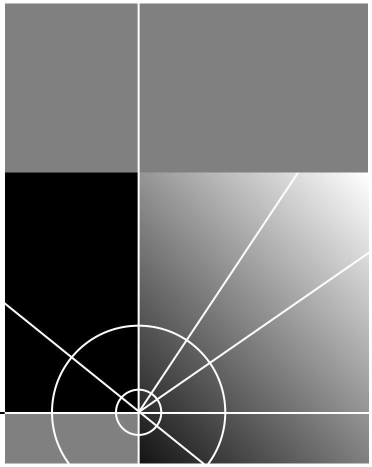
ISP Network Management Guide

Part No. 1.024.1987-00

Version 1.0

ISP Network Management Guide



http://www.3com.com/

Part No. 1.024.1987-00

3Com Corporation
5400 Bayfront Plaza
Santa Clara, California
95052-8145

Copyright © 1998, 3Com Corporation. All rights reserved. No part of this documentation may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from 3Com Corporation.

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty of any kind, either implied or expressed, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

UNITED STATES GOVERNMENT LEGENDS:

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

United States Government Legend: All technical data and computer software is commercial in nature and developed solely at private expense. Software is delivered as Commercial Computer Software as defined in DFARS 252.227-7014 (June 1995) or as a commercial item as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

[Portions of this documentation are reproduced in whole or in part with permission from (as appropriate).]

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. UNIX is a registered trademark of X/Open Company, Ltd. in the United States and other countries.

Other brand and product names may be registered trademarks or trademarks of their respective holders.

YEAR 2000 INFORMATION:

For information on Year 2000 compliance and 3Com products, visit the 3Com Year 2000 web page:

http://www.3Com.com/products/yr2000.html

CONTENTS

ABOUT THIS GUIDE

ISP NETWORK MANAGEMENT GUIDE

APPENDIX

INDEX

About This Guide

About This Guide provides an overview of this guide, describes guide conventions, tells you where to look for specific information and lists other publications that may be useful.

This guide describes network management techniques for Internet service providers (ISPs).

Conventions

These tables list conventions used throughout this guide.

Icon	Notice Type	Description
ℹ	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.

Convention	Description
`Commands`	The word "command" means you must enter the command exactly as shown in text and press the Return or Enter key. Example: To remove the IP address, enter the following command: **`SETDefault !0 -IP NETaddr = 0.0.0.0`** *This guide always gives the full form of a command in uppercase and lowercase letters. However, you can abbreviate commands by entering only the uppercase letters and the appropriate value. Commands are not case-sensitive.*

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”

Related Documentation

The Total Control Hub Documentation Library is an excellent source of detailed information about the chassis. The library is available on CD-ROM and on our web site.

- Total Control Enterprise Network Hub Documentation Library, System Release 3.1, part number 1.035.0008-02.
- Web site: **http://totalservice.3com.com**

Contacting 3Com

Call the appropriate toll free number listed below for technical support.

For European countries that do not have a toll free number listed, call +31 30 602 9900.

Country	Toll Free Number	Country	Toll Free Number
Austria	06 607468	**Netherlands**	0800 0227788
Belgium	0800 71429	**Norway**	800 11376
Canada	1800 2318770	**Poland**	00800 3111206
Denmark	800 17309	**Portugal**	0800 831416
Finland	0800 113153	**South Africa**	0800 995014
France	0800 917959	**Spain**	900 983125
Germany	0800 1821502	**Sweden**	020 795482
Hungary	00800 12813	**Switzerland**	0800 553072
Ireland	1800 553117	**UK**	0800 966197
Israel	0800 9453794	**United States**	1800 2318770
Italy	1678 79489	***All Other Locations*** ***(Outside Europe)***	1847 7976600

Refer to the Total Control Hub Documentation CD-ROM for more information regarding product warranty.

For information about Customer Service, including support, training, contracts, and documentation, visit our website at ***http://totalservice.3com.com***

ISP Network Management Guide

This guide introduces and explains the monitoring and troubleshooting tools that are associated with the Total Control multiservice access platform. In addition, it provides general advice regarding documenting chassis and network configuration to ease troubleshooting.

Important General Advice

To increase the uptime of your network, strive to make progress in these three areas: anticipating problems by monitoring proactively, keeping current configuration records, and providing technicians with the proper tools and training.

Become Proactive

Many ISPs find themselves caught in a reactive mode when it comes to problem resolution. Network issues are addressed only when customers complain about them.

Ideally, you will anticipate network problems and head them off before customers complain. The best way to do that is by adopting proactive, passive monitoring methods. A substantial portion of this guide explains how to do that.

Keep Current Records

As you isolate problems, it is essential that you have recent records of known-good equipment configurations. That way, you have valid configuration data against which to compare problematic ones.

It is best to perform inventories every couple of months and to save the results in an easily accessible location, preferably online. The Inventory function in Total Control Manager is ideal for gathering configuration data.

Additionally, you can use an accounting server to collect performance and network status data that will be useful when you isolate problems. This guide also explains how to do that.

Provide Technicians with the Right Tools and Training

All network technicians should have available to them a management information base (MIB) browser and an alarm server.

MIB browsers allow technicians to retrieve information and manipulate settings from network equipment using the simple network management protocol (SNMP), which is carried over the Internet protocol (IP).

Alarm servers, when connected to IP networks, notify users when SNMP "traps," or alarms, are received from network equipment. The equipment must be preconfigured to issue traps when threshold values of certain key measures are reached.

All network technicians should have a firm grounding in the workings of the IP stack and in managing network equipment using SNMP.

Tools Overview

The Total Control multiservice access platform provides many tools for assessing its status and for troubleshooting.

Total Control Manager

Total Control Manager is a stand-alone SNMP-based management application that is dedicated to Total Control hubs. Total Control Manager provides a number of tools that can be used to monitor, configure, and troubleshoot.

Virtual Front Panel Display

Total Control Manager provides a view of the Total Control chassis front panel, which allows you to view its LEDs remotely.

Performance Monitor / Session Monitor

Performance Monitor (called Session Monitor in Total Control Manager for Windows) is the key tool for gathering performance data from the Total Control hub during operation.

Inventory

The Inventory function gathers information from the chassis and installed cards, including hardware and software version numbers, amount of memory, and DIP switch settings. The results of the inventory can be saved as a text file.

Trap (Alarm) and Accounting Configuration

Use Total Control Manager to set up the chassis to send alarms and accounting data automatically to an alarm server or an accounting server, respectively. Doing so is vital to a proactive approach to chassis management.

HiPer DSP Console

Access the HiPer DSP console interface by connecting a computer (running terminal emulation software) to the Console port in its T1/E1 Network Interface Card (NIC).

Span Statistics

The *display spnstats debug* command provides detailed information about the T1 or PRI span status, including any alarms on the span, counts of various error conditions, number of calls received versus accepted, switch type, and D-channel status.

Timeslot and Protocol Status

The commands *display atstat* and *display atproto* give the status of each timeslot (DS0) of the span and the protocol each modem is using to communicate with remote modems.

