.
RN/FL NAC is Amber for more than 30 seconds	No Application code loaded on the card	Contact CommWorks Technical Support

SDH System Trouble Locating and Clearing

This section details problems and possible solutions for problems within the SDH 1.0 System.

Table 33 SDH System Problems

Trouble Locating	Possible Cause	Trouble Clearing
Alarm LED on the SDH STM-0 Converter NAC is red; Monitor Port LED on the DS-3 Ingress NAC displays the letter "L" (short for **LOS**)	■ SDH STM-0 Converter NIC and DS-3 Ingress NIC are not cabled correctly	First of all, make sure the DS-3 Ingress NAC and NIC are installed properly in the Total Control 1000 chassis. Next, check and make sure the DS-3 cable from the DS-3 transmit port located on the SDH STM-0 Converter NIC is properly connected to the DS-3 receive port located on the DS-3 Ingress NIC. Refer to the *Getting Started Guide* for detailed cabling instructions.
Alarm LED on the SDH STM-0 Converter NAC is red; Monitor Port LED on the DS-3 Ingress NAC displays the letter "R" (short for **RAI**)	■ SDH STM-0 Converter NIC and DS-3 Ingress NIC are not cabled correctly	First of all, make sure the DS-3 Ingress NAC and NIC are installed properly in the Total Control 1000 chassis. Next, check and make sure the DS-3 cable from the DS-3 receive port located on the SDH STM-0 Converter NIC is properly connected to the DS-3 transmit port located on the DS-3 Ingress NIC. Refer to the *Getting Started Guide* for detailed cabling instructions.
Alarm LED on the SDH STM-0 Converter NAC is red; Monitor Port LED on the DS-3 Ingress NAC displays the letter "A" (short for **AIS**)	■ STM-0 transmit and receive optical fiber cables are not cabled correctly ■ STM-0 optical fiber cables are damaged	First of all, make sure the STM-0 transmit and receive optical fiber cables are cabled correctly from the SDH phone switch to the SDH STM-0 Converter NAC. Refer to the *Getting Started Guide* for detailed cabling instructions.
Alarm LED on the SDH STM-0 Converter NAC is amber; Monitor Port LED on the DS-3 Ingress NAC displays the letter "A" (stands for **AIS**)	■ STM-0 transmit optical fiber cable is not cabled correctly ■ STM-0 optical fiber cables are damaged	First of all, make sure the STM-0 transmit optical fiber cable from the SDH phone switch is correctly cabled to the SDH STM-0 Converter NAC. Refer to the *Getting Started Guide* for detailed cabling instructions.

Table 33 SDH System Problems (continued)

Trouble Locating	Possible Cause	Trouble Clearing
Alarm LED on both SDH STM-0 Converter NACs is amber	■ STM-0 optical fiber cables are disconnected, or damaged ■ APS cable is disconnected, or damaged	Check the APS cable. Make sure it is healthy and securely connected. Make sure the transmit and receive STM-1 optical fiber cables from Side 0 on the SDH phone switch are securely connected to the STM-0 transmit and receive ports on the SDH STM-0 Converter NAC located in slot 11. Also, make sure the transmit and receive STM-0 optical fiber cables from Side 0 on the SDH phone switch are securely connected to the STM-0 transmit and receive ports on the SDH STM-0 Converter NAC located in slot 12. Refer to the *Getting Started Guide* for detailed cabling instructions.

Table 33 SDH System Problems (continued)

Trouble Locating	Possible Cause	Trouble Clearing
Network connectivity problems	■ SS7 signaling is not properly configured on the access router card ■ SS7 signaling is not properly configured on the DSP multispan	Refer to the *Getting Started Guide* for detailed configuration information.
The NAC RN/FL LEDs on all of the DSP multispan NACs are amber	■ Serious problems with network management	Check the health of the network management card. Make sure the correct software is installed on the card.