Line Errors

The *display near current* and *display near total* commands show counts of errors received on the T1 or PRI span in the last 15 minutes and 24 hours, respectively.

Disconnect and Call Failure Reasons

Using the *AT-ADn* and *AT-AFn* commands, you can view the past *n* call disconnect and call failure reasons, respectively.

Protocol Tracing

You can trace aspects of the HiPer DSP's functioning in minute detail using the trace debug (*trc dbg*) command.

HiPer ARC Console

Access the HiPer ARC's console interface either locally, from a computer (running terminal emulation software) connected to its Ethernet NIC console port, or remotely by telnetting to the HiPer ARC IP address.

PPP Monitor

Point-to-Point Protocol (PPP) Monitor is useful for examining the PPP negotiation process from the HiPer ARC's point of view.

RADIUS Monitor

Remote Authentication Dial-In User Service (RADIUS) Monitor is useful for examining the RADIUS authentication or accounting process from the HiPer ARC's point of view.

SYSLOG

SYSLOG allows you to track every event that occurs at the HiPer ARC, in exhaustive detail if necessary. Events can be logged to a SYSLOG server or displayed to the console or telnet session.

NETServer Console

The NETServer provides useful tools for problem solving. Access its console interface locally, from a computer (running terminal emulation software) connected to its Ethernet NIC console port, or remotely by telnetting to the NETServer IP address.

Packet Bus / Modem Status

The fundamental NETServer command, *show all*, gives the status of the modems and their connections to the packet bus.

Debug

The *set debug* command causes protocol details to display on screen for further analysis.

Security / Accounting Server

3Com's Total Control Security and Accounting Server performs RADIUS authentication and accounting services. Its configuration files are vital for troubleshooting.

Log File

The **security.log** file is helpful for troubleshooting.

Windows Client

The Windows version of the Security and Accounting Server ships with **client.exe**, a program that simulates a RADIUS client (such as HiPer ARC or NETServer) and is very useful for testing.

Other Tools

These third-party, freeware, and unsupported-3Com tools aid troubleshooting.

Snoop / Tcpdump

Snoop and Tcpdump are IP analyzers for UNIX; Snoop runs on Sun systems and Tcpdump is a freeware program with versions for most any UNIX variant.

NETMON (Event Viewer)

NETMON is a protocol analyzer that ships with Windows NT, but is not installed by default. The version included with Microsoft Systems Manager Server (SMS) captures any packets it detects, but the standard Windows NT version captures only packets sent from or received by the computer on which it is running.

Windows PPP and Modem Logs

Windows 95/98 clients are capable of generating logs of PPP negotiation (through Dial-Up Adapter) and modem activity (through Dial-Up Networking).

Unsupported 3Com Protocol Decoders

These applications were written by 3Com technical support personnel and are not officially supported by 3Com. Among them is RADDEBUG, for decoding RADIUS packets.

Techniques Overview

The remainder of this document explains:

Documenting the system A key to easing troubleshooting is ready access to known-good configuration data. This section explains how to gather it using Total Control Manager.

Passive monitoring This section explains how to set up the Total Control hub (using Total Control Manager) to provide automatic notification of specified events and to send accounting data automatically to a logging server.

Active monitoring Active monitoring is the process of examining the system when there is not necessarily any indication of trouble.

Investigating problems In this case, there is a symptom of trouble, such as user reports of connection problems or network slowness. This section offers techniques for finding the cause.

Correcting problems Problems described in this section have a clear symptom and a straightforward fix.

x2 troubleshooting Provides a reference to another document on this subject.

Documenting the System

Document chassis configurations at least quarterly, and preferably every two months.

Inventory

A simple way to document the physical configuration is to use the Inventory function in Total Control Manager. Inventory gathers:

- Network Application Card (NAC) and NIC names and serial numbers
- Software revisions
- Amount of memory
- DIP switch settings

Inventory does not record software settings.

Inventorying a Chassis

1. Start Total Control Manager.
2. If you have managed the chassis before from this workstation, from the **File** menu, click **Open**, choose the desired chassis from the list, and then click **OK**.

   If you have not managed the chassis before from this workstation, from the **File** menu, click **New**, enter a name for the chassis, the IP address you assigned to the Network Management Card (NMC), plus SNMP community strings (passwords) if you entered them. Then click **OK**.
3. When the chassis appears, from the **Configure** menu, click **Inventory**.
4. Select the chassis from the list, then click **OK**. The inventory appears.

5 Click **Save** to save the inventory to a text file. The output looks like this:

```
   U.S. Robotics 17-Slot Chassis with PB clocking
   MyLabChassis <x.x.250.125>

1  3COM PRI-T1/E1 NACBCG53F2I2.0.0 40961024 00000000000001003.0.2
2  3COM Qd V.34 D-A Mdm NACB1G656B10P70002.0.0    0 000000001100010005.9.9
3  3COM Qd V.34 D-A Mdm NACB1G656BN0P70002.0.0    0 000000001100010005.9.9
4  3COM Qd V.34 D-A Mdm NACB8R68JEZ10T0002.0.0    0 000000001100010005.10.9
5  3COM Qd V.34 D-A Mdm NACB8R68JFG10T0002.0.0    0 000000001100010005.10.9
6  3COM Qd V.34 D-A Mdm NACB8R68JEB10T0002.0.0    0 000000001100010005.10.9
7  3COM H-D 24 Ch NAC56789ABC0.49.0 8192204800000000000000001.2.5
16 3COM ISDN NETServer NACBA27TPFX17C0007.0.0163844096 00000000000000000.8.1
17 3COM NMC with clockBBO78OIP1U60006.016384819200000000000000005.5.5
1  3COM LongHaul Dl T1 NIC 409610240000000000000100
2  3COM Qd Mdm Anlg NIC v1    0 000000001100010001.1.0
7  3COM T1/E1 HDM NIC 819220480000000000000000
16 3COM HS Enet (V.35) NIC1638440960000000000000000
17 3COM Ethernet NIC??????????    0   00000000000000000
```

Configuration Capture

This manual method captures all the software settings for all the cards except the gateways (HiPer ARC or NETServer). It involves stepping through all the configurable parameters for each card in Total Control Manager, copying them, and pasting them into a spreadsheet.

To capture the configuration of all cards except gateways

1 Start Total Control Manager.

2 If you have managed the chassis before from this workstation, from the **File** menu, click **Open**, choose the desired chassis from the list, and then click **OK**.