Table 33 SDH System Problems (continued)

Trouble Locating	Possible Cause	Trouble Clearing
No APS Automatic Switch	■ DS-3 Ingress or SDH STM-0 Converter card is rebooting ■ APS cable is missing ■ APS cable is not hooked up properly ■ APS cable is broken ■ DS-3 cables are missing ■ DS-3 cables are not hooked up properly ■ DS-3 cables are broken ■ Standby SDH STM-0 Converter card is in alarm ■ Standby SDH STM-0 Converter card is in Out of Service mode ■ Standby DS-3 Ingress card is in Out of Service mode ■ User has manually configured the system to not allow an APS switch (via Total Control Manager or the CLI) ■ STM-0 optical line errors ■ One or both of the DS-3 Ingress cards are not properly configured for SDH ingress calls ■ STM-0 optical fiber cables from the SDH switch (Side 0 and Side 1) are not properly connected to the respective SDH STM-0 Converter NACs ■ Network management card is not working properly ■ DS-3 card is not working properly	■ After making sure the SDH STM-0 Converter NAC successfully boots up, check the APS and DS-3 cables first. ■ Second, check the operation mode of the SDH STM-0 Converter card and their partner DS-3 Ingress cards. The Active SDH STM-0 Converter module should be set as "Active" and the Standby SDH STM-0 Converter module should be set as "Standby." ■ Next, make sure that the DS-3 Ingress card is set up for SDH calls. ■ The SDH STM-0 Converter may have an APS switch lock turned on (by a user). ■ If you are still having problems, make sure the transmit and receive STM-1 optical fiber cables from Side 0 on the SDH phone switch are securely connected to the STM-0 transmit and receive ports on the SDH STM-0 Converter NAC located in slot 11. Also, make sure the transmit and receive STM-0 optical fiber cables from Side 0 on the SDH phone switch are securely connected to the STM-0 transmit and receive ports on the SDH STM-0 Converter NAC located in slot 12. Refer to the *Getting Started Guide* for detailed cabling instructions. ■ Make sure all of the cards are functioning properly.

Manually Performing an APS Switch

In a maintenance or testing situation, you can manually perform an APS switch from the active SDH STM-0 Converter module to the standby module. You can do this using either common element manager, total control manager, or the Command Line Interface.

Common Element Manager

To perform a manual APS switch using common element manager, use the following procedure:

Releasing Both SDH STM-0 NACs

You must release both SDH STM-0 Converter NACs before performing routine maintenance functions on the cards.

1. From the **Explorer** tab, double-click the active SDH STM-0 Converter card.

   SDH STM-0 Converter card interfaces appear.
2. Click the **SDH Interface**.
3. From the **Properties** tab, click the **General** tab.
4. Double-click the **ServiceCmdForce** field, and click **fsSwitchRelease** from the drop-down list.
5. Click **Save all**.
6. From the **Explorer** tab, double-click the standby SDH STM-0 Converter card.

   SDH STM-0 Converter card interfaces appear.
7. Click the **SDH Interface**.
8. From the **Properties** tab, click the **General** tab.
9. Double-click the **ServiceCmdForce** field, and click **fsSwitchRelease** from the drop-down list.
10. Click **Save all**.

Switching the Active Card to Standby

After releasing both SDH STM-0 Converter cards from service, you must switch the active card from active to standby.

1. From the **Explorer** tab, double-click the active SDH STM-0 Converter card.

   SDH STM-0 Converter card interfaces appear.
2. Click the **SDH Interface**.
3. From the **Properties** tab, click the **General** tab.
4. Double-click the **ServiceCmdForce** field, and click **cnvSby** from the drop-down list.
5. Click **Save all**. The active SDH STM-0 Converter NAC is now the standby card. You have performed an APS switch.

Total Control Manager

To perform a manual APS switch using total control manager, use the following procedure:

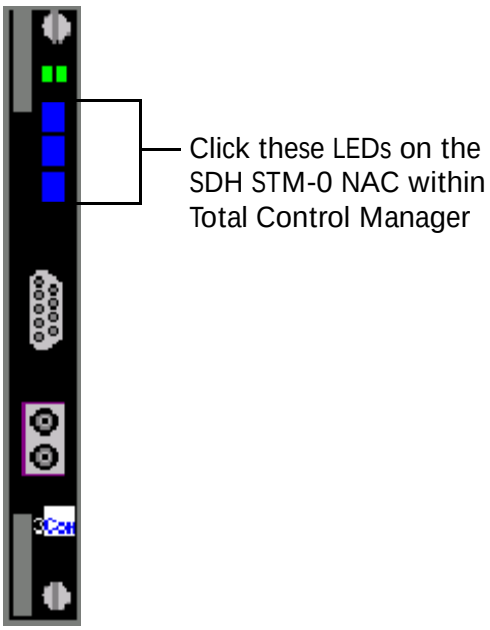
Releasing Both SDH STM-0 NACs

You must release both SDH STM-0 Converter NACs before performing routine maintenance functions on the cards.