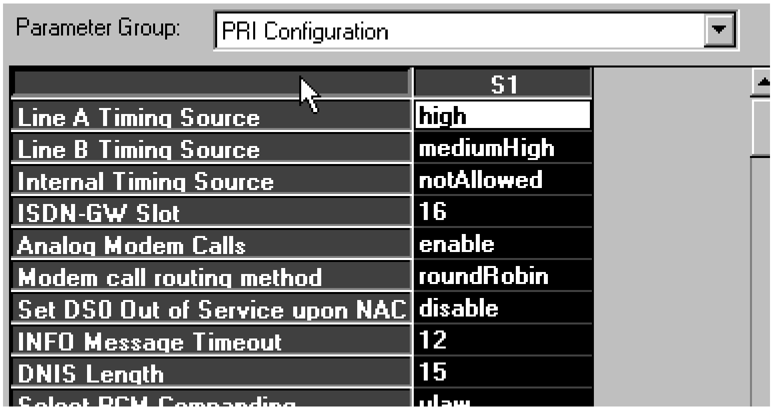
If you have not managed the chassis before from this workstation, from the **File** menu, click **New**, enter a name for the chassis, the IP address you assigned to the Network Management Card (NMC), plus SNMP community strings (passwords) if you entered them. Then click **OK**.

3 When the chassis appears, click the leftmost card (for example, the Dual PRI NAC).

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

5 Select the first menu item that contains user-configurable parameters (for example, PRI Configuration).

6 Click the upper-left cell of the table.



Parameter Group: PRI Configuration

	S1
Line A Timing Source	high
Line B Timing Source	mediumHigh
Internal Timing Source	notAllowed
ISDN-GW Slot	16
Analog Modem Calls	enable
Modem call routing method	roundRobin
Set DS0 Out of Service upon NAC	disable
INFO Message Timeout	12
DNIS Length	15
Select PCM Companding	ulaw

7 Press [Ctrl] + [c] to copy the table to the clipboard.

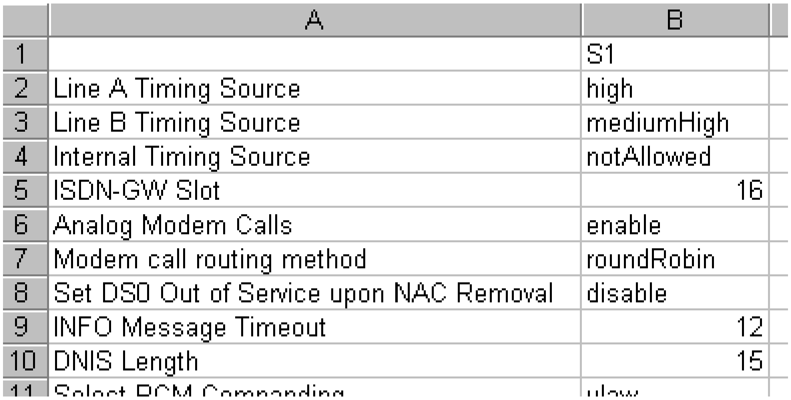
8 Start a spreadsheet program, such as Microsoft Excel, and create a new spreadsheet.

9 Name the first page of the spreadsheet (for example, Dual PRI).

10 Select the first cell on the page, then press [Ctrl] + [v] to paste the cells into the spreadsheet.

11 Adjust the cell widths to fit the text.

The result is an exact copy of the Parameter Group.



	A	B
1		S1
2	Line A Timing Source	high
3	Line B Timing Source	mediumHigh
4	Internal Timing Source	notAllowed
5	ISDN-GW Slot	16
6	Analog Modem Calls	enable
7	Modem call routing method	roundRobin
8	Set DS0 Out of Service upon NAC Removal	disable
9	INFO Message Timeout	12
10	DNIS Length	15
11	Select PCM Companding	ulaw

12 Repeat steps 4–11 until you have captured all user-configurable parameters for the first card.

13 [Optional.] From the Fault menu, select Trap Settings and then repeat steps 5–12.

14 [Optional.] From the Fault menu, select Trap Destinations and then repeat steps 5–12.

15 Start a new page in the spreadsheet and name it (for example, Quad Modem).

16 Repeat steps 4–15 until you have captured all user-configurable parameters for all the cards (except the gateway cards).

To capture a NETServer configuration

1 From a NETServer command prompt, enter

```
show net0
```

2 Enter

```
show global
```

3 Enter

```
show all
```

4 Select the results of these commands, copy them, and save them.

To capture a HiPer ARC configuration

1 From a HiPer ARC command prompt, enter

```
show config
```

2 Select the result of this command, copy it, and save it.

Passive Monitoring

Use Total Control Manager to set up automatic notification of problems and automatic logging of accounting data.

To provide automatic notification of problems, the Network Management Card (NMC) issues SNMP traps. To log accounting data automatically, the NMC sends RADIUS accounting messages. In each case, you must configure a device to receive the messages.

Traps

Alarm notification requires two components: a device (the Total Control chassis) to issue traps and a device to receive them and alert the network manager (an alarm server). The protocol behind this is the Simple Network Management Protocol (SNMP), which runs on the User Datagram Protocol / Internet Protocol (UDP/IP).

To tell the NMC where to send traps

1. Select the **NMC**.
2. From the **Fault** menu, click **Trap Destinations.**
3. Click **Add.**
4. Type the IP address of the alarm server and its community string (password).
5. Click **OK**, then click **Exit**.

To enable the NMC to send traps

Several important chassis-level events send traps by default, such as card insertion and removal, power supply failure, and high temperature.

1. Select the **NMC**.
2. From the **Fault** menu, click **Trap Settings.**
3. From Parameter Group, select **Chassis Trap Enables**.

   Change all the events in this list from enableTrap to enableAll. This requests that, in addition to a trap, the event is logged in the accounting server. See the next section for more information.

Enable traps from specific cards for infrequent, high-impact events such as DS1 red alarms, loss of signal, loss of D-channel. For example, to enable such traps in the HiPer DSP:

1. Select the span LEDs on the HiPer DSP.
2. From the **Fault** menu, click **Trap Settings.**

3 From Parameter Group, select **Trap Enables**.

Enable traps and log (see next section) for several of these events, including On Red Alarm and On Loss of Signal.

If this is a PRI line, from Parameter Group, select **D-Channel Service Traps** and enable **On D-Channel Out of Service**.

Traps can also aid troubleshooting. When warranted, enable traps to help isolate problems.

Accounting

When you enable accounting, events that you specify are logged quietly to an accounting server. You can retrieve and examine the records whenever you choose.

As with alarms, two components are required: a device (the Total Control hub) to issue the accounting messages and a device to receive and log them (an accounting server). The protocol behind this is Remote Authentication Dial-In User Service (RADIUS), which runs on UDP/IP.

For the most effective records, generate an accounting record every time a call fails.

Before continuing, make sure you have the Accounting Server installed.

To tell the NMC where to send accounting messages

1 Select the **NMC**.

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

3 From Parameter Group, select **Logging Group**.

4 At Primary Log Server IP Address, type the IP address of the accounting server**.** Add backup server IP addresses as necessary. Click **Set**, then click **OK**.