1 From the Total Control Manager Virtual Front Panel Display (VFPD), click the LEDs of the active SDH STM-0 Converter NAC.

The LEDs turn blue. See Figure 36 for more information.

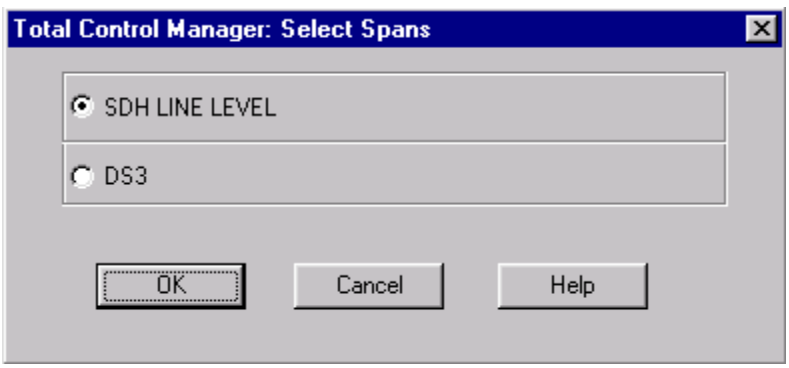
Figure 36 Total Control Manager's Virtual Front Panel Display (VFPD)



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

The Select Spans window displays.

Figure 37 Selecting Spans



3 Select **SDH LINE LEVEL** and click **OK**.

The SDH card Programmed Settings window displays.

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

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

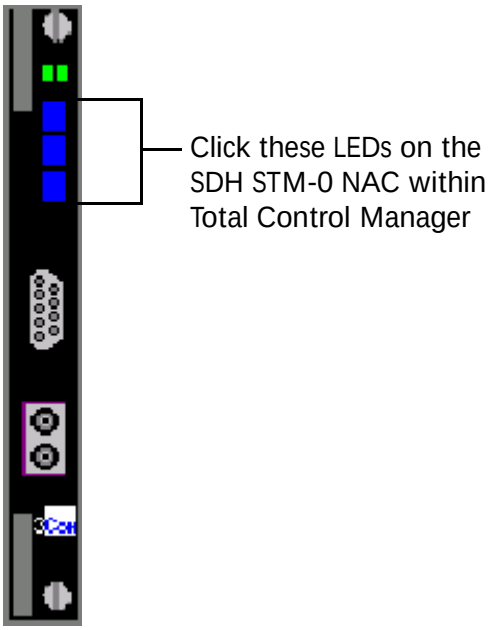
5 From the **Service Cmd Force** field, select **fsSwitchRelease**.

6 Click **Set** and click **OK**.

7 From the Total Control Manager VFPD, click the LEDs of the standby SDH STM-0 Converter NAC.

The LEDs turn blue. See Figure 38 for more information.

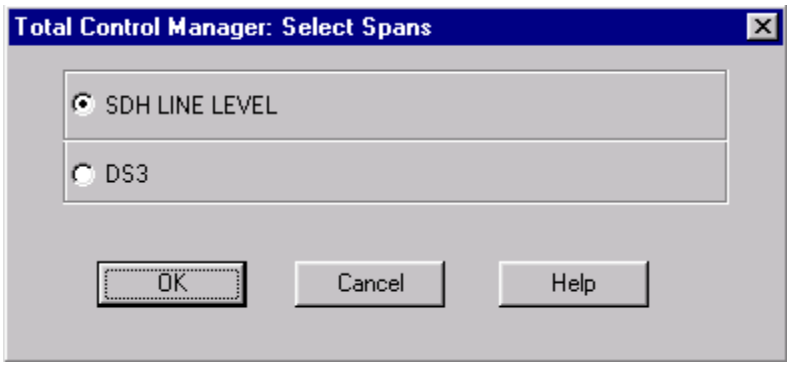
Figure 38 Total Control Manager's Virtual Front Panel Display (VFPD)



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

The Select Spans window displays.

Figure 39 Selecting Spans



9 Select **SDH LINE LEVEL** and click **OK**.

The SDH card Programmed Settings window displays.