Enable these accounting messages for HiPer DSP

1 Click the body of the HiPer DSP card.

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

3 Click **ALL** (use ALL templates), then click **OK**.

4 From Parameter Group, select **Trap Enables**.

5 Select **enableLog** for:

- On Incoming Call
- On Incoming Termination
- Incoming Connection Attempt Failure

6 Click **OK**.

7 Click the span LEDs of the HiPer DSP.

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

9 From Parameter Group, select **Trap Enables**.

10 Select **enableAll** for all events.

*Select **enableAll** only if there is a trap server to which to send the traps. If not, select **enableLog**.*

Enable these accounting messages for Dual T1/PRI

1 Click the body of the Dual T1/PRI card.

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

3 From Parameter Group, select **Trap Enables**.

4 Select **enableLog** for:

- On Call Arrive
- On Call Connect
- On Call Termination
- On Call Failure

5 Click **OK**.

6 Click the top LED of the Dual T1/PRI card.

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

8 From Parameter Group, select **Trap Enables**.

9 Select **enableAll** for all events.

*Select **enableAll** only if there is a trap server to which to send the traps. If not, select **enableLog**.*

Enable these accounting messages for Quad Modems

1 Select the top LED of the Quad Modem card.

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

3 From Parameter Group, select **Trap Enables**.

4 Select **enableLog** for:

- On Incoming Call
- On Incoming Termination
- On Connection Failure

To set logging groups for the NMC

Logging groups are filters for the data the NMC sends to an accounting server when an event occurs. The logging group settings for the NMC affect all cards in the chassis except HiPer DSP.

When an event occurs that generates a trap or an accounting record, the card sends all the data over the management bus to the NMC, but the NMC filters it and sends what you specify according to logging group. The groups are explained fully in the NMC Parameter Reference manual.

Table 1 Descriptions of logging groups

Group number	Description
1	Usage statistics [always sent]
2	Data transfer statistics
3	Performance statistics
4	Operating mode statistics
5	Remote Modem Management Information Exchange (RMMIE)

1 Click the NMC.

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

3 From Parameter Group, select **Logging Group**.

4 For Log Group Selection, select **group2345** (ALL).

To set logging groups for the HiPer DSP

The HiPer DSP logging group setting overrides that of the NMC.

1 Click the body of the HiPer DSP.

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

3 Click **Card Level**, then click **OK**.

4 From Parameter Group, select **Call Statistics**.

5 From Group Settings, select a logging group.

Enable these accounting messages for the TC chassis

1 Click the NMC.

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

3 From Parameter Group, select **Chassis Trap Enables**.

4 Change them all to **enableAll**. This produces a record at the accounting server.

Active Monitoring

Monitor actively by using Total Control Manager or card console interfaces to scan the system.

Using Total Control Manager Software

To scan LEDs for faults

When you open a chassis in Total Control Manager, the virtual front panel display (VFPD) appears. The LEDs on the front of the chassis are updated in nearly real-time.

Important LEDs to watch:

Hub Status LED (second one down on NMC)

- Solid RED indicates a critical failure in the chassis.
  - Check the hub status: click the NMC, then from the **Performance** menu, click **Session Monitor**. From Functional Group, select **Failure Reasons**. From Parameters, select **Hub Status Red**. Click **Add**, then click **OK**.
  - Look for bootup failures: click the NMC, then from the **Configure** menu, click **Programmed Settings**. From Parameter Group, click **NMC Tests**.
  - Check chassis temperature: click the NMC, then from the **Configure** menu, click **Programmed Settings**. From Parameter Group, click **NMC Identification**. The Ideal temperature range 24–25° C. Be concerned if the temperature exceeds 40° C.
  - Check for stopped fans (must visit the chassis).
  - Check accounting or trap logs for failures.
  - A card that is resetting can cause this condition.
  - A PSU that has failed or is unplugged can cause this condition.
- Flashing RED indicates management bus failure.

Quad Modem LED If a modem is RED,

- And there's no NETServer in the chassis, as with Citrix WinFrame, the modem is not receiving the Data Terminal Ready (DTR) signal.

  Make sure the RS-232 cables are connected and verify that your communications software is running and configured correctly.

- And there is a NETServer in the chassis, there's a problem with the packet bus or with the NETServer.

If a modem is ORANGE, the modem is training. Wait.

HiPer DSP

To monitor modem events

1. Click the HiPer DSP modem LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Select the channels (modems) to monitor, then click **OK**.
4. From Functional Group, select **Modem Events**.
5. Select:
   - Incoming Connections Established
   - Incoming Connections Failed
   - Connect Attempt Failures

   Then click **Add**, then click **OK**.

In Total Control Manager for UNIX, you can graph these results.

To check for continuous CRC errors

Indicates true/false.

1. Click span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **DS1**, then click **OK**.
4. From Functional Group, select **Call Statistics**.
5. Click **Continuous CRC Errors**. Click **Add**, then click **OK**.

To check PRI D-channel status

Indicates up or down.

1. Click span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **DS1**, then click **OK**.
4. From Functional Group, select **Call Statistics**.
5. Click **D Channel Operation**. Click **Add**, then click **OK**.

To check whether DS0s are in service

1. Select span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **DS0**.
4. Click **Select All** (or select the DS0s you are interested in), then click **OK.**
5. From Functional Group, select **DS0 Statistics**.
6. Select **DS0 Service State.** Click **Add**, then click **OK**.

To check for excessive connect times

1. Select the modem LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **Select All** (or select the DS0s you are interested in), then click **OK**.
4. From Functional Group, select **Call Statistics**.
5. Select **Call Duration**. Click **Add**, then click **OK**.

Using the HiPer DSP Console Interface

Access the HiPer DSP console interface by connecting a cable from a computer's serial port to the Console port in the HiPer DSP T1/E1 NIC. The computer must run terminal emulation software at 9600 bps.

Issue these *display* commands from a *span* command prompt.

display spnstats debug

This command provides detailed information about the span's status.

Key items to examine:

- *Span line status* details any alarm conditions the line is experiencing (this is physical layer).

```
Span1 Line Status is:
   NO ALARM          = TRUE
   RCV FAR END LOF   = FALSE
   XMT FAR END LOF   = FALSE
   RCV AIS           = FALSE
   XMT AIS           = FALSE
   OUT OF FRAME      = FALSE
   LOSS OF SIGNAL    = FALSE
   LOOPBACK STATE    = FALSE
   T16 AIS           = FALSE
   RCV FAR END LOMF  = FALSE
   XMT FAR END LOMF  = FALSE
   RCV TEST CODE     = FALSE
   OTHER FAILURE     = FALSE
```

- *Continuous CRC error*, true or false.

```
Span1 Continuous CRC Error is:             FALSE
```

- *Modem not available count* gives the number of calls that the span could accept, but found no modems to pass to. There is no active packet bus connection between at least one of the modems and a gateway card. Either the configuration is bad, the modem is dead, or there may be a bug.

  At the gateway card, verify that the packet-bus sessions are active. (From the NETServer, send *show all*. From the HiPer ARC, send *list interfaces*.)

  If the packet bus sessions are ok, in Total Control Manager, select all modems and bring up Performance Monitor. Look for one or more modems with an abnormal number of incoming failed connections.

  From the modem channel with many failed connections, send AT-AF*n* to display call failure reasons. That may point to the source of the problem. AT-SR indicates whether a modem has “hung” or may have a hardware problem.