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

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

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

12 Click **Set** and click **OK**.

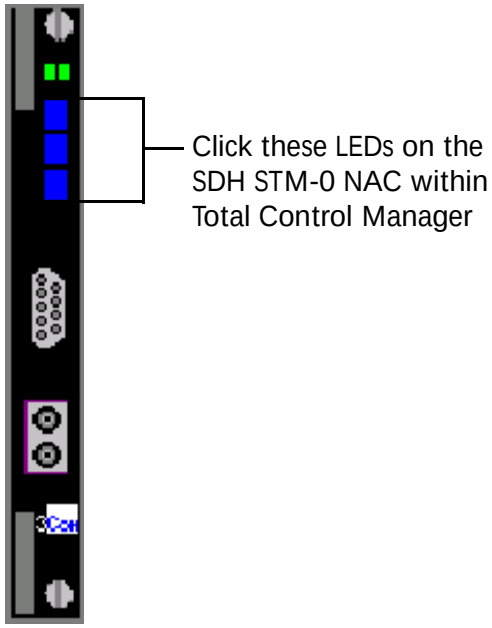
Switching the Active Card to Standby

After releasing both SDH STM-0 Converter cards from service, you must switch the active card from active to standby.

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

The LEDs turn blue. See Figure 40 for more information.

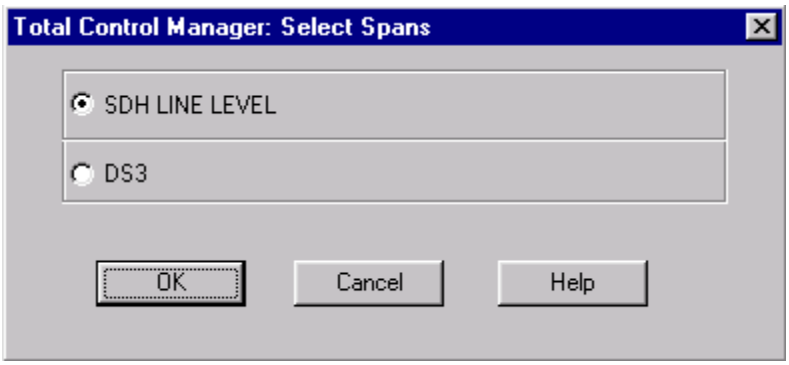
Figure 40 Total Control Manager's Virtual Front Panel Display (VFPD)



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

The Select Spans window displays.

Figure 41 Selecting Spans



3 Select **SDH LINE LEVEL** and click **OK**.

The SDH card Programmed Settings window displays.

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

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

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

6 Click **Set**. The active SDH STM-0 Converter NAC is now the standby card. You have performed an APS switch.

Command Line Interface

To perform a manual APS switch using the CLI, use the following procedure:

Before manually performing an APS switch via the CLI, you must establish a network connection with both SDH STM-0 Converter modules. Please refer to Appendix B for detailed instructions on configuring a local network connection.

Releasing Both SDH STM-0 NACs

You must release both SDH STM-0 Converter NACs before performing routine maintenance functions on the cards.

1. Establish a local network connection with the active SDH STM-0 Converter 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 parameter:

   `set sorder release`

4. Establish a local network connection with the standby SDH STM-0 Converter NAC.
5. Enter the following command from a supported software application (e.g., HyperTerminal):

   `chdev sdh`

   The sdh command prompt appears:

   `sdh>`

6. Enter the following parameter:

   `set sorder release`

Switching the Active Card to Standby

After releasing both SDH STM-0 Converter cards from service, you must switch the active card from active to standby.

1. Establish a local network connection with the active SDH STM-0 Converter 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 parameter:

```
set sorder switch
```

The active SDH STM-0 Converter NAC is now the standby card. You have performed a manual APS switch.

Viewing Manual APS Switch Results

Check the ACT/SBY LED on the front of the SDH STM-0 Converter NACs to make sure the manual APS switch occurred. The ACT/SBY LED on the active module should be solid green; the LED on the standby module should be solid amber.

Using DS-3 and SDH Loopbacks to Diagnose Problems

SDH STM-0 Converter hardware supports several means of loopback. A loopback is a diagnostic test in which a sending device transmits a signal across a medium (e.g., DS-3 span) and waits for its return. Loopbacks check the health of the ingress lines coming into the chassis.