- High *Invalid...* or *Dial in no resp to disc* counts point to problems with the span, probably at the telco. These are errors in the Q.931 frame that you can investigate using tracing (see To examine Q.931 (D-channel) activity on page 37).

```
Span1 Modem Not Available Count is:        0
Span1 Invalid Bearer Capability Count is:  0
Span1 Invalid Channel ID Count is:         0
Span1 Invalid Progress Indicator Count is: 0
Span1 Invalid Calling Party Count is:      0
Span1 Invalid Called Party Count is:       0
...
Span1 Dial In No Resp To Disc Count is:    0
```

- Compare *Calls received* to *Calls accepted*; any difference indicates potential problems.

```
Span1 In Digital Calls Received Count is:  39
Span1 In Digital Calls Accepted Count is:  39
Span1 In Analog Calls Received Count is:   2336
Span1 In Analog Calls Accepted Count is:   2335
```

- *D-channel status*, up or down.

```
Span1 D-channel Operational is:           UP
```

To check the DS0 in-service status

display atstat This command allows you to view the status of the DS0s and each associated modem.

```
span1> di ats

Tslot  Status   Modem    Status        Call ID        Action    Q931
               Connect Srvc State                     Queued    Ref
 01   Conn In   001          IS      0x08ED0002        NONE    0x0000034B
 02      Idle   N/A          IS      0x00000000        NONE    0x00000000
 03      Idle   N/A          IS      0x00000000        NONE    0x00000000
 04   Conn In   004          IS      0x093F0302        NONE    0x0000039D
 05   Conn In   005          IS      0x09050402        NONE    0x00000363
 06   Conn In   006          IS      0x09140502        NONE    0x00000372
 ...
```

To determine which modem protocols are in use

display atproto This command allows you to view protocols in use in each modem connection.

```
span1> di atp

Tslot  Status   Modem   Protocol
               Connect
 01   Conn In    001    V.42/V.42bis/N/A
 02      Idle    N/A    N/A
 03   Conn In    003    V.42/V.42bis/V.34
 04      Idle    N/A    N/A
 05      Idle    N/A    N/A
 06   Conn In    006    V.42/V.42bis/V.34
 ...
```

To display errors that arrived in last 15 min over the T1 or PRI

display near current

This command allows you to view all errors that have arrived over the T1 or PRI line in the past 15 minutes.

```
span1> di near current
   Span1 Near Current Line Index is:                         0
   Span1 Near Current Errored Seconds is:                    0
   Span1 Near Current Severely Errored Seconds is:           0
   Span1 Near Current Severely Errored Framing Seconds is:   0
   Span1 Near Current Unavailable or Failed Seconds is:      0
   Span1 Near Current Controlled Slip Seconds is:            0
   Span1 Near Current Path Coding Violations is:             0
   Span1 Near Current Line Errored Seconds is:               0
   Span1 Near Current Bursty Errored Seconds is:             0
   Span1 Near Current Degraded Minutes is:                   0
   Span1 Near Current Line Code Violations is:               0
   Span1 Near Valid Intervals is:                           96
```

To display errors that arrived in last 24 hours over the T1 or PRI

display near total

This command allows you to view all errors that have arrived over the T1 or PRI line in the past 24 hours.

```
span1> di near total
   Span1 Near Total Line Index is:                         0
   Span1 Near Total Errored Seconds is:                    0
   Span1 Near Total Severely Errored Seconds is:           0
   Span1 Near Total Severely Errored Framing Seconds is:   0
   Span1 Near Total Unavailable or Failed Seconds is:      0
   Span1 Near Total Controlled Slip Seconds is:            0
   Span1 Near Total Path Coding Violations is:             0
   Span1 Near Total Line Errored Seconds is:               0
   Span1 Near Total Bursty Errored Seconds is:             0
   Span1 Near Total Degraded Minutes is:                   0
   Span1 Near Total Line Code Violations is:               0
```

Using HiPer DSP AT Commands

Issue these commands from a modem command prompt (*chdev mdm*).

To examine prior disconnect reasons

AT-ADn

Substitute for *n* the number of disconnect reasons you would like displayed.

Normal disconnect reasons are:

- carrierLoss (expect just a small percentage of these)
- ds0Teardown
- dtrDrop
- escapeSequence
- inactivityTimeout
- loopLoss
- normalUserCallClear
- rcvdGatewayDiscCmd
- V.42DisconnectCmd

Other disconnect reasons may indicate trouble. Refer to the *Trouble Clearing Call Fails and Modem Disconnects* appendix in the HiPer DSP Reference manual for an explanation of disconnect reasons.

```
mdm24> at-ad3

(Ch.255): 11:22:50:184
Number of call disconnects since powerup is 2233.

(Ch.2): 11:22:50:184
Inbound call disconnect reason is Disconnect CMD.

(Ch.2): 11:22:50:184
Call start time 11:02:0426.  Call duration 00:00:13.

(Ch.1): 11:22:51:009
Inbound call disconnect reason is Normal user call clear.

(Ch.1): 11:22:51:009
Call start time 11:02:0426.  Call duration 00:00:22.

(Ch.6): 11:22:51:109
Inbound call disconnect reason is Received Disconnect command from
Gateway Card.

(Ch.6): 11:22:51:109
Call start time 10:18:041.  Call duration 00:45:06.
```

To examine prior call failure reasons

AT-AFn Substitute for *n* the number of call failure reasons you would like displayed.

Note that this is failure to achieve carrier between the two modems. Normal call failure reasons are:

- carrierLoss (expect just a small percentage of these)
- ds0Teardown
- normalUserCallClear

Others may indicate trouble. Refer to the *Trouble Clearing Call Fails and Modem Disconnects* appendix in the HiPer DSP Reference manual for an explanation of call failure reasons.

```
mdm24> at-af3

(Ch.255): 11:22:37:092
Number of failed calls since powerup is 129.

(Ch.15): 11:22:37:092
Inbound call failure reason is GSTN Cleardown Disconnect.

(Ch.15): 11:22:37:092
Call fail time 20:4:29.

(Ch.1): 11:22:37:117
Inbound call failure reason is Normal user call clear.

(Ch.6): 11:22:37:142
Call fail time 21:5:38.

(Ch.10): 11:22:38:017
Inbound call failure reason is No Carrier.

(Ch.10): 11:22:38:017
Call fail time 8:35:8.
```

Quad Modems

To monitor modem events

1. Click the top LED for all modems, or a single modem LED.
2. From the **Performance** menu, click **Session Monitor.**
3. From Functional Group, select **Modem Events**.
4. Select these parameters:
   - Incoming Connections Established
   - Incoming Connections Failed
   - Connect Attempt Failure
5. Click **Add**, then click **OK**.

In Total Control Manager for UNIX, you can graph these results.

To check for excessive connect times

1. Click the top LED for all modems, or a single modem LED.
2. From the **Performance** menu, click **Session Monitor.**
3. From Functional Group, select **Call Statistics**.
4. Select **Call Duration**. Click **Add**, then click **OK**.

Dual T1/PRI

To check CRC errors

1. Click the span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **Span Line**, then click **OK**.
4. From Functional Group, select **Span Line Current Group**.
5. Select **Current Excess CRC Errors**. Click **Add**, then click **OK**.

To check PRI D-channel status

1. Click the span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **Span Line**, then click **OK**.
4. From Functional Group, select **PRI Call Statistics**.
5. Select **D Channel Operational Status**. Click **Add**, then click **OK**.

To check DS0 status

1. Click the span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **Timeslot**, then click **Select All** (or select the DS0s you are interested in).Click **OK.**
4. From Functional Group, select **Timeslot (DS0) Status**. Click **Add**, then click **OK**.

Table 2 DS0 status possibilities

Status	Description
Idle	No call is connected
Dialing	The modem associated with this DS0 is placing a call
Ring received	The modem associated with this DS0 is receiving a call
Link negotiation	The modems are training
Connected	The modems have detected carrier and have connected

If a DS0 is perpetually Idle, check the DS0 service state and make sure it is In Service.

To check DS0 In-service Status

1. Click the span LEDs.
2. From the **Performance** menu, click **Session Monitor.**
3. Click **Timeslot**, then click **Select All** (or select the DS0s you are interested in).Click **OK.**
4. From Functional Group, select **DS0 in service state status**. Click **Add**, then click **OK**.

Then check the gateway card packet bus sessions (NETServer: *show all*; HiPer ARC: *list interfaces*) to make sure they are active.

Investigating Problems

This section explains techniques for in-depth investigation when you suspect a problem.

Chassis

Overheating

When the chassis overheats, the cards produce unusual events—incomplete calls, dropped calls, strange tones when dialing, or random card resets.

To check chassis temperature

1. Select the NMC.
2. From the **Performance** menu, click **Session Monitor**.
3. From Functional Group, select **Status Group**.
4. From Parameters, click **Chassis Temperature (.01 deg. C)**. Click **Add**, then click **OK**.

   The Ideal temperature range is 24–25° C. Be concerned if the temperature exceeds 40° C.

Quad Modems

To check DTE (bus) interface source

1. Click the top LED for all modems, or a single modem LED.
2. From the **Performance** menu, select **Session Monitor.**
3. From Functional Group, select **DTE Interface Settings**.
4. From Parameters, click **DTE Interface Source**. Click **Add**, then click **OK**.

To check line interface source

1. Click a modem (or top LED = all modems on card; or hold [Ctrl] and select multiple modems or top LEDs).
2. From the **Configure** menu, click **Programmed Settings.**
3. From Parameter Group, select **Line Interface Options**.
4. Line Interface Source indicates either t1Tdm, nic, or priTdm.

HiPer DSP

To examine Q.931 (D-channel) activity

If the D-channel is down (and the physical layer is good), perform a Q.931 trace and watch for messages being exchanged between the HiPer DSP and the telco switching equipment.

1 Enable a trace of facility 25. Facility 25 is Q.931 signaling. Level 0 is off, level 1 is most detailed, and level 5 is least detailed.

```
span1> trc dbg 25 2
Debug facility trace 25, level 2 activated
```

2 Disconnect the span from the jack at the HiPer DSP NIC. Wait five seconds.

3 Reconnect the span. Watch for messages for 30 seconds.

Messages on an active span look like this:

```
(Ch.0): 11:21:31:127
TN RX0: len = 4  00 01 01 98

(Ch.0): 11:21:37:122
TN RX0: len = 9  02 01 F4 98 08 02 03 5A 75

(Ch.0): 11:21:37:122
TN TX0: len = 4  02 01 01 F6

(Ch.0): 11:21:37:122
TN TX0: len = 16  00 01 98 F6 08 02 83 5A 7D 08 02 80 9E 14
```

4 Turn off tracing.

```
span1> trc off
Trace deactivated
```

- If no messages appear, the D-channel was probably disabled by the telco. Contact your telco.
- If messages appear, but the D-channel is still down (verify using *display d-chanop*), the switch type setting is probably incorrect.

To send a command to all 24 HiPer DSP modems at once

chmdm 255 Any command you send to modem 255 goes to all 24 modems at once.

```
mdm1> chmdm 255
mdm255> ati4
```

To map all HiPer DSP modem bus interfaces to the AUX port

AT-SU99 This command disconnects all modems from the packet bus and maps their serial connections instead to the AUX PORT. All modems respond as one to commands.

Mapping serial connections to the AUX port is useful for isolating the modems. If they work correctly through the AUX port, the problem must be with other components of the system. Check the packet bus or gateway card.

```
mdm1> chmdm 255
mdm255> at-su99
```

AT-SU100 After testing, send this command to map the modems' serial connections back to the packet bus.

```
mdm1> chmdm 255
mdm255> at-su100
```

You may need to reboot the gateway card (HiPer ARC or NETServer) to restore the packet bus connections.

HiPer ARC

Using HiPer ARC SYSLOG

HiPer ARC SYSLOG sends exhaustive data to the console interface, and optionally to a SYSLOG host or to a telnet session. Some examples of data you can log: call initiation process, IP, IPX, PPP, and SNMP.

For details about setting up SYSLOG, refer to the *Event Messages* appendix in the HiPer ARC Product Reference. For more detail, visit **http://interproc.ae.usr.com**.

show events Enter this command during a telnet session to cause the HiPer ARC to display SYSLOG data.

hide events Use this command to cease the display of SYSLOG data during a telnet session.

list facilities This command shows all the facilities you can have the HiPer ARC display.

set facility loglevel By default, all facilities are displayed at critical level—only critical events are displayed. Use this command to be more permissive about which events are displayed. You might change the log level, for example, if you suspect a particular facility as the cause.

```
set facility <“facility name”> loglevel <loglevel>
```

Send *list facilities* to view a list of facility names. If the facility name is more than one word, enclose the words in quotes.

Log Levels The log levels in order of increased information displayed:

- Critical
- Unusual
- Common
- Verbose

NETServer Issue this command from the NETServer's console interface, which is accessible by telnet or direct serial connection.

To check whether modems are connected to the packet bus

A typical symptom that occurs when modems are disconnected from the packet bus is a fast busy signal experienced by the caller.

show all This command gives the status of all the s-ports, which equate to serial connections to modems.

```
Command> sho all
Local Addr: x.x.250.126
   Gateway: x.x.150.62                       Netmask: 255.255.255.0

Port Speed Mdm Host             Type     Status      Input      Output     Pend
---- ----- --- ---------------- -------- ----------- ---------- ---------- ----
S0    9600 off                  Login/Ne USERNAME             0         27    0
S1   A I P on  -                Netwrk   IDLE                 0          0    0
S2   A I P on  -                Netwrk   IDLE                 0          0    0
S3   A I P on  -                Netwrk   IDLE                 0          0    0
S4   A I P on  -                Netwrk   IDLE                 0          0    0
S5   A R P on  -                Netwrk   IDLE                 0          0    0
S6   A R P on  -                Netwrk   IDLE                 0          0    0
S7   A R P on  -                Netwrk   IDLE                 0          0    0
S8   A R P on  -                Netwrk   IDLE                 0          0    0
S9   A R P on  -                Netwrk   IDLE                 0          0    0
...
```

Interpreting the Speed Column

The Speed column provides information about the modems and their connections to the packet bus.