Monitoring DS-3 Loopbacks

The SDH STM-0 Converter NIC has the capability of performing two types of loopbacks on the DS-3 span side. The two supported loopbacks are described in Table 34:

Table 34 DS-3 Loopbacks on the SDH STM-0

Loopback	Description
DS-3 Line Loopback	Monitor a line loopback at the DS-3 Line Interface Unit (LIU)/DS-3 physical span interconnection. This provides a minimal amount of testing to the DS-3 Ingress circuit. DS-3 loopback signal towards the DS-3 line after it has passed through the DS-3 LIU. This is done in response to user (network management or console) commands.
DS-3 Payload Loopback	Monitor a payload loopback at the DS-3 Multiplexer/DS-3 LIU interconnection. This verifies functionality of the DS-3 LIU and part of the M13 multiplexer. This consists of a command to loopback all 28 DS-1 signals towards the DS-3 line without the DS-3 signal being in loopback. The DS-3 overhead data is not looped back. When the command to clear this loopback is executed, all 28 DS-1 loopbacks are cleared regardless of any previous loopback state on any DS-1 span. The loopback is done in response to user (network management or console) commands.

Monitor these loopbacks by using external DS-3 equipment such as a:

- DS-3 Bit Error Rate Testing (BERT) analyzer
- DS-3 network equipment with built-in BERT testing

Configuring DS-3 Loopbacks

You can set DS-3 loopbacks using either common element manager, total control manager, or the Command Line Interface.

Common Element Manager

To set DS-3 loopbacks using common element manager:

1. From the **Explorer** tab, double-click the active SDH STM-0 Converter card.

   SDH STM-0 Converter card interfaces appear.

2. Click the **DS-3 span**.
3. From the **Properties** tab, click the **Configuration** tab.
4. Double-click the **LoopbackConfig** field, and select the desired loopback from the drop-down list. See Table 35 for more information regarding DS-3 loopbacks.
5. Click **Save all**.

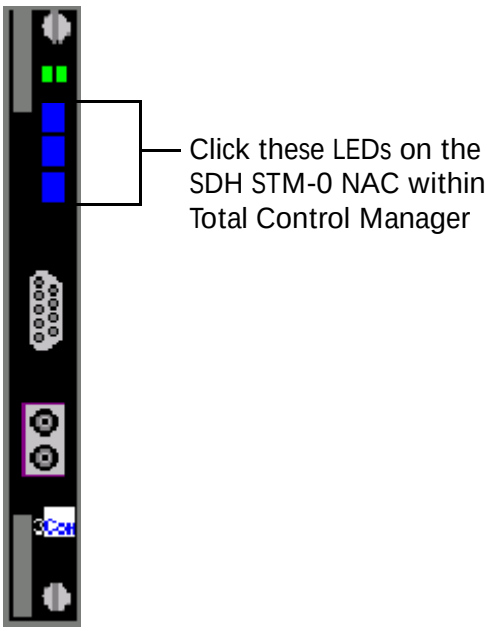
Total Control Manager

To set DS-3 loopbacks using total control manager:

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

   The LEDs turn blue. See Figure 42 for more information.

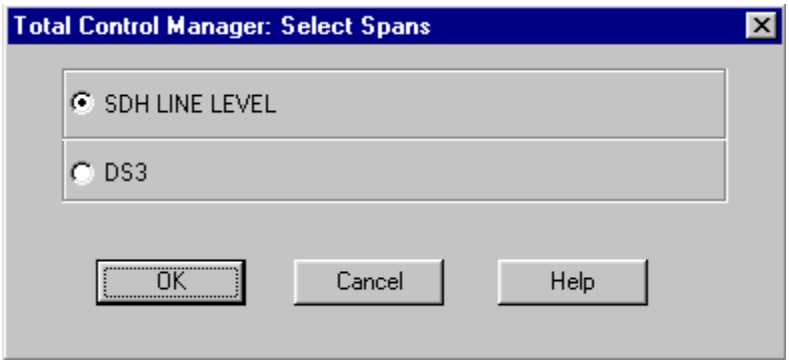
   Figure 42 Total Control Manager's Virtual Front Panel Display (VFPD)



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

The Select Spans window displays.

Figure 43 Selecting Spans



3 Select **DS3**.

4 Click **OK**.

The DS-3 Line Level Programmed Settings window displays.

5 From the Parameter Group drop-down menu, click **DSx3 Configuration**.

The current general programmed settings for the DS-3 Line Level appear.

6 From the **dsx3 Loopback Config** field, select the loopback of choice.

See Table 35 for DS-3 loopback descriptions.

Table 35 DS-3 Loopbacks - MIB Objects

Loopback	Description
dsx3NoLoop	This is the default setting. This is used during normal STM-0 service.
dsx3PayloadLoop	Select a DS-3 Payload Loopback.
dsx3LineLoop	Select a DS-3 Line Loopback.

7 Click **Set** to save the settings in active memory. Settings stored in active memory are lost when a card reboots. The SDH STM-0 Converter module retrieves configurations from Non-volatile Random Access Memory (NVRAM) during reboot.

Command Line Interface

To set DS-3 loopbacks:

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

```
chdev ds3
```

The DS-3 command prompt appears:

```
ds3 1>
```

2 Enter the following command with the associated parameter. See Table 36 for a list of supported parameters:

For example:

```
set d3loconfig payload
```

Table 36 DS-3 Loopbacks - Command Line Interface

Loopback	Description
noloop	Normal operation
payload	Used to determine if the M13 is configured correctly
line	Used to determine if the cabling path for the DS-3 is valid. This loopback does **not** indicate that the DS-3 interface on the SDH STM-0 Converter module is functioning properly.

Monitoring SDH Loopbacks

The SDH STM-0 Converter NIC has the capability of performing three types of loopbacks on the STM-0 span side. The three supported loopbacks are described in Figure 44 and Table 37:

Figure 44 Locating SDH Loopbacks

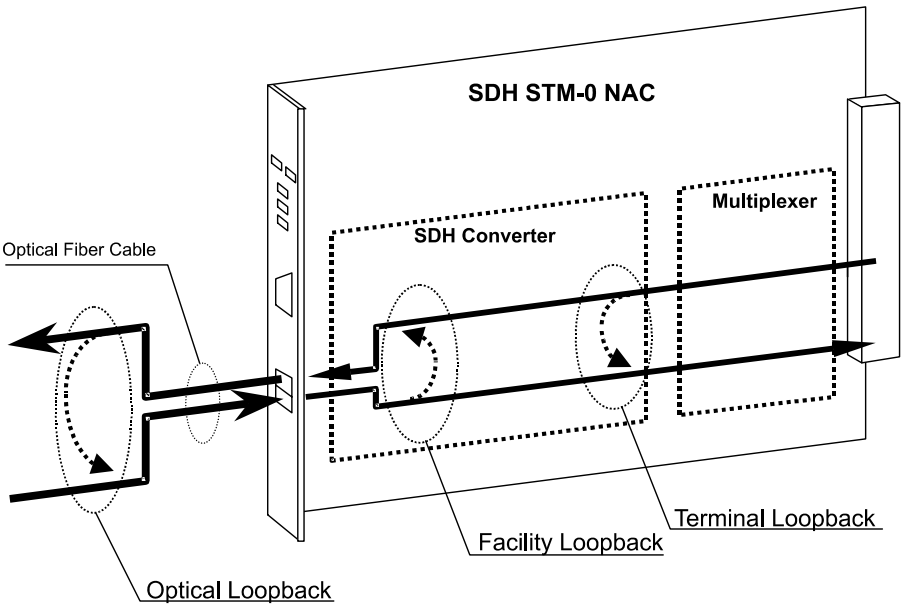


Table 37 describes SDH loopbacks.

Table 37 SDH Loopbacks on the SDH STM-0

Loopback	Description
SDH Facility Line Loopback	The SDH STM-0 Converter sends an electrical loopback signal towards the SDH network after it has passed through the SDH STM-0 Converter. This loopback occurs in response to user (network management or console) commands.
SDH Terminal Local Loopback	The SDH STM-0 Converter sends an electrical loopback signal towards the DS-3 interface (Multiplexer) after it has passed through the SDH STM-0 Converter. This loopback occurs in response to user (network management or console) commands.
SDH Optical Local Loopback	The SDH STM-0 Converter sends a loopback signal towards the DS-3 interface after it has passed through the electrical/optical converter and subsequently loops back using an external fiber optic cable that connects the fiber optic transmitter to the fiber optic receiver. This loopback occurs in response to user (network management or console) commands.

Monitor the SDH Facility Line Loopback by using external SDH STM-0 Converter equipment such as an:

- SDH BERT analyzer
- SDH network equipment with built-in BERT testing

Configuring SDH Loopbacks

You can set SDH loopbacks using either common element manager, total control manager, or the Command Line Interface.