Packet bus activity The first field indicates whether the packet bus connection is configured as active or inactive.

Table 3 Packet bus activity

Indicator	Meaning
A	Active
I	Inactive

Packet bus connection status The second field reflects the actual status of the packet bus connection. It has four possible values:

Table 4 Packet bus connection status

Indicator	Meaning
A	Activating. The packet bus is forming the connection.
D	Disconnecting. The packet bus connection is being taken down.
I	Inactive. Either the port has been configured as Inactive or the modem has been physically disconnected.
R	Ready. The packet bus connection is up and ready.

Modem presence The third field indicates whether a modem is physically present:

Table 5 Modem presence

Indicator	Meaning
P	Modem present
?	Unidentifiable device present (can indicate transition between **–** and **P**)
–	Empty slot

set debug 0xnn *nn* is a hex value between 00 and FF.

Table 6 Useful debug settings (for a complete list see Appendix)

0x00	Ends debug
0x18	Logs route updates
0x51	PPP / LMI / Annex-D status
0x1200	Show packet destination, type, and length

set console The NETServer displays results to the console during a telnet session.

reset console Stops the flow of debug information.

PPP System

HiPer ARC and NETServer, as well as Windows 95/98 clients, offer tools for PPP exploration.

To capture a PPP session using NETServer

1 From a NETServer command prompt, send the commands *set debug 0x51* and then *set console*.

```
Command> set debug 0x51
Setting debug value to 0x51
Command> set console
Setting CONSOLE to admin session
```

2 Capture the PPP session (save it as a text file).

3 Reset the console.

```
Command> reset console
Console RESET
```

4 Turn off debug.

```
Command> set debug 0x00
Setting debug value to 0x0
```

To capture a PPP session using HiPer ARC

1 From a HiPer command prompt, enter **monitor ppp**, or an abbreviation.

```
HiPer>> mon ppp
Hiper PPP Monitor

 Select a letter for one of the following options:
```

2 Select one of the monitoring options from the list, depending on what exactly you are trying to figure out.

3 Press Esc to stop monitoring.

4 Capture the PPP session (save it as a text file).

5 Press Esc to end the session.

6 Press X to close PPP Monitor.

To diagnose problems with PPP negotiation

Usually a configuration issue, such as:

- A mismatch in addressing between server and client
- A bad IP pool on the HiPer ARC, NETServer, or RADIUS Server

To generate a modem event log with Windows 95/98

Compare this with the PPP negotiation data gathered from the HiPer ARC or NETServer.

1. Right-click the icon for the dial-up connection. From the menu that appears, select **Properties**.
2. From the **General** tab, click **Configure.**
3. Select the **Connection** tab, and then click **Advanced**.
4. From the Advanced Connection Settings dialog, select **Record a log file**.

   When you make a call using Dial-Up Networking, Windows writes the modem events in the following file: **\windows\modemlog.txt**

To generate a PPP event log with Windows 95/98

Compare this record to the record from the HiPer ARC (*monitor ppp*) or NETServer (*set debug 0x51*).

1. From the Windows taskbar, click **Start**, then **Settings**, then **Control Panel**.
2. Double-click **Network**.
3. Click **Dial-Up Adapter**, then click **Properties**.
4. Click the **Advanced** tab.
5. For the property **Record a log file**, select the value **Yes**.

   You must restart your computer before PPP logging will start.

   When you make a call using Dial-Up Networking, Windows writes the PPP events in the following file: **\windows\ppplog.txt**

PPP Requests for Comments

Table 4 lists the PPP Requests for Comments (RFCs) that are relevant for debug.

Table 7 PPP Debug-Relevant RFCs

RFC #	Title
RFC 1661	The Point-to-Point Protocol (PPP)
RFC 1662	PPP in HDLC-like Framing
RFC 1334	PPP Authentication Protocols
RFC 1994	PPP Challenge Handshake Auth. Protocol (CHAP)
RFC 1332	The PPP IP Control Protocol (IPCP)
RFC 1552	The PPP IPX Control Protocol (IPXCP)
RFC 2097	The PPP NetBIOS Frames Control Protocol (NBFCP)
RFC 1990	The PPP Multilink Protocol (MP)
RFC 1700	Assigned Numbers

For more information, refer to Carlson, James: PPP Design and Debugging. Addison-Wesley Publishing Company; ISBN: 0201185393.

RADIUS System

Follow these steps to diagnose authentication problems between a HiPer ARC (which is a Remote Authentication Dial-In User Service [RADIUS] client) and a RADIUS server.

Keep in mind that the most common reason for authentication failure is an incorrect shared secret.

1 Determine whether you can ping the security server from the HiPer ARC.

If not, perform standard IP troubleshooting. When you can ping the security server, proceed to the next step.

```
HiPer>> ping x.x.250.111
PING Destination: x.x.250.111 Status: ALIVE
```

2 Open two telnet sessions to the HiPer ARC.

Session 1: Run RADIUS monitor.

a From a HiPer command prompt, enter **monitor radius**, or an abbreviation.

```
HiPer>> mon rad
HiPer RADIUS Monitor

 Select a letter for one of the following options:
```

b Select one of the monitoring options from the list, depending on what exactly you are trying to figure out.

Session 2: Run authentication test.

c From a second telnet session, enter **_authenticate <username> <password>**. Do not type the angle brackets, but use a username and password that you are certain is in the RADIUS server database.

```
HiPer>> _auth userx xyz123
CLI - User: userx is Authenticated
```

d Watch what happens in the first telnet session.

```
---------------------------------------------------------------------
   Source-IP        Src-Port Destination-IP Dest-Port Id Packet-Type
---------------------------------------------------------------------
  x.x.250.122         1645    x.x.250.111      1645    7 Access-Reque
---------------------------------------------------------------------

                    User-Name : jim
                User-Password : xxxxxxxxxx
               NAS-IP-Address : x.x.250.122
```

One of the following happens:

- You receive an Access-Accept message
- You receive an Access-Reject message
- You receive no response at all

See the following table for information about what to do about responses from the security server.

Table 8 What to do about responses from the security server

Response	What to do
Access-Accept	Nothing. This indicates correct operation.
Access-Reject	Verify that the username/password are listed in user table. This indicates that the security server is receiving the Access-Request packet but cannot find the username/password in its user table. Verify that the shared secret between the client and server matches exactly.
None	Verify that the security server is receiving packets. Verify that the client and server are communicating using the same UDP port. The well-known UDP port for RADIUS authentication traffic is 1645.

Tools

- SECURITY.LOG on Total Control S/A Server—Assuming packets are making it through, this is your best source. It shows every packet that comes in.
- CLIENT.EXE included with Windows S/A Server can run from anywhere but remember you have to add that station as a client at the security server!
- LOGONT.EXE on Windows NT when using SAM database proxy LOGONT <USERNAME> <PASSWORD> [DOMAIN]
- NETMON comes on Windows NT CD-ROM but is not installed by default. Start | Programs | Administrative Tools | Event Viewer. Will capture only those packets coming to or leaving the computer it’s running on.
- DICTNARY.DAT If you don’t know what a value means.
- DEBUG.LOG and ERROR.LOG (associated with third-party security servers).

Windows Log Location

- If running S/A Server as an application: **\usrsuite\security\security.log**
- If running S/A Server as a service: **\winnt\system32\security.log**

UNIX Log Location

- /SA60/LOG/SASERV.LOG

If you cannot determine the cause of the problem by comparing HiPer ARC and Security server log files, insert your workstation in the routed path between them and monitor the IP packets being exchanged.

If you have a UNIX-based computer, you can run either of two freeware IP analyzers, SNOOP (for Sun computers) or TCPDUMP (for others).

Once you capture the packets, use RADDEBUG, a 3Com internal-use tool to decode them. See **http://coredump.ae.usr.com/radius/**

To capture a PPP session using NETServer

These commands capture basics of the RADIUS negotiation at the Link Control Protocol (LCP) level. For help in interpreting the results, contact 3Com Customer Support.

1 From a NETServer command prompt, send the commands *set debug 0x51* and then *set console*.

```
Command> set debug 0x51
Setting debug value to 0x51
Command> set console
Setting CONSOLE to admin session
```

2 Capture the RADIUS session (save it as a text file).

3 Reset the console.

```
Command> reset console
Console RESET
```

4 Turn off debug.

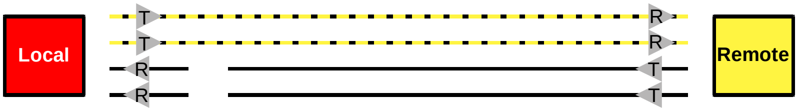
```
Command> set debug 0x00
Setting debug value to 0x0
```

Correcting Problems

Span Alarms

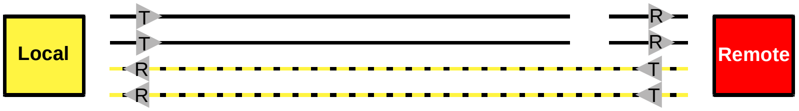
Red

A device experiences a red alarm when the signal it receives is not valid. A device experiencing red alarm sends a yellow alarm signal on its transmit pair.



Yellow

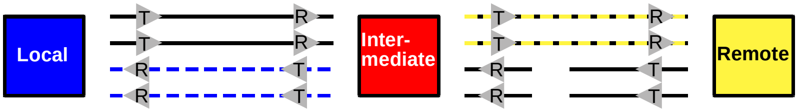
A device experiences a yellow alarm when it receives a yellow alarm signal. This means the device immediately upstream is not receiving a valid signal (it is experiencing red alarm).



A yellow alarm is also known as a Remote Frame Alarm (RFA).

Blue

A device experiences a blue alarm when it receives a blue alarm signal. This means the device upstream (an intermediate device, such as an intelligent repeater) is not receiving a valid signal from *its* upstream device.



The intermediate device is in red alarm, and the remote device is in yellow alarm.

A blue alarm is also known as an Alarm Indication Signal (AIS).

Telco Loopback Testing

The telco initiates loopback tests. They loop the line at the smart jack and run a standard battery of tests. This will verify signal integrity up to the demarc (point of demarcation between the telco's equipment and yours). You can set up the hub so it performs the loopback (instead of the smart jack), to check the path all the way to the hub. If the line is clean to the demarc and faulty when looped to the hub, the problem is usually with the premises wiring.

Dual PRI

To resolve a RED alarm on a T1/PRI

Examine the premises wiring. Verify that the switch configuration and Total Control configuration match. Check out the cables, the Dual PRI hardware, and power. If you cannot solve the problem, report the problem to the telco and ask the telco to perform a loopback test.

To resolve a YELLOW alarm on a T1/PRI

Examine the premises wiring. If the physical connection is good, call telco.

If CRC errors are incrementing

Examine the premises wiring. Check out the cables, the Dual PRI hardware, and power. If you cannot solve the problem, report the problem to the telco and ask the telco to perform a loopback test.

If all DS0s go down simultaneously

Examine premises wiring. Check for alarm conditions. Then call the telco.

HiPer DSP

To resolve a RED alarm on a T1/PRI

Examine the premises wiring. Verify that the switch configuration and Total Control configuration match. Check out the cables, the HiPer DSP hardware, and power. If you cannot solve the problem, report the problem to the telco and ask the telco to perform a loopback test.

To resolve a YELLOW alarm on a T1/PRI

Examine the premises wiring. If the physical connection is good, call the telco.

If CRC errors are incrementing

Examine the premises wiring. Check out the cables, the HiPer DSP hardware, and power. If you cannot solve the problem, report the problem to the telco and ask the telco to perform a loopback test.

If all DS0s go down simultaneously

Examine premises wiring. Check for alarm conditions. Then call the telco.

If D-channel is down

If D-channel is down, do a Q.931 trace to see whether messages are being passed at all. If not, call telco and ask them to bring up the D-channel.

Quad Modem

To change line interface source

The Line interface source of the Quad (T1tdm, PRItdm, or nic) must match that of the telco access card.

1 Click a modem (or top LED = all modems on card; or hold [Ctrl] and select multiple modems or top LEDs).

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

3 From Parameter Group, select **Line Interface Options**.

4 From Line Interface Source, select t1Tdm, nic, or priTdm.

NETServer

To join modems to the packet bus

To join modems to the packet bus, use the *set modem active* command. To interpret the results of the *show all* command, see To check whether modems are connected to the packet bus on page 40.

```
Command> show all
Command> set modem s5-s8 active
Command> save all
Command> reset s5-s8
Command> show all
```

x2 and V.90 Troubleshooting

x2 troubleshooting is covered in detail in the paper *x2: Understanding the Issues / Troubleshooting Problems*, which is available from the TotalService web site as filename **x2shoot4.pdf**.

V.90 troubleshooting is covered in detail in a paper that is to-be-determined.

Visit and search the 3Com Carrier Technical Support web site at **http://totalservice.3com.com**.

APPENDIX

NETServer Debug Settings

This is a complete list of debug settings for NETServer.

Table 9 NETServer debug settings

0x00	Ends debug
0x18	Logs route updates
0x51	PPP / LMI / Annex-D status
0x54	Displays the last 60 characters of in/out flow control when you issue the command show port
0x72	Watch FLASH
0x74	Last 60 characters of input/output
0x75	Last 60 characters of input/output—verbose
0x78	Telnet negotiation options
0x81	ARP updates
0x1100	Debugs RIP
0x1200	Show packet destination, type, and length

INDEX