Common Element Manager

To set DS-3 loopbacks using common element manager:

1. From the **Explorer** tab, double-click the active SDH STM-0 Converter card.

   SDH STM-0 Converter card interfaces appear.
2. Click the **SDH Interface**.
3. From the **Properties** tab, click the **General** tab.
4. Double-click the **MediumLoopbackConfig** field, and select the desired loopback from the drop-down list. See Table 38 for more information regarding SDH loopbacks.
5. Click **Save all**.

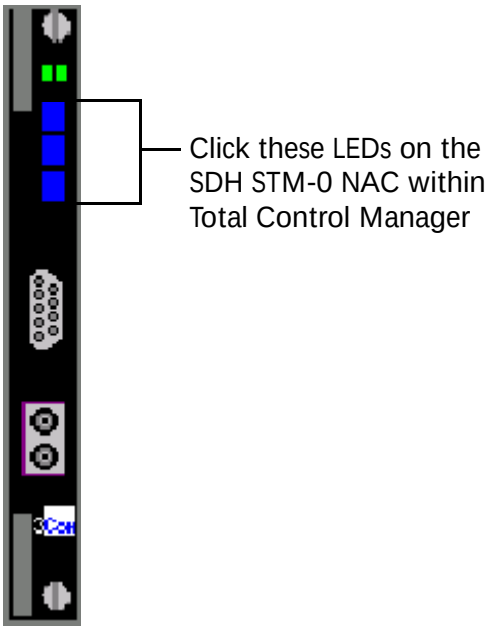
Total Control Manager

To set SDH Line loopbacks using Total Control Manager:

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

   The LEDs turn blue. See Figure 45 for more information.

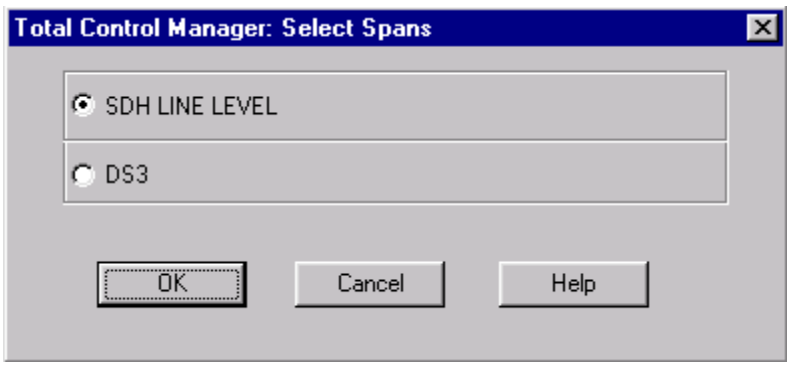
Figure 45 Total Control Manager's Virtual Front Panel Display (VFPD)



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

The Select Spans window displays.

Figure 46 Selecting Spans



3 Select **SDH LINE LEVEL**.

4 Click **OK**.

The SDH Line Level Programmed Settings window displays.

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

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

6 From the **Medium Loopback Config** field, select the loopback of choice.

See the following table for SDH Line loopback descriptions.

Table 38 SDH Line Loopbacks - MIB Objects

Loopback	Description
noLoop	This is the default setting. This is used during normal STM-0 service.
facilityLoop	Selects a Facility Loopback
terminalLoop	Selects a Terminal Loopback.
opticalLoop	Selects an Optical Loopback.

7 Click **Set** to save the settings in active memory. Settings stored in active memory are lost when a card reboots. The SDH STM-0 Converter module retrieves configurations from Non-volatile Random Access Memory (NVRAM) during reboot.

Command Line Interface

To set SDH loopbacks via the CLI:

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

```
chdev sdh
```

The sdh command prompt appears:

```
sdh>
```

2 Enter the following command with the associated parameter. See Table 38 for a list of supported parameters.

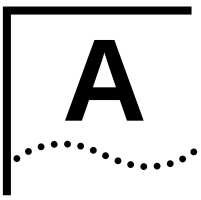
For example:

```
set sloconf facility
```

Table 39 lists SDH loopback options:

Table 39 SDH Loopbacks - Command Line Interface

Loopback	Description
noloop	Normal Operation (default setting)
facility	Used to perform an SDH facility loopback.
Terminal	Used to perform an SDH terminal loopback
Optical	Used to perform an SDH optical loopback



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 10048400